DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BAJO LA NORMA ISO/IEC 27001 PARA EL DEPARTAMENTO DE SISTEMAS DE LA FUNDACIÓN UNIVERSITARIA TECNOLÓGICO COMFENALCO, UTILIZANDO LA METODOLOGÍA DE ANÁLISIS DE RIESGO MAGERIT V 2.0

FREDY PATERNINA MATOS

EDER SANTANA PÉREZ

UNIVERSIDAD TECNOLOGICA DE BOLIVAR

FACULTAD DE TELECOMUNICACIONES

CARTAGENADE INDIAS

2010

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BAJO LA NORMA ISO/IEC 27001 PARA EL DEPARTAMENTO DE SISTEMAS DE LA FUNDACIÓN UNIVERSITARIA TECNOLÓGICO COMFENALCO, UTILIZANDO LA METODOLOGÍA DE ANÁLISIS DE RIESGO MAGERIT V 2.0

FREDY PATERNINA MATOS

EDER SANTANA PÉREZ

Monografía de grado presentado como requisito para optar al título de

Especialista en Telecomunicaciones

UNIVERSIDAD TECNOLOGICA DE BOLIVAR

FACULTAD DE TELECOMUNICACIONES

CARTAGENA DE INDIAS

2010

Cartagena de Indias, 21 de Octubre 2010

Señores
Comité curricular del programa de Telecomunicaciones
Universidad Tecnológica de Bolívar
L. C.

Respetados señores:
Por medio de la presente nos permitimos informarles que la monografía titulada **"Diseño de un sistema de gestión de seguridad de la información bajo la norma ISO/iec 27001 para el departamento de sistemas de la Fundación Universitaria Tecnológico Comfenalco, utilizando la metodología de análisis de riesgo Magerit v 2.0"** ha sido desarrollada de acuerdo a los objetivos y justificaciones establecidas con anterioridad.

Como autores de la monografía consideramos que el trabajo investigativo es satisfactorio y merece ser presentado para su evaluación.
Atentamente,

FREDY PATERNINA MATOS **EDER SANTANA PÉREZ**

Nota de aceptación

……..

……..

……..

Presidente del jurado

……..

Jurado

……

Jurado

……

Cartagena Octubre 21 de 2010

DEDICATORIAS

Dedico este logro de mi vida a mis padres quienes me dieron la fuerza

Y que apoyados de la mano de Dios nunca me

Dejaron desfallecer en este largo camino

Eder Santana Pérez

Agradezco primero antes que nada a Dios por estar conmigo en cada paso que doy

Y haberme iluminado cuando todo se oscurecía, también a mi madre Aura Matos

por estar conmigo todo el tiempo y por estar siempre apoyándome en las

Decisiones que tome en la trayectoria de mi carrera y brindándome

El más sincero amor, a mis tíos por comprenderme cada día y noche

Que pase estudiando

Fredy Paternina Matos.

Pág.

Glosario

- **Definición del ámbito o alcance:** En esta fase es donde se define y se delimita las áreas de aplicabilidad del sistema de gestión.

- **Identificación de Activos de Información**: Esta es la parte donde se puede definir e identificar todo aquello que genera un valor para la organización, todo lo relacionado con los sistemas de información.

- **Tasación de los activos de información:** En esta parte se define cuanto valor representa el activo para la organización teniendo en cuenta los criterios establecidos tales como confidencialidad, integridad, confidencialidad y autenticidad.

- **Análisis GAP:** Esta fase hace más referencia a la revisión y balance de las falencias que presenta la organización en cuanto a la seguridad y los sistemas de información.

- **Análisis de riesgo:** Etapa donde se valora el impacto y los riesgos de las que está expuesta la organización.

- **Definición de políticas de seguridad:** Componente donde se definen los lineamientos específicos para la gestión y seguridad de la información.

- **Selección de Controles:** Estos controles son mecanismos para establecer las políticas de seguridad.

- **Definición de la documentación:** En esta parte es donde se establecen y se redactan los documentos que apoyaran los controles de seguridad.

- **ISO/IEC 27001:** Es un estándar internacional que permite realizar a cabalidad un sistema de gestión de seguridad de la información, este estándar se basa en la gestión de riesgos y subministra las pautas necesarias para la implementación de controles y la creación de políticas de seguridad. La ISO/IEC 27001 BS 7799-2:2005, está orientada a aspectos netamente organizativos y por tal motivo busca proponer el establecimiento, implementación, operación, monitorización de la gestión de la seguridad de la información.

- **BS7799**: Esta sirve para la auditoria del sistema de gestión de seguridad de la información, y está basada en los requisitos que deben ser cubiertos por la organización, y contiene especificaciones para certificar los dominios individuales de seguridad para poder registrarse en esta norma; los dominios de control son 11 y estas contemplados de la siguiente manera.

- **MAGERIT V2:** Es una metodología desarrollada para el análisis y la gestión de riesgos de los sistemas de información, esta proporciona las pautas, las técnicas y los métodos necesarios para auditar sistemas de información que manejan medios electrónicos, informáticos, telemáticos e información mecanizada en sus operaciones. MAGERIT está estructurado en tres fases que se pueden implementar a una solución de una SGSI como son:

- **Planificación:** En esta primera fase se identifican y se definen los objetivos, la pertinencia, los requerimientos y las condiciones necesarias para realizar un proyecto.

- **Análisis de Riesgo:** En esta fase hace más énfasis en la identificación de todos y cada uno de los activos a tratar en la organización, sus dependencias y las amenazas a las que están expuestos. También se tiene en cuenta el impacto, la degradación y la frecuencia que tienen cada una de estas amenazas en el activo, analizando las salvaguardas existentes pata mitigar este efecto.

- **Gestión de riesgos:** En esta última fase se buscan los mecanismos y las salvaguardas apropiadas y oportunas para mitigar el impacto y el riesgo de cada una de las amenazas a niveles aceptables a través del diseño de un plan de seguridad.

- **DISPONIBILIDAD:** Es la disposición de los servicios a ser usados cuando sea necesario. También podemos decir que es la propiedad que puede ser accesible y utilizable a pedido de un agente autorizado.

- **INTEGRIDAD:** Es la propiedad de salvaguardar la exactitud y completitud de los activos. Contra la integridad, la información puede aparecer manipulada, corrupta o incompleta. La integridad afecta directamente al correcto desempeño de las funciones de una organización.

- **CONFIDENCIALIDAD:** Consiste en que la información llegue solamente a las personas autorizadas. Contra la confidencialidad pueden darse fugas y filtraciones de información, así como accesos no autorizados. También se puede decir que es la propiedad de la información que no se revela ni se encuentra a disposición de individuos, organizaciones o procesos no autorizados.

- **AUTENCIDAD (De quien hace uso de los datos o servicios):** Este término hace referencia a que no hay duda de quién se hace responsable de una información o prestación de un servicio, tanto a fin de confiar en él como de poder perseguir posteriormente los incumplimientos o errores.

A normalizar este esfuerzo se dedican las metodologías de análisis y gestión de riesgos que comienzan con una definición:

- **Riesgo:** Es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización. El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente; un riesgo para un sistema informático está compuesto por la terna de activo, amenaza y vulnerabilidad, estos conceptos se define a continuación:

- **Activo:** Sistema o conjunto de sistemas sobre los que se desea calcular el riesgo asociado.

  El activo tendrá un valor que consistirá en la suma de todos los costes necesarios para volver a la normalidad ante un ataque a su seguridad.

  Cabe resaltar que los activos son clasificados por la **ISO17799:2005** en las siguientes categorías.

  - **Activos de información** (Datos, manuales, usuarios, etc.).
  - **Documentos de papel** (Contratos).
  - **Activos de software** (Aplicación, software de sistemas etc.)
  - **Activos Físicos** (Computadores, medio magnético etc.)
  - **Personal** (Clientes, personal)
  - **Imagen de la compañía y reputación.**
  - **Servicios** (Comunicaciones etc.)

- **Amenaza:** Las amenazas comprenden todos los agentes que pueden atacar a un sistema; entre esas amenazas se pueden resaltar las catástrofes naturales, cortes de tensión, virus informáticos o los hackers.

- **Vulnerabilidades:** Una vulnerabilidad es un punto en el que un recurso es susceptible de ataque. Los sistemas poseen un grado de facilidad para ser atacados.

- **Análisis de Riesgo:** Es un proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una organización. Sabiendo lo que podría pasar; A demás sirve para identificar dichos riesgos, cuantificar su impacto y evaluar el costo para mitigarlos.

- **Gestión de riesgos:** es aquella selección e implementación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados. También se puede decir que son las actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.

RESUMEN

En la **Fundación Universitaria Tecnológico Comfenalco** existe un componente fundamental en el proceso de negocio: *la Información*. Uno de los mayores retos de las organizaciones, y en especial de los Departamentos de Sistemas e Informática, es garantizar la seguridad de la información y de los recursos informáticos. Por tanto, los profesionales en informática deben reflexionar sobre los conceptos tradicionales en el área de seguridad, para procurar mayores y mejores niveles de aseguramiento de la información, con el fin que se concienticen de la necesidad de salvaguardar su información, a través de mecanismos que garanticen el mantenimiento de la integridad, confidencialidad y disponibilidad de la misma.

El estudio que se desarrolla a continuación sobre la norma **ISO/IEC 27001:2005** será necesario para la estructuración del diseño de un Sistema de Gestión de Seguridad de información **(SGSI),** que permitirá "Organizar la seguridad de la información" bajo estándares internacionales que generen mayor confianza en la utilización de las redes de datos que maneja la **Fundación Universitaria Tecnológico Comfenalco**.

Como parte preliminar de este documento se hace una introducción a ciertos conceptos y razones que aclaran acerca de la necesidad de tener un SGSI por lo tanto sea estructurado en varias etapas iniciando con la **Determinación del Ámbito** o el alcance que tendrá el **SGSI** (Sistemas de Gestión de la Seguridad de la Información) sobre el cual girara el estudio para encontrar las recomendaciones acerca de los controles y políticas que se deben aplicar en esta. Seguidamente se realiza una **Identificación de los Activos** de información que hace parte del ámbito y las posibles amenazas a que estos están expuestos.

En el diseño del sistema de gestión de seguridad de información, para el Departamento de Sistemas de la **Fundación Universitaria Tecnológico de Comfenalco,** se llevara un procedimiento el cual cubre varias etapas las cuales comienza con el entendimiento de los requerimientos del modelo, en donde se hizo necesario y preciso manejar técnicas de recolección de información como fueron entrevistas al personal encargado del Sistemas y al Director del Departamento, los cuales nos abrieron las puertas para que se pudiera desarrollar la investigación plenamente en la Institución. Esta parte del proceso se divide en sub-actividades las cuales son:

- **Conocimiento del Departamento de Sistemas:** En este punto, se procede a reconocer la misión y visión, así como las funciones de cada uno de los que laboran en las División, Además de esto se solicitó los manuales de procedimientos en los cuales están redactados las tareas y actividades que debe realizar estrictamente.

- **Identificación de Activos de información:** En esta etapa se pidió el inventario de activo actualizado, con el fin de identificar los activos con que cuenta el Departamento de Sistemas, así como preguntas directas al director y los jefes de esta sección, Además de esto también se indago acerca de la importancia de cada activo, de que tan indispensable era para la división y la institución si alguno de estos hiciera falta.

- **Valoración de activos de información:** Ya habiendo establecido claramente los activos de información con que cuenta cada división, continuamos con darle valor a cada activo teniendo en cuenta lo parametrizado en la metodología Magerit V2, este paso lo que pretende brevemente es darle un valor en cuanto a ciertos criterios tales como disponibilidad, integridad de los datos, confidencialidad de los datos, autenticidad de los usuarios y autenticidad de el origen de los datos, así como también la trazabilidad del servicio y de los datos.

Con la ayuda de **MAGERIT Versión 2** (Metodología de Análisis de Riesgo), se calculara el impacto que estas tendrían sobre los activos y con este resultado entrar a la etapa de análisis de riesgo que permitirá definir los requerimientos y/o salvaguardas del sistema de gestión de seguridad de información.

Para esta valoración se puede tomar cualquier escala de valores pero para ceñirnos a la pauta de **Magerit V2**, se usó una escala común para todas las dimensiones, teniendo en cuenta que es cualitativa por cada una se tomó un grado del 0 al 10, teniendo en cuenta que 0 es despreciable, 1- 3 bajo, 4-6 medio, 7-9 alto y 10 muy alto, esto para simplificar la tarea a el momento de realizar un análisis de riesgo. En estos puntos está incluida la seguridad de las personas, la información de carácter personal, las obligaciones derivadas de ley, la capacidad para la persecución de delitos, intereses comerciales y económicos, pérdidas financieras y por último la interrupción del servicio.

La segunda fase tiene por nombre **Determinación de la brecha** en esta etapa lo que se trata de determinar que tanto se tiene implementado en el Departamento de Sistemas, como los son controles y políticas para la seguridad de la información teniendo en cuenta lo parametrizado en la **norma ISO 27001**, entre los ítem que se comparan están los 11 puntos de políticas de seguridad que son: organización de la seguridad, clasificación y control de activos, seguridad personal, seguridad física y ambiental, gestión de comunicaciones y operaciones, control de accesos, desarrollo, mantenimiento de sistemas, administración de la continuidad del negocio y cumplimiento.

Para realizar esta etapa tuvimos que implementar una actividad que en los sistemas de seguridad de información se le conoce como **Análisis GAP**, el cual es una herramienta metodológica que nos permite comparar dos prácticas distintas

una de las practicas es aquella que está utilizando en el Departamento de Sistemas y la otra es aquella que establece un estándar que es aceptable mundialmente **ISO/IEC 27001:2005**, la cual está basada en un conjunto de documentos y herramientas que demuestran y ayudan a realizar la gestión de la seguridad. El objetivo es saber que le hace falta a una de estas.

Luego de haber hecho el análisis Gap completamente procedemos a determinar la brecha lo cual se hizo teniendo como base los porcentajes totales que presento EL departamento en el Checkeo anterior, los cuales dicen que tan cerca se encuentra la empresa con las políticas que deberían estar implementadas.

Un paso muy vital e importante el cual se convierte en otra etapa de nuestro proyecto es el de **Análisis y Evaluación de Riesgo** para efectuar este hay que tener en cuenta los riesgos y amenazas posibles sobre los activos; Entre las amenazas y riesgos que se pueden evaluar están desastres naturales, de origen industrial, errores y fallos no intencionados y por ultimo ataques intencionados. Al ser capaces de reconocer las posible amenazas tendremos también la capacidad de crear contramedidas para estas, las cuales minimicen y en el mejor de los casos eviten que alguna de estas se lleve a cabo, este punto también es importante.

El siguiente paso se realiza teniendo en cuenta todo lo anteriormente recopilado acerca de los activos de la institución los riesgos y amenazas, este paso se denomina **Cálculo del Impacto Acumulado,** Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema.

El impacto acumulado contiene el valor calculado del activo tanto así como el de los que dependen de él, también sujeta las amenazas a que está expuesto. Este se calcula por cada activo, cada amenaza y cada dimensión de valoración. El objetivo de este paso en la metodología es determinar las salvaguardas de que hay que dotar a los medios de trabajo.

De esta manera, las políticas de seguridad en informática emergen como el instrumento para concientizar a sus miembros acerca de la importancia y sensibilidad de la información y servicios críticos, de la superación de las fallas y de las debilidades, de tal forma que permiten a la institución cumplir con su misión.

Finalmente se diseña la estructura documentaria de las políticas de seguridad, guías, controles y procedimientos aplicar dentro del Departamento de Sistemas de la **FUNDACIÓN UNIVERSITARIA TECNOLÓGICO COMFENALCO,** basados en toda la información arrojada en todas estas etapas mencionadas.

1. INTRODUCCIÓN

Con la evolución y avance en nuevas tecnologías, la historia nos ha mostrado que la información se ha convertido en la herramienta fundamental de las organizaciones que le permite desarrollar nuevos modelos de negocios, mejorarlos y tomar decisiones que le ayuden a establecer ventajas competitivas dentro de su mercado. La forma como puede estar representada la información puede ser muy variable, la podemos encontrar escrita en papel, difundiéndose por medios electrónicos, o almacenada en cualquier dispositivo de almacenamiento; Por lo tanto cualquiera que sea la forma que adquiera esta, se debe tener presente que no está exenta de estar expuesta a ciertas amenazas y vulnerabilidades que puedan causar degradación total o parcial de la información y que ponen en riesgo la continuidad comercial del negocio; Antes que todo esto ocurra, se debe tener procedimientos y políticas que protejan la información como un activo de mucho valor para la organización o negocio en cuestión.

Como modelo para establecer un Sistema de Gestión de Seguridad de Información, la organización internacional de estándares (ISO) ha diseñado la norma 27001:2005 en la cual se contemplan las pautas para el establecimiento del mismo convirtiéndola en la mejor herramienta para profesionales, estudiantes y gerentes, que desean proteger su información con altos estándares internacionales.

1.2 PLANTEAMIENTO DEL PROBLEMA

1.2.1 DESCRIPCIÓN DE LA SITUACIÓN GENERAL

La Fundación Universitaria Tecnológico Comfenalco cuenta con mecanismos de control para asegurar la confidencialidad, integridad y disponibilidad de la información. Estos mecanismos han sido implantados a través de herramientas como: Windows 2003 Server e ISA Server entre otros, en donde se tienen configurados diferentes parámetros que permiten establecer controles de acceso por parte de los usuarios a diferentes tipos de información. Estos mecanismos no son suficientes para garantizar un alto nivel en la gestión de la seguridad, la eficiencia y la protección de la información, tanto de manera física como de manera lógica.

Un sistema de gestión para la seguridad de la información no debe implementarse por mantener un esquema, sino que deben ser fundamentado bajo un estándar existente que proteja uno de los activos más importante de la Fundación Universitaria Tecnológico Comfenalco como lo es la información, ya que el flujo y almacenamiento de la misma es muy alto y por lo tanto se debe garantizar la confidencialidad, integridad y disponibilidad de la información que son factores esenciales para mantener ventajas competitivas.

Como sabemos, La información es un activo que, como otros activos importantes del negocio, tiene valor para la organización y requiere en consecuencia una protección adecuada.

1.2.2 FORMULACIÓN DEL PROBLEMA

¿CÓMO EL DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN (SGSI) PUEDE MINIMIZAR EL RIESGO Y MEJORAR SU GESTIÓN Y PROTECCIÓN DE LOS ACTIVOS TANTO DE CARÁCTER LÓGICO COMO FÍSICO POR MEDIO DE LOS CONTROLES Y POLÍTICAS DE SEGURIDAD PARA EL SISTEMAS DE INFORMACIÓN DEL DEPARTAMENTO DE SISTEMAS DE LA **FUNDACIÓN UNIVERSITARIA TECNOLÓGICO COMFENALCO**?

1.3 OBJETIVOS

1.3.1 OBJETIVO GENERAL

Diseñar un Sistema de Gestión de Seguridad Informático (SGSI) basado en los estándares de la ISO 27001, utilizando la metodología de análisis de riesgo de los sistemas de información MAGERIT V2, para el Departamento de Sistemas de la **Fundación Universitaria Tecnológico Comfenalco**, con el fin de gozar y garantizar la confidencialidad, integridad y disponibilidad de la información.

1.3.2 OBJETIVOS ESPECÍFICOS

- ✓ Identificar los activos y la importancia de estos para la organización y entender el esquema de trabajo o funciones que estas realizan.

- ✓ De acuerdo a la metodología de análisis de riesgo, Identificar las falencias, amenazas y riesgos a los cuales están expuestos los activos de la información, determinando el impacto que estos ocasionarían a la Universidad.

- ✓ Determinar las políticas y controles pertinentes como medidas de seguridad para la preservación de la integridad, confidencialidad y disponibilidad permitiendo gestionar los riesgos identificados.

- ✓ Diseñar la estructura documentaria de políticas, guías, controles y procedimientos aplicados, basados en la norma ISO 27001 del diseño del sistema de gestión seguridad de la información para el Departamento de Sistemas de la **FUNDACIÓN UNIVERSITARIA TECNOLÓGICO COMFENALCO.**

1.4 JUSTIFICACIÓN.

El mundo de hoy gracias a la evolución y la construcción de grandes redes de telecomunicaciones, han contribuido a que muchas organizaciones manejen grandes volúmenes de información, ya sea a través de redes públicas o privadas para el normal desarrollo de sus actividades, por lo tanto la información, constituye uno de los recursos más importante dentro de la empresa la cual debe gozar de alta confidencialidad, integridad y disponibilidad en el momento requerido.

Para toda organización es vital determinar el grado de importancia que tiene la información que estas manejan, para ello se debe tener implementado ciertos mecanismos que garanticen la seguridad de la misma.

Los controles expuestos en la norma ISO 27001 definen los requerimientos necesarios para diseñar un sistema de gestión de la seguridad de la información, por lo tanto estos deben ser objeto de estudio para una correcta aplicación de la norma y futuras certificaciones.

La **FUNDACIÓN UNIVERSITARIA TECNOLÓGICO COMFENALCO** es una institución educativa que tiene como visión la estandarización y certificación de muchos de sus procesos, por ende se muestra pertinente un estudio que tenga como finalidad el diseño de un sistema de gestión de la seguridad de la información basada en la norma ISO 27001.

1.5. ALCANCE, BENEFICIOS Y P*E*RTINENCIA

El sistema de Gestión de Seguridad de Información (**SGSI**) que se diseñara para el Departamento de Sistemas de la **FUNDACIÓN UNIVERSITARIA TECNOLÓGICO COMFENALCO,** contribuirá a establecer un marco de gestión , que proporcionara un mayor nivel de seguridad en la Confidencialidad, Integridad, Disponibilidad y Autenticidad de la información, esta será objeto de tratamiento en la organización ya que el **SGSI** será diseñado bajo los conceptos desarrollados en la Metodología de Análisis y Gestión de Riesgo de los sistemas de Información **(MAGERIT – Versión 2).** Apoyando la normatividad **BS 17799:2005(ISO/IEC 27001:2005)** para la selección de controles.

Este **SGSI** se centra en el procesamiento e interrelación de la información que se genera en la Departamento de Sistemas del Tecnológico Comfenalco.

Además, con este diseño se obtendrán muchos beneficios para la organización tales como:

- ✓ Contar con la protección apropiada de los activos de información.
- ✓ Establecer controles para cada uno de los activos de información.
- ✓ Reducir los riesgos relacionados con los errores humanos, robo, fraude o mal uso de la información teniendo en cuenta aspecto como:
  - ➢ Incluir la seguridad como parte de las responsabilidades del personal.
  - ➢ Acuerdos de confidencialidad.
  - ➢ Entrenamiento al personal**.**

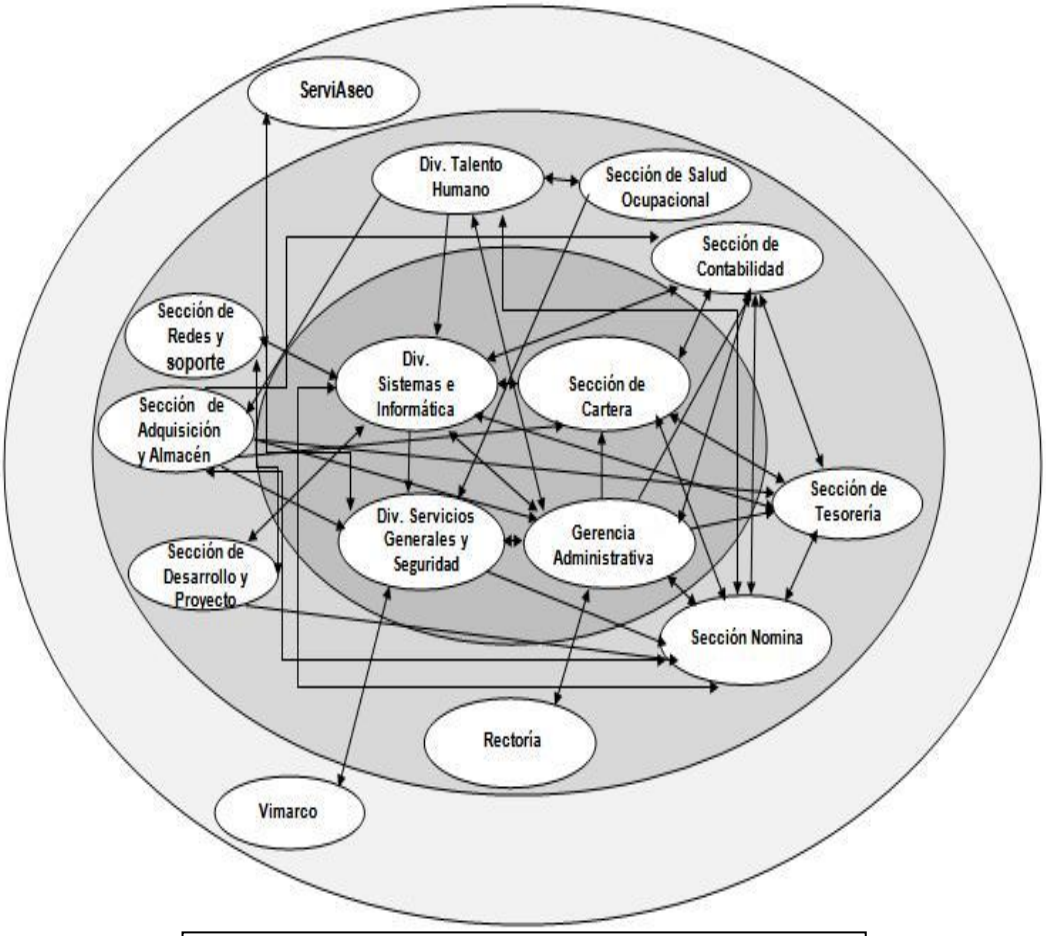
- Manejo de incidente de seguridad.

✓ Aumentar el grado de confianza en el uso de los sistemas de información. Proyecto

Todo lo anterior justifica la intención de adelantar este proyecto, ya que con este se podrá minimizar el impacto de una eventual de amenaza a la organización y facilitar la recuperación si esto se presenta, colocándolos a un nivel aceptable para la operación y buen funcionamiento de los procesos llevados a cabo en el Departamento de Sistemas de la **FUNDACIÓN UNIVERSITARIA TECNOLÓGICO COMFENALCO.**

En materia de alcance es válido señalar que nuestro propósito es el de diseñar controles y políticas de seguridad, teniendo en cuenta la definición del ámbito que se tomó, identificación de activos de información, todo esto esta encasillado dentro de la fase de entendimiento de los requerimientos del modelo, otro paso el cual abarcaremos será el de determinación de la brecha donde se realizaran las actividades concernientes a el análisis GAP y determinación de la brecha, seguido a esto y como fase final tocaremos la etapa de análisis y evaluación de riesgo, donde se efectuara el análisis y la evaluación de los mismos y posteriormente la redacción de controles y políticas de seguridad, todo esto se hará apoyado de las guías que nos brinda **MAGERIT versión 2.**

1.6 Definición del Ámbito



Fuente: Diseño de un sistema de Gestión de Seguridad de Información Óptica ISO 27001:2005, Alberto G. Alexander. Alfaomega. Pág. 41

Para establecer el alcance en la Organización se utilizó el método del Elipse. Esta metodología permite, con gran precisión, poder identificar posteriormente los activos de información y las relaciones con otras dependencias. Aquí solo se abarca el Área Administrativa; ya que nuestro estudio es el Departamento de Sistemas que pertenece a

esta Área, como lo muestra la gráfica, ya que existe otra sede donde solo actúa la sección Académica

La metodología elipse, es un método que permite, dado un determinado alcance de un Sistemas de Gestión de la Seguridad Informática (SGSI), identificar sus interfaces, interdependencia con áreas y procesos, así como averiguar el tipo de memorando de entendimiento que existe o debiera de elaborarse, así como los contratos existentes y los grados de acuerdos necesarios.

Para poder relacionar cada una de las dependencias del Tecnológico Comfenalco, se utilizó la entrevista, en ella se le pregunto a cada jefe de área las relaciones que esta tiene en sus procesos con los procesos del Departamento de Sistemas.

Lo primero que se hiso fue determinar en la elipse concéntrica los distintos procesos y subprocesos que conforman o que está relacionada con el proceso del Departamento de Sistemas, los procesos básicos que la conforman son: Sección de Cartera, Gerencia Administrativa, Servicios Generales. A cada proceso se le identificaron sus respectivos subprocesos. En el segundo paso en la metodología, consiste en identificar en la elipse intermedia las distintas interacciones que los procesos de la elipse concéntrica tienen con otros procesos en la organización, seguidamente, en la elipse externa, se identifica aquellas organizaciones extrínsecas a la empresa que tiene cierto tipo de interacción con los procesos y subprocesos identificados en la elipse concéntrica. Las flechas indican el tipo de interacción, y la direccionalidad que tiene el flujo de información.

La metodología utilizar fue extraída o analizada del libro “Diseño de Un Sistemas de Gestión de Seguridad de Información”[1]

1.7 ANALISIS DE REQUERIMIENTOS

En el Departamento de Sistemas del Tecnológico Comfenalco se ha detectado la necesidad de poseer un enunciado de políticas y controles para la seguridad de la información, que contrarresten amenazas (naturales, humanas, operacionales, sociales, tecnológicas y de instalaciones) y que seguido a esto minimicen los riesgos a los cuales están expuestas los activos de la organización, además, contamos con la colaboración y aprobación del Director del Departamento de Sistemas, donde se ha llegado a la conclusión que es pertinente diseñar un Sistema de Gestión de Seguridad de Información **(SGSI),** que permita minimizar los niveles de riesgos presentes en la utilización de los recursos informáticos, para tener un mayor control sobre los activos que manejan.

[1]Diseño de un sistema de Gestión de Seguridad de Información, Óptica ISO 27001:2005, Alberto G. Alexander. Alfaomega. Pág. 41

1.8 MARCO CONCEPTUAL O DE REFERENCIA

A continuación conoceremos las teorías que dan soporte a la realización del Sistema de Gestión de Seguridad Informática (SGSI) y a los conceptos relacionados con la rama de la ingeniería redes y seguridad informática.

Un **SGSI**, es un sistema de gestión para la seguridad de la información por medio de un diseño lógico documentado, aplicable a los sectores educativos y a las organizaciones de diferentes razones sociales, tiene por misión el establecimiento de políticas y controles cuyos objetivos es la seguridad de la información en el contexto de la organización. Este se basa en un conjunto de documentos y herramientas que demuestran y ayudan a realizar la gestión de la seguridad como es la ISO 27001 y la metodología para el análisis y gestión de riesgo de los sistemas de información **MAGERIT V2**.

A demás este diseño de SGSI contempla ciertos componentes y fases que facilitan el entendimiento y el buen manejo del mismo tales los cuales se describen a continuación.

1.7.1. Componentes y fases del SGSI

- **Definición del ámbito o alcance:** En esta fase es donde se define y se delimita las áreas de aplicabilidad del sistema de gestión.

- **Identificación de Activos de Información**: Esta es la parte donde se puede definir e identificar todo aquello que genera un valor para la organización, todo lo relacionado con los sistemas de información.

- **Tasación de los activos de información:** En esta parte se define cuanto valor representa el activo para la organización teniendo en cuenta los criterios. establecidos tales como confidencialidad, integridad, confidencialidad y autenticidad.

- **Análisis GAP:** Esta fase hace más referencia a la revisión y balance de las falencias que presenta la organización en cuanto a la seguridad y los sistemas de información.

- **Análisis de riesgo:** Etapa donde se valora el impacto y los riesgos de las que está expuesta la organización.

- **Definición de políticas de seguridad:** Componente donde se definen los lineamientos específicos para la gestión y seguridad de la información.

- **Selección de Controles:** Estos controles son mecanismos para establecer las políticas de seguridad.

- **Definición de la documentación:** En esta parte es donde se establecen y se redactan los documentos que apoyaran los controles de seguridad.

1.7.2. ISO/IEC 27001.

Es un estándar internacional que permite realizar a cabalidad un sistema de gestión de seguridad de la información, este estándar se basa en la gestión de riesgos y subministra las pautas necesarias para la implementación de controles y la creación de políticas de seguridad. La ISO/IEC 27001 BS 7799- 2:2005, está orientada a aspectos netamente **10**

organizativos y por tal motivo busca proponer el establecimiento, implementación, operación, monitorización de la gestión de la seguridad de la información.

Esta norma va acompañada de una guía La **BS7799**, que sirve para la auditoria del sistema de gestión de seguridad de la información, está basada en los requisitos que deben ser cubiertos por la organización, y contiene especificaciones para certificar los dominios individuales de seguridad para poder registrarse en esta norma; los dominios de control son 11 y estas contemplados de la siguiente manera.

1. Política de Seguridad.
2. Organización de la información de seguridad.
3. Administración de recursos.
4. Seguridad de los recursos humanos.
5. Seguridad física y del entorno.
6. Administración de las comunicaciones y operaciones.
7. Control de acceso.
8. Adquisición de sistemas de información, desarrollo y mantenimiento.
9. Administración de los incidentes de seguridad.
10. Administración de la continuidad de negocio.
11. Cumplimientos (Legales, de estándares, técnicos y auditorias).

1.7.2.1 Evolución de la Norma ISO/IEC 27001.

La BSI (Institución Británica de estándares) como primera entidad de normalización a nivel mundial ha sido creadora de normas internacionales tales como ISO 9000, 14001, 18001; las cuales les han permitido a las empresas la implantación de diferentes Sistemas de Gestión que le sirven de respaldo y aceptación ante la comunidad internacional.

La norma ISO/IEC 27001 también tiene sus orígenes en la BSI la cual definió la BS 7799 en el año 1995 con el objeto de proporcionar un código o manual de buenas prácticas para la gestión de la seguridad de la información.
La primera parte de la norma (BS 7799-1) es una guía de buenas prácticas, para la que no se establece un esquema de certificación. Es la segunda parte (BS 7799-2) publicada por primera vez en 1998, la que establece los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente. Las dos parte de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000.En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión.

En 2005, con más de 1700 empresas certificadas en BS 7799-2, este esquema se publicó por ISO como estándar ISO 27001, al tiempo se revisó y actualizo ISO17799.

1.7.3. MAGERIT V2.

Es una metodología desarrollada para el análisis y la gestión de riesgos de los sistemas de información, esta proporciona las pautas, las técnicas y los métodos necesarios para auditar sistemas de información que manejan medios electrónicos, informáticos, telemáticos e información mecanizada en sus operaciones; también podemos decir que es una herramienta que nos permitir **identificar las amenazas** a las que se encuentran expuestos dichos activos, estimar la frecuencia de materialización de tales amenazas y valorar el impacto que supondría en nuestra Organización esa materialización.

A continuación haremos una descripción detallada de los pasos con que cuenta nuestra metodología de análisis de riesgo, la cual consideramos el punto central de la definición de una estrategia de seguridad, perfectamente alineada con la visión del departamento de Sistemas dentro de su entorno de operación.

Esta metodología es el resultado de la combinación de diferentes propuestas existentes en la **industria,** y utiliza métodos tanto **cualitativos**, como **cuantitativos**, los primeros permiten agilidad en el proceso y facilidad en la asignación de valores de impacto o riesgo, y los segundos nos permiten la precisión y exactitud, necesarias a la hora de tomar decisiones de tipo financiero, por ejemplo, en el caso de la selección de los controles adecuados, para mitigar un posible evento negativo a la operación y continuidad del negocio.

Mediante este tipo de aproximación el Departamento de Sistemas busca entender los diferentes aspectos que la conforman, tanto en el aspecto tecnológico, como en los procesos críticos, los cuales a su vez, son soportados por las aplicaciones y la infraestructura tecnológica.

Es por eso que tómanos esta metodología, ya que nos ayuda a identificar detalladamente los activos de información y a su vez valorarla, de esta manera podemos demostrar que tan importante se convierta está en el **Departamento de Sistemas**.

La evaluación de riesgos identifica las amenazas, vulnerabilidades y riesgos de la información, sobre la plataforma tecnológica de una organización, con el fin de generar un plan de implementación de los controles que aseguren un ambiente informático seguro, bajo los criterios de disponibilidad, confidencialidad e integridad de la información.

Esta fue creada por el Consejo Superior de Administración Electrónica en Madrid-España,(**CSAE**), órgano del Ministerio de Administraciones Públicas encargado de la preparación, elaboración, desarrollo y aplicación de la política informática del Gobierno Español. La primera versión fue creada el 1997, y la versión dos que es la actual fue diseñada el 20 de junio de 2006 donde está estructurada por tres libros: "Método", "Catálogo de Elementos" y "Guía de Técnicas".

En el campo del Análisis de Riesgos, en España se tiene una referente indiscutible cuando se va a utilizar una metodología a seguir. Ese referente es **MAGERIT** que actualmente goza de una excelente salud y está reconocida por **ENISA** (European Network and Información Security Agency) junto a otras metodologías europeas e internacionales

A continuación se describe brevemente su estructura:

- **Método:** Describe los pasos y las tareas básicas para realizar un proyecto de análisis y gestión de riesgos, y proporciona una serie de aspectos prácticos. Describe la metodología desde tres ángulos:

  - El capítulo 2 describe los pasos para realizar un análisis del estado de riesgo y para gestionar su mitigación. Es una presentación netamente conceptual.
  - El capítulo 3 describe las tareas básicas para realizar un proyecto de análisis y gestión de riesgos, entendiendo que no basta con tener los conceptos claros, sino que es conveniente pautar roles, actividades, hitos y documentación para que la realización del proyecto de análisis y gestión de riesgos esté bajo control en todo momento.
  - El capítulo 4 aplica la metodología al caso del desarrollo de sistemas de información, en el entendimiento que los proyectos de desarrollo de sistemas deben tener en cuenta los riesgos desde el primer momento, tanto los riesgos a que están expuestos, como los riesgos que las propias aplicaciones introducen en el sistema.

- **Catálogo de Elementos:** Ofrece unas pautas y elementos estándar en cuanto a: tipos de activos, dimensiones de valoración de los activos, criterios de valoración de los activos, amenazas típicas sobre los sistemas de información y salvaguardas a considerar para proteger sistemas de información.

Se hostigan dos objetivos:

- Por una parte, facilitar la labor de las personas que acometen el proyecto, en el sentido de ofrecerles elementos estándar a los que puedan adscribirse rápidamente, centrándose en lo específico del sistema objeto del análisis.
- Por otra, homogeneizar los resultados de los análisis, promoviendo una terminología y unos criterios uniformes que permitan comparar e incluso integrar análisis realizados por diferentes equipos.

- **Guía de Técnicas:** Se trata de una guía de consulta que proporciona algunas técnicas que se emplean habitualmente para llevar a cabo proyectos de análisis y gestión de riesgos: técnicas específicas para el análisis de riesgos, análisis mediante tablas, análisis algorítmico, árboles de ataque, técnicas generales, análisis coste-beneficio, diagramas de flujo de datos, diagramas de procesos, técnicas gráficas, planificación de proyectos, sesiones de trabajo (entrevistas, reuniones y presentaciones) y valoración Delphi.

Unos de los aspectos positivos de utilizar e implementar esta metodología es que sus valores son reflejados en valores económicos.

MAGERIT pretende alcanzar los siguientes objetivos:

- “Concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de atajarlos a tiempo”.
- “Ofrecer un método sistemático para analizar tales riesgos”
- “Ayuda a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control”.
- “Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso”.

MAGERIT está estructurado en nueve fases que se pueden implementar a una solución de una SGSI como son:

1. **Planificación:** En esta primera fase se identifican y se definen los objetivos, la pertinencia, los requerimientos y las condiciones necesarias para realizar un proyecto.

2. **Análisis de Riesgo:** En esta fase hace más énfasis en la identificación de todos y cada uno de los activos a tratar en la organización, sus dependencias y las amenazas a las que están expuestos. También se tiene en cuenta el impacto, la degradación y la frecuencia que tienen cada una de estas amenazas en el activo, analizando las salvaguardas existentes pata mitigar este efecto.

3. **Gestión de riesgos:** En esta última fase se buscan los mecanismos y las salvaguardas apropiadas y oportunas para mitigar el impacto y el riesgo de cada una de las amenazas a niveles aceptables a través del diseño de un plan de seguridad.
4. **Modelo de valor:** Caracterización del valor que representan los activos para la Organización así como de las dependencias entre los diferentes activos.

5. **Mapa de riesgos:** Relación de las amenazas a que están expuestos los activos.

6. **Evaluación de salvaguardas.** Evaluación de la eficacia de las salvaguardas existentes en relación al riesgo que afrontan.

7. **Estado de riesgo:** Caracterización de los activos por su riesgo residual; es decir, por lo que puede pasar tomando en consideración las salvaguardas desplegadas.

8. **Informe de insuficiencias:** Ausencia o debilidad de las salvaguardas que aparecen como oportunas para reducir los riesgos sobre el sistema.

9. **Plan de seguridad:** Conjunto de programas de seguridad que permiten materializar las decisiones de gestión de riesgos

1.9. METODOLOGIA

En el diseño del sistema de gestión de seguridad de información, para el Departamento de Sistemas**,** se llevara un procedimiento el cual cubre varias etapas las cuales comienza con el entendimiento de los requerimientos del modelo, en donde se hizo necesario y preciso manejar técnicas de recolección de información como fueron entrevistas al personal encargado de Sistemas y al director del Departamento, los cuales nos abrieron las puertas para que se pudiera desarrollar la investigación plenamente en la institución. Esta parte del proceso se divide en sub-actividades las cuales son:

- **Conocimiento del Departamento de Sistemas:** En este punto, se procede a reconocer la misión y visión, así como las funciones de cada uno de los que laboran en las división, Además de esto se solicitó los manuales de procedimientos en los cuales están redactados las tareas y actividades que debe realizar estrictamente.

- **Identificación de Activos de información:** En esta etapa se pidió el inventario de activo actualizado, con el fin de identificar los activos con que cuenta el Departamento de Sistemas, así como preguntas directas al director y los jefes que de esta sección, Además de esto también se indago acerca de la importancia de cada activo, de que tan indispensable era para la división y la institución si alguno de estos hiciera falta.

- **Valoración de activos de información:** Ya habiendo establecido claramente los activos de información con que cuenta cada división, continuamos con darle valor a cada activo teniendo en cuenta lo parametrizado en Magerit V2, este paso lo que pretende brevemente es darle un valor en cuanto a ciertos criterios tales como disponibilidad, integridad de los datos, confidencialidad de los datos, autenticidad de los usuarios y autenticidad de el origen de los datos, así como también la trazabilidad del servicio y de los datos.

  Para esta valoración se puede tomar cualquier escala de valores pero para ceñirnos a la pauta de Magerit V2, se usó una escala común para todas las dimensiones, teniendo en cuenta que es cualitativa por cada una se tomó un grado del 0 al 10, teniendo en cuenta que 0 es despreciable, 1- 3 bajo, 4-6 medio, 7-9 alto y 10 muy alto, esto para simplificar la tarea a el momento de realizar un análisis de riesgo. En estos puntos está incluida la seguridad de las personas, la información de carácter personal, las obligaciones derivadas de ley, la capacidad para la persecución de delitos, intereses comerciales y económicos, pérdidas financieras y por último la interrupción del servicio.

  La segunda fase tiene por nombre **Determinación de la brecha** en esta etapa lo que se trata de determinar que tanto se tiene implementado en el Departamento de Sistemas, como los son controles y políticas para la seguridad de la información teniendo en cuenta lo parametrizado en la norma ISO 27001, entre los ítem que se comparan están los 11 puntos de políticas de seguridad que son: organización de la seguridad, clasificación y control de activos, seguridad personal, seguridad física y ambiental, gestión de comunicaciones y operaciones, control de accesos, desarrollo, mantenimiento de sistemas, administración de la continuidad del negocio y cumplimiento.

  Para realizar esta etapa tuvimos que implementar una actividad que en los sistemas de seguridad de información se le conoce como análisis GAP, el cual es

una herramienta metodológica que nos permite comparar dos prácticas distintas una de las practicas es aquella que está utilizando en el Departamento de Sistemas y la otra es aquella que establece un estándar que es aceptable mundialmente. El objetivo es saber que le hace falta a una de estas

Luego de haber hecho el análisis Gap completamente procedemos a determinar la brecha lo cual se hizo teniendo como base los porcentajes totales que presento EL departamento en el Checkeo anterior, los cuales dicen que tan cerca se encuentra la empresa con las políticas que deberían estar implementadas.

Un paso muy vital e importante el cual se convierte en otra etapa de nuestro proyecto es el de **análisis y evaluación de riesgo** para efectuar este hay que tener en cuenta los riesgos y amenazas posibles sobre los activos.

Entre las amenazas y riesgos que se pueden evaluar están desastres naturales, de origen industrial, errores y fallos no intencionados y por ultimo ataques intencionados. Al ser capaces de reconocer las posible amenazas tendremos también la capacidad de crear contramedidas para estas, las cuales minimicen y en el mejor de los casos eviten que alguna de estas se lleve a cabo, este punto también es importante.

El siguiente paso se realiza teniendo en cuenta todo lo anteriormente recopilado acerca de los activos de la institución los riesgos y amenazas, este paso se denomina **Cálculo del impacto acumulado,** Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. "Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema" [2]

[2] Consejo Superior de Administración Electrónica, "Magerit V2, Metodología", P. 23.

El impacto acumulado contiene el valor calculado del activo tanto así como el de los que dependen de él, también sujeta las amenazas a que está expuesto. Este se calcula por cada activo, cada amenaza y cada dimensión de valoración. El objetivo de este paso en la metodología es determinar las salvaguardas de que hay que dotar a los medios de trabajo.

De esta manera, las políticas de seguridad en informática emergen como el instrumento para concientizar a sus miembros acerca de la importancia y sensibilidad de la información y servicios críticos, de la superación de las fallas y de las debilidades, de tal forma que permiten a la institución cumplir con su misión.

2. Activos de información

2.1. Definición.

La identificación de activos es tanto una información documental de interés como un criterio de identificación de amenazas potenciales y salvaguardas apropiadas a la naturaleza del activo.

Se denominan activos los recursos del sistema de información o relacionados con éste, necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por su dirección.

El activo esencial es la información que maneja el sistema; o sea los datos. Y alrededor de estos datos se pueden identificar otros activos relevantes:

- **Los servicios** que se pueden prestar gracias a aquellos datos, y los servicios que se necesitan para poder gestionar dichos datos.
- **Datos de información** Elementos de información que, de manera singular o agrupada de alguna forma, representan el conocimiento que se tiene de algo.
- **Las aplicaciones informáticas** *(software)* que permiten manejar los datos.
- **Los equipos informáticos** *(hardware)* y que permiten hospedar datos, aplicaciones y servicios.
- **Los soportes de información** que son dispositivos de almacenamiento de datos.
- **El equipamiento auxiliar** que complementa el material informático.
- **Las redes de comunicaciones** que permiten intercambiar datos.
- **Las personas** que explotan u operan todos los elementos anteriormente citados.

2.2 Clasificación

La relación que sigue se clasifica los activos dentro de una jerarquía, determinado para cada uno un nombre y una breve descripción de las características. Nótese que la pertenencia de un activo a un tipo no es excluyente de su pertenencia a otro tipo; es decir, un activo puede ser simultáneamente de varios activos.

[S] Servicios
Función que satisface una necesidad de los usuarios (del servicio). Para la prestación de un servicio Los servicios aparecen como activos de un análisis de riesgos bien como servicios finales (prestados por la Organización a terceros), bien como servicios instrumentales (donde tanto los usuarios como los medios son propios), bien como servicios contratados (a otra organización que los proporciona con sus propios medios). ➢ **Servicios Internos:** Son los servicios prestados por el Departamentos de Sistemas, para satisfacer las necesidades a las Dependencias de la misma organización. ➢ **Servicios Contratados:** Son los servicios que prestan otras organización (Outsourcing), y que se requiere en la empresa para llevar a feliz término un proceso y cumplir con los objetivos propuestos.

[SI] Servicios Internos

[SI_C_Elec] Servidor de Correo Electrónico **(1)**

[SI_Ftp] Transferencia de Archivos **(2)**

[SI_S_Domino] Servidor de Dominio **(3)**

[SI_S_Arch] Servidor de Archivo **(4)**

[SI_S_Proxy] Servidor Proxy **(5)**

[SI_S_Web] Servidor Web **(6)**

[SC] Servicios Contratados

[SC_Internet] Servicio de Internet **(7)**

[SC_Luz] Energía Empresarial **(8)**

[SC_Agua_Alcan] Servicio de Agua y Alcantarillado **(9)**

[SC_Comuni] Servicio de comunicaciones **(10)**

[SC_Segur] Servicio de seguridad **(11)**

1. Es la aplicación informática que les permite enviar mensajes de correos entre los usuarios internos como externos, con independencia de la red que los usuarios estén utilizando. Cuyo dominio es usuario@tecnologicocomfenalco.edu.co
2. Protocolo de Transferencia de Archivos lo utilizan los usuarios para acceder a los ficheros informáticos situados en el servidor, para llegar a establecer la conexión, la persona tiene que tener una cuenta en el domino de la Organización, con el fin de que esta se pueda “loguear” en el servidor, una vez establecida la conexión, se visualiza la estructura de archivos mediante carpetas, donde se pueden realizar diversas acciones sobre los archivos como descargarlos, subirlos, renombrarlos, borrarlos o modificar los permisos de acceso de cada uno de ellos.
3. Este servicio se encuentra alojado en Windows 2003 Server Standard Edition, el cual se encarga de administrar los diferentes dominios, en el cual todos los usuarios pertenecientes a la red se autentican al solicitar un servicio.
4. Este servicio es él encarga de almacenar y compartir los archivos en la red LAN,

esta se encuentra alojada en Windows 2003 Server Standard Edition, para poder acceder el usuario tiene que estar “logueado” en el servidor.

5. Este servicio es el que permite el acceso a internet a todos los equipos de la organización.
6. Este servicio es donde se tiene montado diferentes aplicación Web, la cual es consultado por los usuarios internos como externos. Este servidor se encuentra alojado en el Sistema operativo Linux Centus 5.0.
7. Es el servicio de Internet Contratado por la empresa TELECOM.
8. El servicio de luz está contratado con la empresa ENERGÍA EMPRESARIAL.
9. Servicio de agua y alcantarillado está firmado con la empresa AGUACAR.
10. Las comunicaciones celulares están concertados con las entidades como son COMCEL y MOVISTAR.
11. Servicio de seguridad es contratada por la empresa VIMARCO.

[D] DATOS / INFORMACIÒN
Elementos de información que, de manera singular o agrupada de alguna forma, representan el conocimiento que se tiene de algo. Para la **Fundación Universitaria Tecnológico Comfenalco** los datos son el corazón que permite a una organización prestar sus servicios. Son en cierto sentido un activo abstracto que será almacenado en equipos o soportes de información (normalmente agrupado en forma de bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos.
➢ **Datos Vitales:** Son esenciales para la supervivencia de la Organización, su carencia o daño afectarían directamente los procesos realizados o la existencia de la Organización. ➢ **Datos de Configuración:** Es la configuración de las aplicaciones realizadas por la organización, código fuente, código fuentes de las mismas. ➢ **Datos de Carácter Personal:** Cualquier información concerniente a personas fiscas identificadas o identificables. Estos datos son regulados por leyes y reglamentos en cuento afectan a las libertades públicas y derechos fundamentales de los trabajadores. ➢ **Datos Interno**: Son aquellos procesos que maneja la organización para distribuir cualquier comunicado. ➢ **Datos Clasificados**: Son los que están sometidos a normatividad de acceso y distribución, son confidencialmente relevantes. (datos secretos, confidenciales, reservado y de difusión limitada.)
[DC] Datos de Configuración **[D_C_Fuente]** Código fuente de las aplicaciones. **(1)** **[D_C_Eje]** Código Ejecutable. **(2)** **[D_C_Apli]** Configuración de las aplicaciones de la Organización. **(3)** **[D_C_Serv]** Configuración de los Servidores. **(4)** **[DP] Datos de Carácter Personal**

[D_Hoja_Per] Hoja de vida de los equipos de cómputos, Servidores **(5)** **[D_Correo]** Correo electrónico **(6)** **[DC] Datos Clasificados** **[D_R]** Datos Reservados **(7)** **[D_C]** Datos Confidencial **(8)** **[D_SC]** Datos sin clasificar **(9)**
1. En esta se encuentra el código fuente de los aplicativos diseñado e implementado en la Fundación Universitaria Tecnológico Comfenalco. 2. En esta se encuentra las aplicaciones desarrolladas por los programadores de la Fundación Universitaria Tecnológico Comfenalco. 3. En esta se encuentra los manuales de instalación y configuración de las aplicaciones. 4. Manual de requerimientos, instalación y configuración de los servidores de la Fundación Universitaria Tecnológico Comfenalco. 5. Aquí se encuentra los datos de los equipos de cómputos, como también los servidores y todos los activos que componen el sistema de comunicación de la fundación. 6. Es el medio de comunicación de manera interna entre los funcionario de la Institución ya sea de forma pública o privada. 7. Es el servicio de la red que ofrece el Tecnológico Comfenalco para difundir alguna información ya sea de manera privada o pública. 8. Las contraseña de los servidores, licencia del software, Backup y contraseña personales, Datos de Administración de página Web, código fuente de la página Web y aplicaciones, Consultas a bases de datos, datos de nómina, prestaciones sociales. 9. En esta se encuentra el cronograma de mantenimiento preventivo y correctivo de los equipos de cómputos y servidores.

[SW] Aplicaciones (Software)
Tareas que han sido Automatizadas por la **Fundación Universitaria tecnológico Comfenalco,** para su mejor desempeño en un equipo informático. Las aplicaciones, analizan y transforma los datos permitiendo la explotación de la información generada en la organización para prestar un buen servicio. En esta clasificación se encuentran los activos con denominaciones concernientes a programas, aplicativos y desarrollos, para las tareas o procesos que han sido automatizadas en la Institución; su desempeño o utilización se realizaran a través de equipos informáticos, en miras a gestionar, analizar y transformar los datos permitiendo la explotación de la información para la prestación de los servicios.
[SW_Pro] Desarrollo propio **[SW_Swap]** Software de administración de proyectos de aulas. **(1)** **[SW_Sedoc]** Softwarede evaluación de docente. **(2)** **[SW_Saepro]** Software de autoevaluación de programas. **(3)** **[SW_Moodle]** Aula Virtual**.** **(4)** **[SW_Credi]** Software para realizar el crédito estudiantil. **(5)** **[SW_Web]** Pagina Web del Tecnológico Comfenalco **(6)** **[SW_Std] Software Estándar** **[SW_Syne]** Synersis **(7)** **[SW_Anti]** Antivirus **(8)** **[SW_SO]** Sistemas Operativos **(9)** **[SW_Office]** Ofimáticas **(10)** **[SW_Browser]** Navegador **(11)** **[SW_Sap]** Nomina **(12)** **[SW_Edpro]** Editores para el diseño y programación **(13)**

[SW_Dbms] Sistemas de gestión de bases de datos **(14)** **[SW_Len_pro]** Lenguaje o plataforma de Programación **(15)** **[SW_email]** Servicio de correos **(16)** **[SW_Backup]** Sistemas de Backup**(17)**	

1. Es el Software de Administración de Proyectos de Aula de la Fundación Universitaria Tecnológica Comfenalco, este Software permite a los estudiante gestionar su proyecto de aula durante todo el semestre y realizar procesos como: inscribir una propuesta, cargar un avance del proyecto, revisar las notas de su proyecto, entre otras; a los docentes les permite realizar un seguimiento de cada proyecto de aula que tiene a su cargo.
2. Es el software que permite realizar las evaluaciones de los docentes de las materias que tiene matriculadas.
3. El Sistema de Autoevaluación de Programas, SAEPRO, permite optimizar la etapa de recolección, procesamiento y generación de resultados del proceso de Autoevaluación, además permite examinar la dinámica de las instituciones educativas o programas académicos mediante la ejecución de una secuencia articulada de actividades que permite detectar sus fortalezas, debilidades, amenazas y oportunidades, con el objetivo de buscar mejoramiento continuo de la calidad de sus procesos.
4. Sistema de administración de aprendizaje para el apoyo de los cursos presenciales de la Institución.
5. Sistemas para diligenciar su crédito estudiantil.
6. Página Web de la **Fundación Universitaria Tecnológico Comfenalco**, desarrollada bajo la tecnología Php y java en el cual se realizan publicaciones sobre las diferentes actividades de formación, culturales y pedagógicas.
7. Sistema de Información Interna de la **Fundación Universitaria Tecnológico Comfenalco**, a través del cual se manejan todos los programas del área académica, financiera y administrativa.
8. Se cuenta con Trend Micro Officescan corporativo que están instalados en todos los equipos de la institución. Su actualización se realiza a través de una consola

automáticamente, la cual es programado por el administrador de la red.

9. Se utiliza el sistema Operativo Windows Xp Professional Service Pack II en todos los equipos informáticos que se encuentra en cada una de las oficinas y en los laboratorios informáticos, aunque hay algunos usuarios que tienen el Windows Vista Home en sus portátiles. Mientras que los servidores DELL tiene Windows 2003 Server Standard Edition y el sistema operativo Linux Centus 5.0

10. Se cuenta con el paquete de Microsoft Office 2007 para el procesamiento de texto y hojas de cálculos, además se cuenta con Adobe Reader 8.0 Microsoft Project 2007 para el montaje de proyectos, Visio 2007, Autocad2000.

11. Se utiliza el Internet Explorer 7.0 y Mozilla Firefox 3.0 como navegador Web en todos los equipos de la **Fundación Universitaria Tecnológico Comfenalco.**

12. SAP, aplicación donde se lleva a cabo la gestión de nómina de la Institución.

13. Se utiliza el paquete de Macromedia 2004 para la programación y diseño de la página, este contiene las aplicaciones de Flash, Dreamweaver, Fireworks, FreeHand entre otras.

14. Utiliza el motor Mysql para las páginas Web y Oracle como dbms (Sistemas de Manejador de Bases de Datos) para las aplicaciones en el cual se manejan todos los programas del área académica, financiera y administrativa, esta se encuentra instalada y configurada en un Servidor DELL corriendo bajo el Sistema Operativo Windows 2003 Server Standard Edition.

15. Se utiliza el lenguaje de programación Java con sus aplicaciones de Java Script y acción Script para el diseño y desarrollo de la página Web.

16. Para este fin se cuenta con su propio servidor de manejador de correspondencia Microsoft Outlook Exchange 2007 y 2003, la cual se encuentra configurados en todas las máquinas de trabajo de la Institución. Este se encuentra alojado en el Sistema Operativo Windows 2003 Server Standard Edition.

17. Los sistemas de Backup con la que cuenta la Fundación Universitaria Tecnológico Comfenalcoes **autobackup mysql from backup,** es un programa para Windows que le permite respaldar los datos automáticamente desde un Servidor de Bases de Datos MySQL en archivos de Texto/SQL/PHP/CSV/XML/HTML o en otras bases de datos MySQL, además esta es programada para que realice las copias en horas que el usuario predetermine. **Export/Import Oracle**, es una utilidad de Oracle para realizar backups lógicos de Oracle (y luego poderlos restaurar).

[HW] Equipos Informáticos (Hardware)	
Bienes materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos.	
[HW_Serv_Web] Servidor Web	**(1)**
[HW_Serv_PV] Servidor PV	**(2)**
[HW_Serv_CC] Servidor Cc	**(3)**
[HW_Serv_Ctgex] Servidor ctgexc	**(4)**
[HW_Serv_ISA] Servidor Isa	**(5)**
[HW_Serv_SP] Servidor Sp	**(6)**
[HW_Serv_DHCP] Servidor Dhcp	**(7)**
[HW_Serv_RC] Servidor Rc	**(8)**
[HW_Serv_Alma] Servidor Alma	**(9)**
[HW_Serv_Syne] Servidor10 Synersis	**(10)**
[HW_Pc] Información Personal	**(11)**
[HW_Mobile] Informática Móvil	**(12)**
[HW_Printer] Medios de Impresióny escáner	**(13)**
[HW_Swith] Conmutadores	**(14)**
[HW_Router] Encaminadores	**(15)**

[HW_Acces_P] Access Point	**(16)**
[HW_Arma] Armarios	**(17)**

1. Marca DELL, Descripción Servidor WEB, referencia PowerEdge R200, procesador Intell Xeon 3000 Conroe 3065,2.33,1333,4M,G0, Memoria Ram DIMM,4G, 2X2G,667 Mhz, Disco Duro de 160GB, Sistema operativo Linux Centos 5,1.
2. Marca DELL, Descripción Plataforma Virtual, referencia PowerEdge 2950, procesador intell xeon 5130 Dual Core 3Ghz, Memoria Ram 4 GB 1024 x 4, 3 Disco Duro de HD,146G,SAS,3,10K,3.5,MXT,GEN, Sistema operativo Linux Centos 5,1.
3. Marca DELL, Descripción Conexiones Cartagena, referencia PowerEdge 2950, procesador intell xeon 5050, Memoria Ram 2 GB 512 x 4, 2 Disco Duro de HD,73G,SAS,3,10K,3.5, Sistema operativo Linux Centos 4,4, Servicios que están corriendo Apache 2.0/Tomcat 5.5.25/PHP 4.3.9/Java 1.5.0_14/Mysql 4.1.20
4. Marca DELL, Descripción EXCHANGE Server, referencia PowerEdge 2950, procesador intell xeon 3GHZ, Memoria Ram 4 GB 1024 x 4, 3 Disco Duro de HD,146G,SAS,3,10K,3.5,MXT,GEN, Sistema operativo Windows 2003 Server, Servicios que están corriendo Echange 2003 Server/PDC y DNS Primario.
5. Marca DELL, Descripción ISA Server 2006, referencia PowerEdge 2950, procesador intell xeon 5110 Dual Core 1,6 Ghz, Memoria Ram 2 GB 512 x 4, 1 Disco Duro de HD,73G,SAS,3,15K,3.5,SGT,15K4, Sistema operativo Windows 2003, Servicios que están corriendo Server, ISA server.
6. Marca DELL, Descripción Portal Institucional (SharePoint), referencia PowerEdge 2950, procesador intell xeon E5310 Quad Core 1,6 Ghz, Memoria Ram 2 GB 512 x 4, 2 Disco Duro de HD,73G,SAS,3,15K,3.5,SGT,15K4, Sistema operativo Windows 2003 Server, Servicios que están corriendo SharePoint /Consola Antivirus.
7. Marca DELL, Descripción Académico Dominio DHCP, referencia PowerEdge 2950, procesador intell xeon E5310 Quad Core 1,6 Ghz, Memoria Ram 2 GB

512 x 4, 1 Disco Duro de HD,73G,SAS,3,15K,3.5,SGT,15K4, Sistema operativo Windows 2003 Server, Servicios que están corriendo Controlador De Dominio/DHCP/DNS.

8. Marca DELL, Descripción Respaldo Exchange, referencia PowerEdge 2950, procesador intell xeon E5310 Quad Core, Memoria Ram 4GB 1024 x 4, 3 Disco Duro de HD,146G,SAS,3,10K,3.5,MXT,GEN.
9. Marca DELL, Descripción Almacenamiento, con referencia PowerVault MD1000, 6 Disco Duro de HD,300G,SAS,10K,3.5, Servicios que ejecuta Copias Synersis/ Dependencias Backup Echange.
10. Marca HP, Descripción Synersis, referencia Proliant ML350 G4, procesador intell xeon 2.4G,512K, Memoria Ram DIMM,1G,266M, 1 Disco Duro de HD 36GB SCSI,U320, Sistema operativo Windows Linux Red hat 9, el Servicios que se están corriendo, software Académico y Financiero SYNERSIS .
11. La **Fundación Universitaria Tecnológico Comfenalco,** cuenta aproximadamente 190 equipos de cómputo para la parte administrativa, los cuales tienen las siguientes característica, disco duro de 40 GB a 160 GB Maxtor, Seagate, Toshiba, Pentium IV de 2.8 GB a Pentium Dual 1,8 Ghz, Unidad de DVD/RW, 1 GB en memoria Ram a 2 GB, Sistema operativo Windows Xp Professional Service Pack II, Microsoft Oficces 2007, Software Académico y Financiero llamado Synersis, Adobe Reader 8.0, el comprensor de archivo 7zip. Para la parte académica se cuenta con 180 equipos de cómputo distribuidos de la siguiente manera, 100 pertenecen a la sede España y 80 a la sede Zaragocilla, estos equipos tienen la siguiente configuración, disco duro de 40 GB a 120 GB, Pentium IV de 2.8 GB a Pentium Dual 1,8 Ghz, Unidad de DVD/RW, 1 GB en memoria Ram a 2 GB, Sistema operativo Windows Xp Professional Service Pack II, Microsoft Oficces 2007 entre otras aplicaciones que se manejan por salas.
12. En el **Tecnológico Comfenalco** cuenta aproximadamente45 computadora portátil, que están asignados a la parte Administrativa, los cuales se utilizan para la gestión de los procesos académicos, financieros, sistemáticos, administrativos y algunas tareas personales; estos equipos tienen las siguiente configuración, CORE DUO 1,4GHZ - DUAL CORE 1,8 GHZ - CORE 2 DUO 1,6 GHZ, memoria

Ram de 2 GB, disco duro de 80 GB – 160 GB, Unidad DVD/RAM, Sistema operativo Windows Xp Professional Service Pack II, Microsoft Oficces 2007, Software Académico y Financiero llamado Synersis, Adobe Reader 8.0, el comprensor de archivo 7zip.

13. Aquí se cuenta aproximadamente8 escáneres Hp para digitalizar los documentos, 35 impresoras de diferentes modelos, entre ellas están las impresoras Láser, de tinta, las Multifuncionales, las cuales están ubicados en diferentes secciones o divisiones de la Institución.

14. En el Tecnológico Comfenalco se cuenta con una gama de Switches, Ciscos Catalyst System 2800, 3com 4050 con número de puertos de 8 hasta 24, Modem Huawey, 1 Panasonic Kx-TDA200 que es la central telefónica Hibrida Análoga/Digital.

15. 1 Router Marca Cisco 2800 Series.

16. En esta se cuenta aproximadamente8 Acces Point 3com 2750 distribuidos en puntos estratégicos de la Universidad y 2 3com 8760.

17. Se cuenta con 2 Almarios Rack de 2 metros x 19", y uno de 1.5 Mt de marca QUEST; en los cuales se encuentra los siguientes tipos de equipos: Switch; Router, Pach Panel, Modem de fibra, Quidway AR 28-09, Rad Fomi-40.

[COM] Redes de Comunicaciones
Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro.
[COM_Pstn] Red Telefónica **(1)** **[COM_Cel]** Red Celular **(2)** **[COM_Micro]** Microondas **(3)** **[COM_Lan]** Red Local **(4)** **[COM_Internet]** Internet **(5)** **[COM_Boqui]** Radios Boquitoqui **(6)**

1. Es la utilizada por la Institución para la comunicación por voz local, el servicio es prestado por Telecom, cuenta con un PBX Panasonic KX-TDA200.
2. Se utiliza dos teléfono celulares para la comunicación entre los funcionarios de la Institución que están por fuera o cuando hay alguna emergencia de comunicación con algún personal Externo, esta servicios es prestada por Comcel y Movistar.
3. Existe una antena microonda D-LINK la cual permite la conexión con la sede de Zaragocilla.
4. A nivel interno el Tecnológico Comfenalco maneja una LAN de cableado estructurado, la cual comunica todas las dependencias administrativas y académicas entre sí, con topología en cascada.
5. Existe una conexión a internet suministrada por Telecom de 4 Megas dedicado, 2 MG en rehúso y Flycom con 2 Megas dedicado, las cuales esta distribuidos para la Red Administrativa y Académica, y otras la tienen configurada para diferentes aplicaciones.
6. Se utiliza 7 radios de comunicación Motorola (boquitoqui) para la comunicación interna, estos radios lo utilizan los técnico de sistemas y el personal de Servicios Generales de la institución.

[SI]Soporte de Información	
Se consideran dispositivos físicos que permiten almacenar información de forma Permanente o, al menos, durante largos periodos de tiempo.	
[SI_ Electro] Sistemas de Información Electrónico	
[SI_Usb] Dispositivos USB	**(1)**
[SI_Cd] Cd-Rom	**(2)**
[SI_Dvd] Dvd	**(3)**
[SI_Tape] Cintas Magnéticas	**(4)**
[SI_Disk] Discos Duros	**(5)**

[Sl_ N_Electro] Sistemas de Información No Electrónico **[Sl_Printed]** Material Impreso **(6)**
1. Se usa para el almacenamiento temporal de la información, estos varían la capacidad de almacenamiento desde 1 Gb a 8 Gb. 2. Se emplea para el almacenamiento permanente de la información del Tecnológico Comfenalco, con capacidad de almacenamiento de 700 Mb de datos. 3. Se emplea para el almacenamiento permanente de la información con capacidad de 4.4 Gb. 4. Disco magnéticos que se utiliza para sacar Backup en el servidor donde está montada las diferentes aplicaciones. 5. Dispositivos de almacenamiento que tiene un rango de 40 Gb. a 200 Gb. De marca Maxtor y Segate. 6. Contiene el material impreso de la Fundación Universitaria Tecnológico Comfenalco que contiene un alto grado de importancia en los procesos que se manejan.

[AUX] Equipamiento Auxiliar
Se consideran otros equipos que sirven de soporte a los sistemas de información, Sin estar directamente relacionados con datos.
[AUX_Ups] Sistema de Alimentación Interrumpida **(1)** **[AUX_Gen]** Generadores Eléctricos **(2)** **[AUX_Ac]** Equipos de Climatización **(3)** **[AUX_Cabling]** Cableado **(4)** **[AUX_Furniture]** Armario **(5)**
1. En la Fundación Universitaria Tecnológico Comfenalco cuenta con 2 Inversores

Xantrex DR Serie Inverter/Charger, las cuales suministra la energía al departamento de sistema en caso de la ausencia del fluido eléctrico. 2. En el Tecnológico Comfenalco cuenta con un respaldo eléctrico autosuficiente que son alimentadas por 4 baterías de automotor MTEK. 3. En el centro de información del tecnológico Comfenalco posee dos Aires acondicionado de los cuales se utiliza uno que suministra todo el cuarto de telecomunicaciones y el otro para la División de Sistemas. 4. Como medio de trasmisión de datos, se utiliza en algunos tramos cableados de fibra óptica y en otros cableado UTP CAT 6 para la conexión de los equipos de las diferentes secciones y divisiones del Tecnológico. 5. Para la fácil administración y organización se los equipos, se cuenta con 2 Almarios Rack de 2 metros x 19", y uno de 1.5 Mt de marca QUEST; en los cuales se encuentra los siguientes tipos de equipos: Switch; Router, Pach Panel, Modem de fibra, Quidway AR 28-09, Rad Fomi-40 y equipos de VozIP. Siendo este el núcleo de la topología física desde el cual se le lleva el servicio a las estaciones de servicios.

[P] Personal	
Aparecen las personas relacionadas con los sistemas de información.	
[P_Ui] Usuariointerno(1)	
[P_Adm] Administrador del Sistemas	**(2)**
[P_Tec] Técnico de Sistemas	**(3)**
[P_Dba] Administrador de bases de datos	**(4)**
[P_Desa] Desarrolladores	**(5)**
[P_C_aca] Coordinador de proyectos	**(6)**
1. Son aquellos que trabajan por mantener día a día la razón social de la Fundación Universitaria tecnológico Comfenalco, como lo son el personal Administrativo; dentro de esto encontramos; Directores de la División, Asistentes, Secretarias, Técnicos de sistemas , Aseadores, Docentes.	

2. Aquella persona que organizan, administran y dan soporte a sistema en general, en el departamento de sistema y tecnología.
3. Son aquellas personas que le dan soporte de Software y Hardware a los equipos de cómputo tanto en la parte Administrativa como Académica de la Fundación Universitaria tecnológico Comfenalco.
4. Es la persona de la división de sistemas, que dentro de sus funciones esta la administración de la bases de datos.
5. Son los encargados del desarrollo, actualización y sostenimiento de la página Web del Tecnológico Comfenalco y aplicaciones. Esto está a cargo de 2 personas de tecnología y sistemas y un coordinador de desarrollo y proyectos.
6. Es el encargado de programar y gestionar todas las actividades de desarrollo de Aplicaciones Académica y Administrativas. Esto está a cargo por el coordinador de desarrollo y proyectos.
7. Es la persona que está encargado de aprobar y apoyar los procesos que se llevan a cabo en el núcleo productivo de los sistemas de información que se desarrollan en el Tecnológico Comfenalco.

2.3. Propietarios de los activos

ACTIVO DE INFORMACIÒN	PROPIETARIOS	RESPONSABLE
Servidor de Correo Electrónico	Tecnológico Comfenalco	Leandro Pájaro
Servidor de Dominio	Tecnológico Comfenalco	Leandro Pájaro
Servidor de Archivo	Tecnológico Comfenalco	Leandro Pájaro
Servicio de Internet	Telecom, Flycom	Juan Harold Silva
Servicio de Energía	Energía Empresarial	Luis meza
Servicio de Agua y Alcantarillado	Aguacar	Luis meza
Código fuente de las aplicaciones	Tecnológico Comfenalco	Julio Orozco Mattos
Código Ejecutable	Tecnológico Comfenalco	Julio Orozco Mattos
Configuración de las aplicaciones de la Organización.	División de Sistemas	Juan Harold Silva
Configuración de los Servidores.	División de Sistemas	Juan Harold Silva
Datos Reservados / Contraseña de los Servidores	División de Sistemas	Juan Harold, Leandro Pájaro
Servidor Synersis	Tecnológico Comfenalco	Leandro pájaro
Antivirus	Tecnológico Comfenalco	Leandro Pájaro
Sistemas Operativos	Tecnológico Comfenalco	Leandro Pájaro
Ofimáticas	Tecnológico Comfenalco	Leandro Pájaro
Servidor de Nomina	Tecnológico Comfenalco	Juan Harold Silva
Sistemas de gestión de bases de datos	Tecnológico Comfenalco	Leandro Pájaro, Juan Harold Silva
Servicios de correos Electrónico	Tecnológico Comfenalco	Juan Harold Silva
Sistemas de Backup	Tecnológico Comfenalco	Juan Silva, Julio Orozco
Servidor WEB	Tecnológico Comfenalco	Leandro pájaro

Servidor Conexiones Cartagena	Tecnológico Comfenalco	Leandro pájaro	
Servidor ctgexc	Tecnológico Comfenalco	Leandro pájaro	
Servidor Isa Server	Tecnológico Comfenalco	Leandro pájaro	
Servidor Portal Institucional (SharePoint)	Tecnológico Comfenalco	Leandro pájaro	
Servidor Dhcp	Tecnológico Comfenalco	Leandro pájaro	
Servidor Respaldo Exchange	Tecnológico Comfenalco	Leandro pájaro	
Servidor Almacenamiento	Tecnológico Comfenalco	Leandro pájaro	
Servidor Synersis	Tecnológico Comfenalco	Leandro pájaro	
Conmutadores	Tecnológico Comfenalco	Juan Harold Silva	
Encaminadores	Tecnológico Comfenalco	Leandro Pájaro	
Access Point	Tecnológico Comfenalco	Leandro Pájaro	
Armarios	Tecnológico Comfenalco	Leandro pájaro	
Red Telefónica	Tecnológico Comfenalco	Leandro pájaro	
Microondas	Tecnológico Comfenalco	Leandro pájaro	
Red Local	Tecnológico Comfenalco	Leandro pájaro	
Radios Boquitoqui	Tecnológico Comfenalco	Leandro Pájaro	
Sistema de Alimentación Interrumpida	Tecnológico Comfenalco	Luis Meza	
Generadores Eléctricos	Tecnológico Comfenalco	Luis Meza	
Cableado	Tecnológico Comfenalco	División de Sistemas	
Archivos datos Informático	Tecnológico Comfenalco	Juan Harold Silva	
Servicio de Internet Inalámbrico	División de Sistemas	Juan Harold Silva	
Servicio Técnico	División de Sistemas	Técnicos de Sistema	
Servicio de Backup	División de sistemas	Juan Silva, Julio Orozco	

Hostin	Telecom	Juan Harold Silva
Armario, Rack	Tecnológico Comfenalco	Leandro Pájaro
Cableado de datos	Tecnológico Comfenalco	Leandro Pájaro
Equipo de Climatización	Tecnológico Comfenalco	Luis Meza
Sistemas de Alimentación Interrumpida	Tecnológico Comfenalco	Leandro Pájaro
Aplicaciones	Tecnológico Comfenalco	Justo Sarabia Agamez

2.4. Criterios de valoración

Valoración De Los Activos

Son las características o atributo que hacen valioso un activo. Estos se valoran por medios de dimensiones o facetas de un activo (Disponibilidad, integridad, confidencialidad y autenticidad), independiente de otras facetas. Estas se utilizan para valorar las consecuencias de la materialización de una amenaza. La valoración que recibe un activo en cierta dimensión en la medida del perjuicio para la organización si el activo se ve dañado en dicha dimisión.

Relación De Dimensiones

[D] Disponibilidad
Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran la información y sus activos asociados.
¿Qué importancia tendría que el activo no estuviera disponible para la **Fundación Universitaria Tecnológico Comfenalco**?
➢ Un activo tiene un gran valor desde el punto de vista de disponibilidad si una amenaza afectara a su disponibilidad, las consecuencias serían graves. ➢ Un activo carece de un valor apreciable desde el punto de vista de disponibilidad cuando puede no estar disponible frecuentemente y durante largos periodo de tiempo sin por ellos causar mayor daño. ➢ La disponibilidad es una característica que afecta a todo tipo de activos. ➢ A menudo la disponibilidad requiere un tratamiento por escalones pues el coste

de la indisponibilidad aumenta de forma no lineal con la duración de la interrupción, desde breves interrupciones sin importancia, pasando por interrupciones que causan daños considerables y llegando a interrupciones que no admiten recuperación: la organización está acabada.

[I] Integridad
Garantía de la exactitud y completitud de la información y los métodos de su procesamiento.
¿Qué importancia tendría que los datos fueran modificados fuera de control?
➢ Los datos reciben una alta valoración desde el punto de vista de integridad cuando su alteración, voluntaria o intencionada, causaría graves daños a la organización. ➢ los datos carecen de un valor apreciable desde el punto de vista de integridad cuando su alteración no supone preocupación alguna.

[C] Confidencialidad de los datos
Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.
¿Qué importancia tendría que el dato fuera conocido por personas no autorizadas?
➢ Los datos reciben una alta valoración desde el punto de vista de confidencialidad cuando su revelación causaría graves daños a la organización. ➢ Los datos carecen de un valor apreciable desde el punto de vista de confidencialidad cuando su conocimiento por cualquiera no supone preocupación

alguna.

[A_S] Autenticidad de los usuarios del servicio
Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.
Aseguramiento de la identidad u origen.
¿Qué importancia tendría que quien accede al servicio no sea realmente quien se cree?
La autenticidad de los usuarios de un servicio es lo contrario de la oportunidad de fraude o uso no autorizado de un servicio. ➢ Un servicio recibe una elevada valoración desde el punto de vista de autenticidad cuando su prestación a falsos usuarios supondría un grave perjuicio para la **Fundación Universitaria Tecnológico Comfenalco**. ➢ Un servicio carece de un valor apreciable desde el punto de vista de autenticidad cuando su acceso por cualquiera no supone preocupación alguna.

[A_D] Autenticidad del origen de los datos
Aseguramiento de la identidad u origen.
¿Qué importancia tendría que los datos no fueran realmente imputables a quien se cree?
➢ Los datos reciben una elevada valoración desde el punto de vista de autenticidad del origen cuando un defecto de imputación causaría graves quebrantos a la organización. Típicamente, se habilita la oportunidad de repudio. ➢ Los datos carecen de un valor apreciable desde el punto de vista de autenticidad del origen cuando ignorar la fuente es irrelevante.

Criterios De Valoración

La valorización de los activos se realiza en forma cualitativa, respondiendo a criterios subjetivos. Se ha elegido una escala detallada de diez valores, tomando el valor 0 como determinante de lo que sería in valor despreciable a efectos de riesgo y 10 como valor muy alto.

VALOR		CRITERIO
10	Muy alto	Daño muy grave a la organización
7 – 9	Alto	Daño grave a la organización
4 – 6	Medio	Daño importante a la organización
1 – 3	Bajo	Daño menor a la organización
0	Despreciable	Irrelevante a efectos prácticos

La tabla siguiente pretende guiar con más detalle de forma homogénea los activos cuyo valor es importante por diferentes motivos, habiéndose tomado en consideración los siguientes:

- ✓ Seguridad de las personas
- ✓ Información de carácter personal
- ✓ Obligaciones derivadas de la ley, del marco regulatorio, de contratos, etc.
- ✓ Capacidad para la persecución de delitos
- ✓ Intereses comerciales y económicos
- ✓ Pérdidas financieras
- ✓ Interrupción del servicio
- ✓ Orden público
- ✓ Política corporativa
- ✓ Otros valores intangibles

Lo más normal es que un activo reciba una simple valoración en cada dimensión en la que es valioso. Este planteamiento puede y debe ser enriquecido en el caso de dimensiones más complejas como es el caso de la disponibilidad, en la que las consecuencias varían dependiendo del tiempo que dure la interrupción. En estos casos, la dimensión no recibe una única calificación, sino tantas como escalones se hayan considerado relevantes.

2.5. Valoración

	DIMENSIÓN DE VALOR DE SEGURIDAD				
ACTIVO	***[D]***	***[I]***	***[C]***	***[A_S]***	***[A_D]***
[SI_C_Elec] Servicio de Correo Electrónico	**[3]**[3]	**[7]**[11]	**[10]**[2]	**[6]**[1]	**[10]**[1]
[SI_S_Domino] Servidor de Dominio	**[1]**[1]			**[10]**[2]	
[SI_S_Arch] Servidor de Archivo	**[5]**[4]	**[9]**[8]	**[10]**[2]	**[10]**[3]	
[SI_S_Proxy] Servidor Proxy	**[9]**[1]				
[SI_S_Web] Servidor Web	**[9]**[1]	**[7]**[11]	**[10]**[2]	**[6]**[1]	
[SC_Internet] Servicio de Internet	**[9]**[1]			**[7]**[2]	**[6]**[1]
[SC_Luz] Energía Empresarial	**[9]**[1]				
[SC_Comuni] Servicio de comunicaciones	**[7]**[1]				
[SC_Segur] Servicio de seguridad	**[9]**[4]				
[D_C_Fuente] Código fuente de las aplicaciones.	**[9]**[4]	**[7]**[5]	**[9]**[12]		
[D_C_Eje] Código Ejecutable.	**[9]**[4]	**[7]**[5]	**[9]**[12]		
[D_C_Apli] Aplicaciones de la Organización	**[9]**[4]	**[7]**[5]	**[9]**[12]		
[D_C_Serv] Configuración de los Servidores.	**[9]**[1]	**[9]**[1]	**[9]**[6]		**[9]**[6]
[D_Correo] Correo electrónico	**[5]**[1]			**[7]**[8]	**[3]**[1]
[D_R] Datos Reservados		**[10]**[3]	**[7]**[8]	**[7]**[1]	**[7]**[8]
[D_C] Datos Confidencial	**[7]**[1]	**[7]**[1]	**[7]**[11]	**[9]**[1]	**[7]**[11]

[D_SC] Datos sin clasificar		**[5][10]**	**[5][10]**	**[5][10]**	
[SW_Swap] Administración de proyectos de aulas	**[9][1]**	**[9][1]**	**[9][1]**	**[9][1]**	**[9][6]**
[SW_Sedoc] Softwarede evaluación de docente.	**[9][1]**	**[9][1]**	**[9][1]**	**[9][1]**	**[9][6]**
[SW_Saepro] Autoevaluación de programas.	**[9][1]**	**[9][1]**	**[9][1]**	**[9][1]**	**[9][6]**
[SW_Moodle] Aula Virtual**.**	**[9][1]**	**[9][1]**	**[9][1]**	**[9][1]**	**[9][6]**
[SW_Web] Web del Tecnológico Comfenalco	**[9][1]**			**[6][1]**	
[SW_Anti] Antivirus	**[3][1]**			**[7][5]**	
[SW_SO] Sistemas Operativos	**[7][1]**	**[7][1]**	**[7][1]**	**[7][1]**	
[SW_Office] Ofimáticas	**[7][1]**			**[7][1]**	
[SW_Browser] Navegador	**[7][1]**			**[7][5]**	
[SW_Sap] Nomina	**[9][1]**	**[9][5]**	**[9][1]**	**[9][1]**	**[3][6.3]**
[SW_Edpro] Editores de diseño y programación	**[3][1]**			**[7][5]**	
[SW_Dbms] Sistemas gestión de bases de datos	**[10][1]**	**[10][3]**	**[9][5]**	**[9][8]**	**[7][11]**
[SW_Len_pro] Plataforma de Programación	**[3][1]**			**[7][5]**	
[SW_email] Servicio de correos	**[3][1]**			**[7][5]**	
[SW_Backup] Sistemas de Backup	**[7][1]**	**[9][12]**	**[3][1]**	**[4][1]**	
[HW_Serv_PV] Servidor PV	**[9][1]**	**[9][12]**	**[3][1]**	**[4][1]**	
[HW_Serv_CC] Servidor Cc	**[9][1]**	**[9][12]**	**[3][1]**	**[4][1]**	
[HW_Serv_Ctgex] Servidor ctgexc	**[9][1]**	**[9][12]**	**[3][1]**	**[7][1]**	
[HW_Serv_ISA] Servidor Isa	**[9][1]**	**[9][12]**	**[3][1]**	**[4][1]**	
[HW_Serv_PV] Servidor PV	**[9][1]**	**[9][12]**	**[3][1]**	**[4][1]**	
[HW_Serv_SP] Servidor Sp	**[9][1]**	**[9][12]**	**[3][1]**	**[4][1]**	
[HW_Serv_DHCP] Servidor Dhcp	**[9][1]**	**[9][12]**	**[3][1]**	**[4][1]**	
[HW_Serv_RC] Servidor Rc	**[9][1]**	**[9][12]**	**[3][1]**	**[4][1]**	
[HW_Serv_Alma] Servidor Almacenamiento	**[9][1]**	**[9][12]**	**[3][1]**	**[4][1]**	
[HW_Serv_Syne]Servidor Synersis	**[9][1]**	**[9][12]**	**[3][1]**	**[7][1]**	
[HW_Printer] Medios de Impresióny escáner	**[2][3]**				

[HW_Acces_P] Access Point	**[7][1]**				
[HW_Arma] Armarios	**[1][5]**				
[HW_Swith] Conmutadores	**[5][1]**				
[HW_Router] Encaminadores	**[7][1]**				
[COM_Pstn] Red Telefónica	**[5][1]**				
[COM_Cel] Red Celular	**[5][1]**				
[COM_Micro] Microondas	**[9][1]**				
[COM_Lan] Red Local	**[9][1]**				
[COM_Internet] Internet	**[7][1]**				
[COM_Boqui] Radios Boquitoqui	**[5][1]**				
[SI_Usb] Dispositivos USB	**[7][6]**				
[SI_Cd] Cd-Rom	**[7][8]**				
[SI_Dvd] Dvd	**[7][6]**				
[SI_Tape] Cintas Magnéticas	**[7][8]**				
[SI_Disk] Discos Duros	**[7][8]**				
[SI_Printed] Material Impreso	**[7][6]**		**[9][12]**	**[6][1]**	
[AUX_Ups] Sistema de Alimentación Interrumpida	**[9][1]**				
[AUX_Gen] Generadores Eléctricos	**[8][1]**				
[AUX_Ac] Equipos de Climatización	**[5][1]**				
[AUX_Cabling] Cableado	**[7][1]**				
[AUX_Furniture] Armario	**[1][5]**				
[P_Adm] Administrador del Sistemas	**[9][1]**				
[P_Tec] Técnico de Sistemas	**[7][1]**			**[1][1]**	
[P_Dba] Administrador de bases de datos	**[9][1]**			**[9][5]**	
[P_Desa] Desarrolladores	**[3][1]**				
[P_C_aca] Coordinador de proyectos	**[3][1]**				

3. Análisis GAP

3.1 Definición

Consiste en examinar el desempeño de una organización con respecto a las mejores prácticas, estándares y regulaciones legales, evaluar la desviación y establecer los planes para dirigir la organización hacia el cumplimiento de las mismas. Los resultados obtenidos representan el grado en el que una empresa ha cumplido sus objetivos comparativos y otras valoraciones. Una vez entendida la expectativa general de gestión en el sector, es posible compararla con el nivel de rendimiento actual de la compañía. Esta comparación es el análisis Gap. Dicho análisis puede ser realizado a un nivel estratégico u operacional en una estructura.

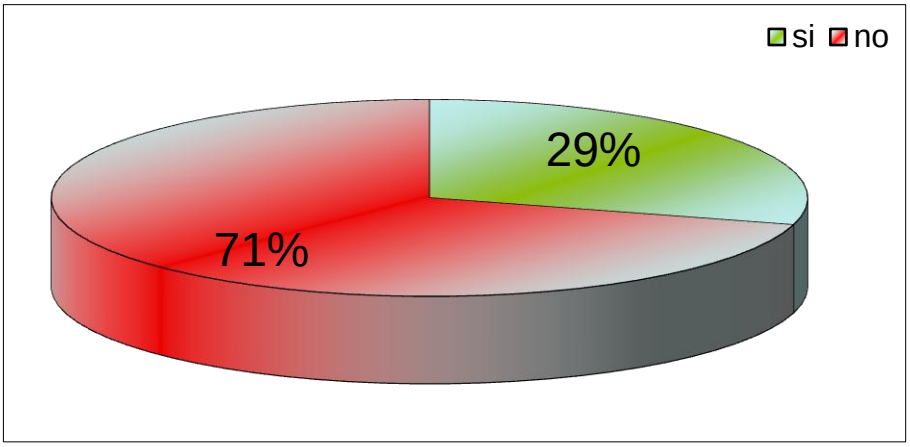
Esta fase, hace referencia a la revisión y balance de las falencias que presenta la organización en cuanto a los procesos de seguridad con los lineamientos de la norma ISO 27001 que estableces en que área o procesos debe priorizar y enfocar esfuerzo para incrementar la seguridad sobre la información.

Para obtener esta información se diseñó una estructura en Excel donde se encuentra los 11 dominios de la norma ISO 27001, donde cada uno de los dominios se encuéntralos lineamientos de buenas prácticas que debe tener toda Organización. "Ver Anexo # 1"

Esta lista de que chequeo, que la podemos llamar a si, fue respondida por el Director del Departamento de Sistemas de la Fundación Universitaria Tecnológico Comfenalco, el Ingeniero Justo Sarabia Agamez en su oficina de trabajo siendo las 4:15 pm del 30 de agosto del presente año. Todas la graficas que se muestran a continuación fueron generadas automáticamente a medidas que el director finalizaba cada unidad de la norma ISO 27001, para mejor entendimiento se extrajo cada una de ellas y se describió de acuerdo al estudio que se realizó de esta misma.

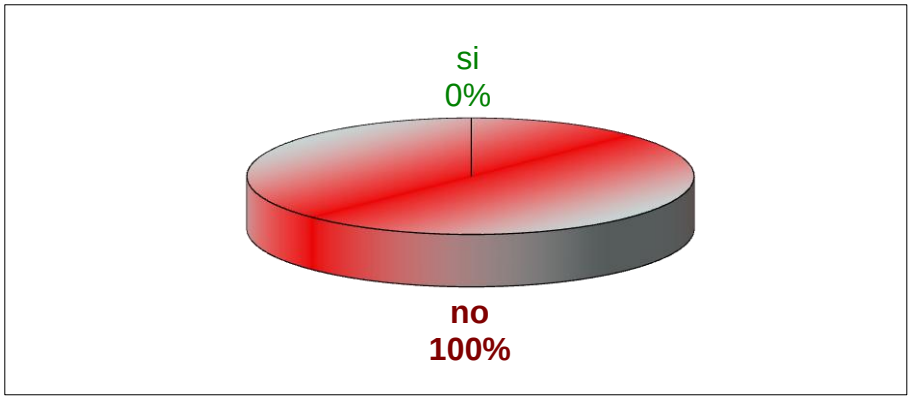
AUTODIASNOSTICO ISO 27001	PUNTAJE	
	SI	NO
1. Políticas de seguridad	0%	100%
2. Organización de la Seguridad	25%	75%
3. Administración de activos	16,67%	83,33%
4. Seguridad de los RRHH	11,11%	88,89%
5. Seguridad física y del ambiente	63,64%	36,36%
6. Gestión de la comunicaciones y operaciones	25%	75%
7. Control de acceso	12,50%	87,50%
8. Desarrollo y mantenimiento de los sistemas	12,50%	87,50%
9. Administración de incidentes	60%	40%
10. Gestión de la continuidad del negocio	0%	100%
11. Cumplimiento	0%	100%
Complimiento general alcanzado por la norma ISO 27001	29%	71%

Resultado General del Diagnóstico



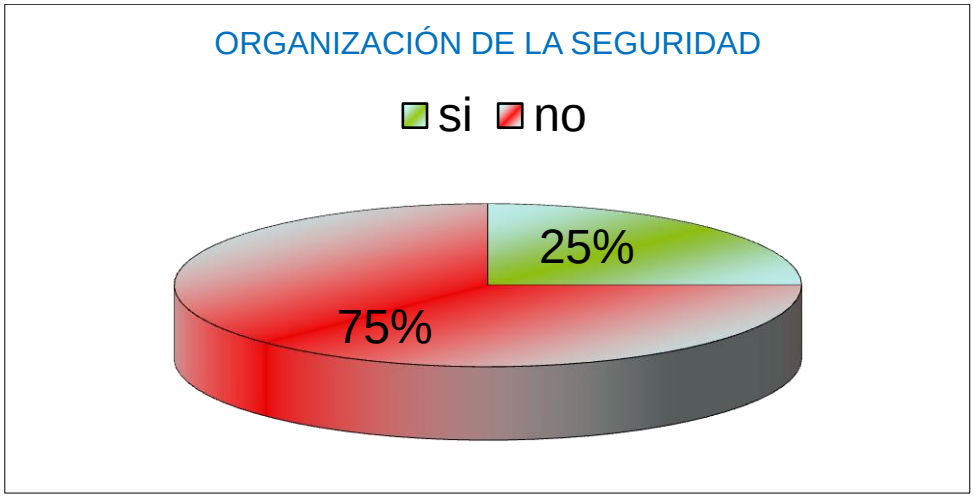
Resultado del Diagnóstico por dominio

1. **Políticas de Seguridad**



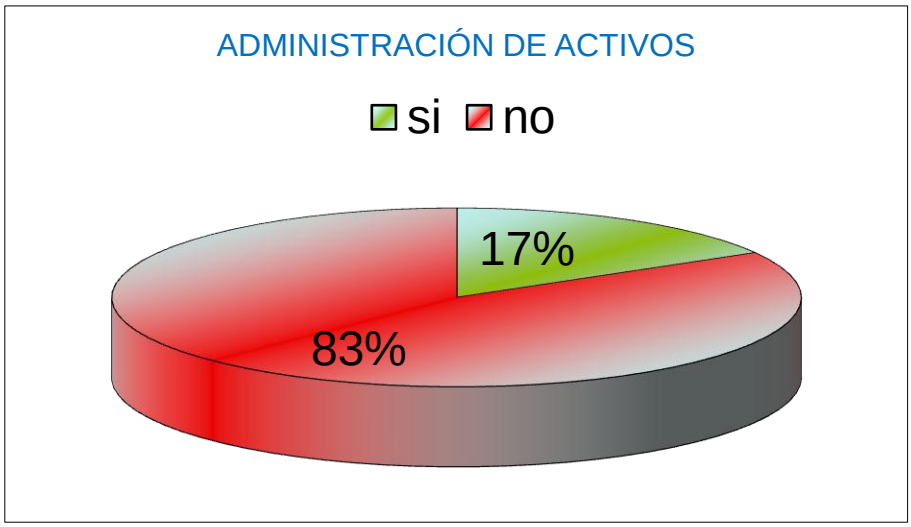
En cuanto al punto de **Políticas de Seguridad** se obtuvo como respuesta que la gerencia no tiene aprobado y publicado un documento que contiene las políticas de seguridad, así como tampoco hay un responsable de las mismas, además de lo anterior la institución carece de un mecanismo de comunicación para los usuarios acerca de las normas.

2. Organización de la Seguridad



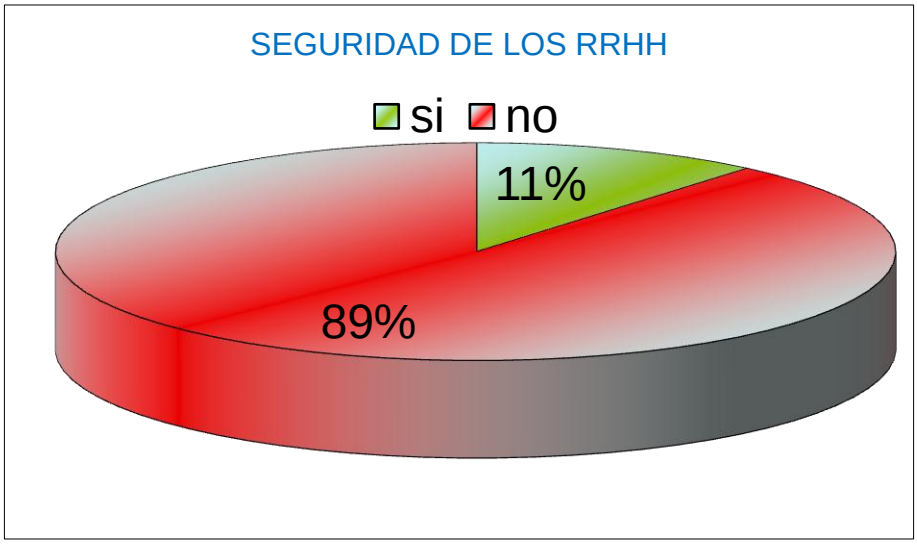
La **Organización de La Seguridad:** entre los roles que se tiene en este nivel solo se cuenta con un responsable de la adquisición o cambio de los sistemas de información, y también se cuenta con la participación de la dirección y las áreas organizativas para los temas de seguridad de información. Como aspectos faltantes obtuvimos que en el ámbito de la organización de la seguridad no se ha establecido los roles necesarios para delegar responsabilidades a las personas que están implicadas en el tema de seguridad, teniendo como consecuencia, el desconocimiento de los procedimientos a seguir, a quien se debe acudir o que hacer para contrarrestar el incidente que esté sucediendo, así como tampoco no hay condiciones contractuales de seguridad con terceros o outsourcing , hacen falta criterios de seguridad en el manejo que hacen estas terceras partes, también se encontró que no existen programas para la formación en seguridad para los clientes usuarios, en cuanto al acuerdo de confidencialidad de la información, el momento es nulo no existe alguno, así como tampoco no hay una supervisión externa de alguna empresa que revise la organización de la seguridad, además que no se tiene documentación, sobre los procedimientos que se deben seguir, cuando un incidente puede afectar el desarrollo normal de los procesos que se llevan a cabo.

3. Administración de activos



En cuanto a la **Administración de Activos** vemos que se tiene un inventario de activos actualizado, pero este inventario no contiene activos de datos, software, equipos y servicios, no existen procedimientos adecuados para el rotulado y manejo de la información, según sea el esquema de la clasificación adoptado por la organización, como tampoco está clasificada la información según su grado de criticidad que esta representa. Además no se tiene definido un responsable del activo de la información. En general se observa que los activos no están correctamente administrados.

4. Seguridad de los RRHH



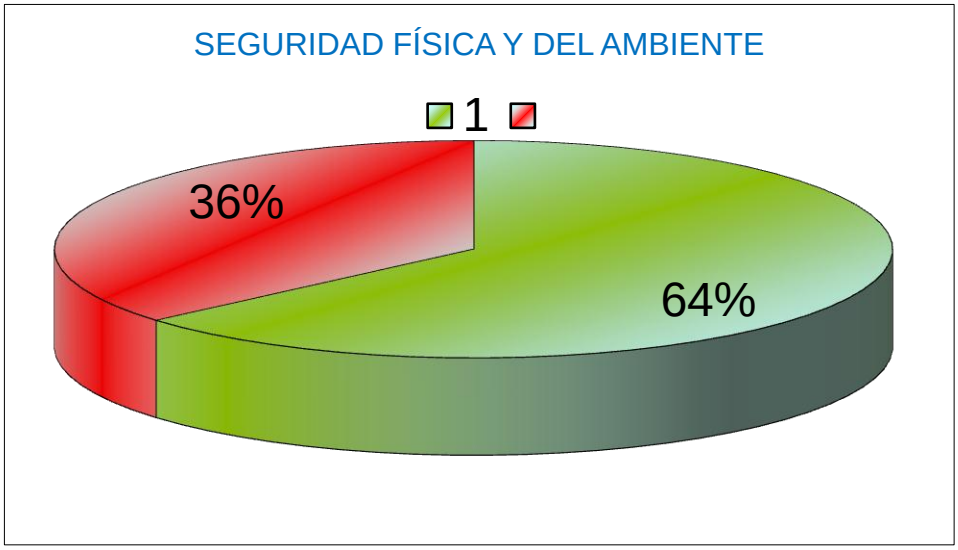
El Objetivo principal de este punto es asegurar a los empleados, contratistas y usuarios de terceros entiendan sus responsabilidades y sean adecuados para las funciones en las que se les han considerado, así como reducir el riesgo de robo, estafa o mal uso de las instalaciones.

En la institución se trabaja en funciones y responsabilidades en materia de roles en seguridad. Se aconseja que se deben llevar a cabo controles de verificación del personal permanente en el momento en que se solicita el puesto, como deficiencia en este apartado se halló queno están plasmada las condiciones de confidencialidad y responsabilidad de la seguridad de la información, los empleados no reciben información acerca de tratamiento de activos y seguridad de los mismos.

También se encontró que hace falta un canal y procedimientos claros en caso de incidentes de seguridad, otro eslabón que hace falta por implementar son losresúmenes de incidentes, además carece de un medio ni hay informes de parte de los usuarios de las vulnerabilidades observadas o sospechosas, ni tampoco se les informa a los usuarios que

no deben probar estas vulnerabilidades u otras encontradas, hace falta un proceso disciplinario de la seguridad de la información.

5. Seguridad física y del ambiente

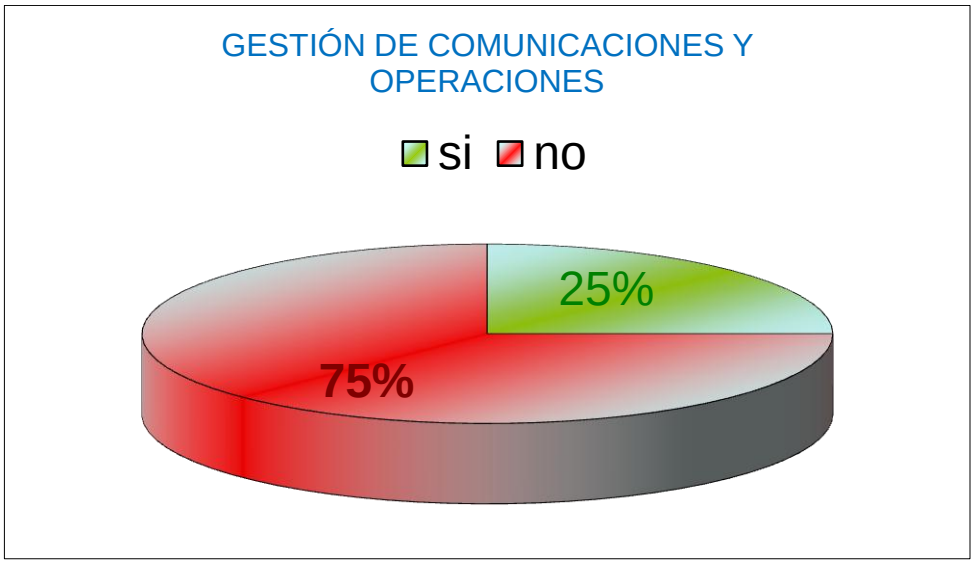


El punto de La **Seguridad Física Y Ambiental** tiene como objetivo impedir el acceso físico no autorizado, daños e interferencias en los locales y la información de la organización.

En la institución se tienen establecidos los parámetros de seguridad física(**ver anexo fotos**)**,** también hay controles para la entrada del personal para protegerse de personal no autorizado, se tiene claro que las áreas seguras deben estar aisladas de eventos naturales, así como las áreas de cargue y descargue de mercancía debe estar alejada de las zonas donde se maneja la información, entre otros se tiene protección ante fallos de alimentación eléctrica(**ver anexo fotos**) y los equipos se tiene ubicados de tal manera que se minimice el riesgo de acceso no autorizado. No existe ninguna clase de seguridad

en el cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información ya que podría haber intercepciones o daños, el equipamiento debe mantenerse en forma adecuada para asegurar que su disponibilidad e integridad sean permanentes, por otra parte los equipos no están asegurados en materia de disponibilidad e integridad, lo cual hace que este sea un punto en el cual la institución pueda tambalear a el momento de que los usuarios necesiten hacer uso de estos.

6. Gestión de la comunicaciones y operaciones

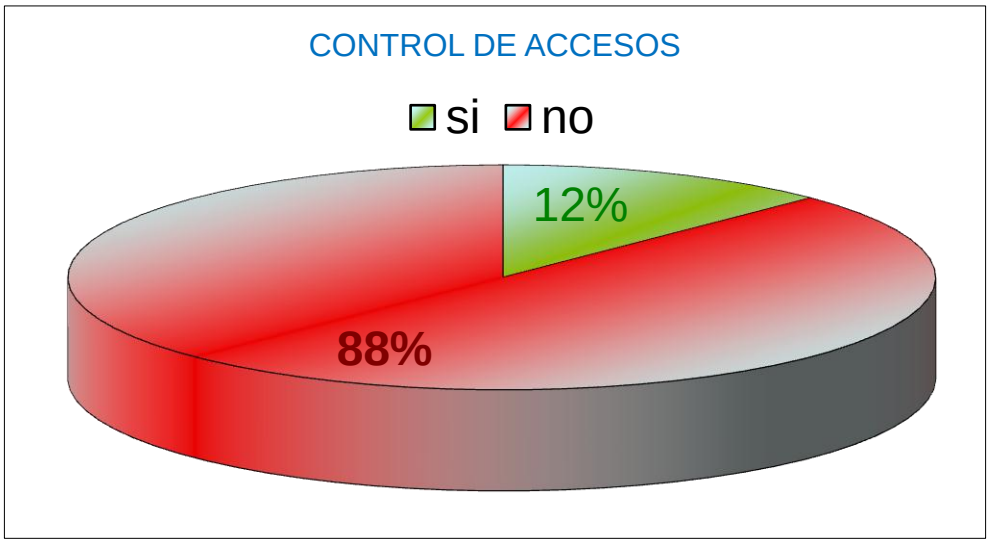


En cuanto a la **gestión de la comunicación y operaciones,** se ha detectado que no existen políticas que permita tener seguridad en la documentación de los sistemas informáticos, como también no se tiene establecido los procedimientos para el manejo de accidente que permita garantizar una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad, no se tienen definido ni documentado las reglas para las transferencias de software desde el estado de desarrollo hacia el estado operativo, no existe ningún plan donde se debe estar monitoreando las demandas de capacidad

de los sistemas informáticos y donde se pueda realizar proyecciones de los futuros requerimientos de capacidad, a fin de garantizar la disponibilidad adecuada, además, se deben establecer criterios de aprobación para nuevos sistemas de información, actualizaciones de la nuevas versiones, y se deben llevar a cabo adecuadas pruebas de los sistemas antes de su aprobación. Hace falta tener implementado controles de detección y prevención para la protección contra el software malicioso así como tampoco procedimientos adecuados de concientización de usuarios, poniendo en riesgo la información, para llegar más a cabo tampoco se tiene establecido ningún conjunto de controles donde se pueda lograr y mantener la seguridad de las redes informáticas. No existe ningún control ni procedimientos para la administración de los medios informáticos, cuando ya estos no son requeridos, los medios informáticos deben eliminarse de manera segura, caso contrario esa información almacenada puede ser filtrado por personas ajenas a la organización.

Como otros faltantes se puede agregar que no se tienen establecidos ningún procedimiento detallado para el manejo y almacenamiento de la información para protegerla contra su uso inadecuado o divulgación no autorizada. No se tiene establecido ningún procedimiento ni estándar para proteger la información y los medios de intercambio en la organización. También vemos que existe falencia con el comercio electrónico, ya que no se tiene implementado políticas ni lineamientos para controlar las actividades de la organización y riesgos de seguridad relacionados con los sistemas electrónicos de oficinas, ya que estas se deben aplicar controles para protegerlo de dichas amenazas, como sabemos el comercio electrónico es unos de los medios más vulnerable y que está expuesto a diversas amenazas relativas a las redes, donde se puede tener como resultados actividades fraudulentas, disputas contractuales y divulgación o modificación a la información, donde constantemente se debe estar monitoreando las actividades relacionados con la seguridad.

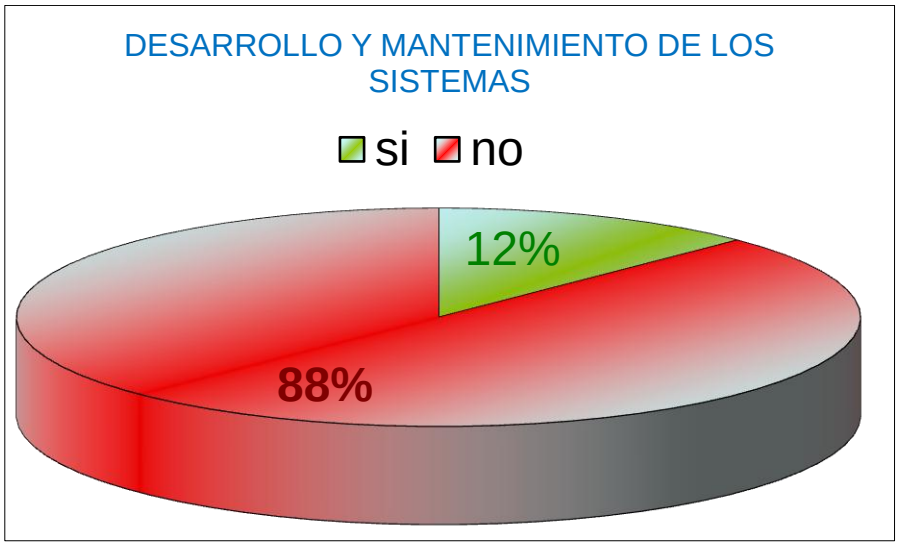
7. **Control de acceso**



No se tiene definidos ni documentados lo requerimientos de negocio para el control de acceso, asignación de derechos, limitaciones y el uso de privilegios a los sistemas de información, para cada usuario o grupo de usuarios. No sea configurado ni documentado los eventos de cuando un equipo de cómputo se encuentra desatendido por un periodo de tiempo, estos están protegido para evitar acceso a personas no autorizadas, como tampoco no se tiene controlado el acceso a los servicios de red tanto internos como externos, esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a los servicios de red no comprometan la seguridad de los servicios que ofrece la organización, ya que las conexiones no seguras a los servicios de red pueden afectar todo el proceso. No existe autenticación con conexiones externas o accesos por los puertos de diagnósticos se puede agregar a esto que tampoco tienen establecidos Identificadores Únicos a todos los usuarios, incluyendo a todo el personal de soporte técnico como (los operadores, Administradores de red, programadores de sistemas, Administradores de bases de datos). Tampoco se tiene establecido una política formal que tome en cuenta los

riesgos que implica trabajar con herramientas informáticas móviles, en particular en ambientes no protegidas, dicha política debe incluir los requerimientos de protección física, controles de acceso, técnicas de criptográficas, protección contra virus, resguardos; también se debe incluir reglas y asesoramiento en materia de conexión de dispositivos móviles a redes y orientación sobre uso de estos dispositivos en lugares públicos.

8. **Desarrollo y mantenimiento de los sistemas**

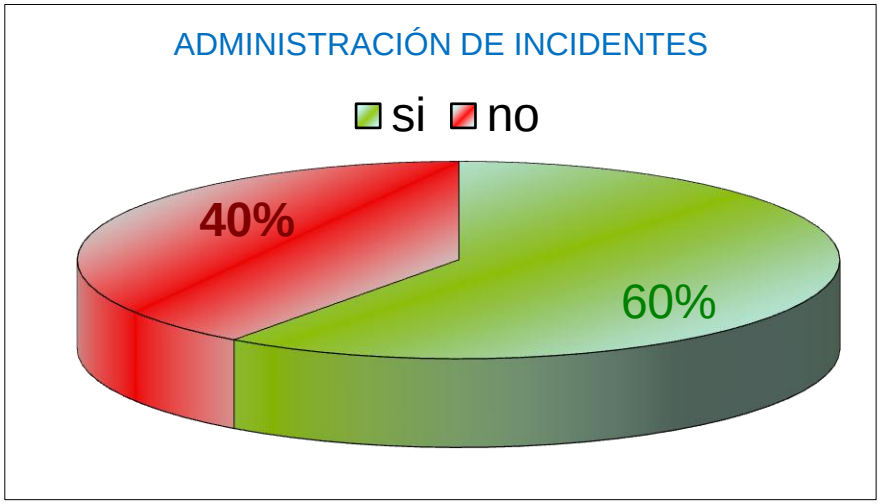


En la organización no existen controles criptográficos, que le permitan tener un alto grado de seguridad en el transporte de la información, ya sea a través de la red local, utilizando cableado o cuando se envía información utilizando la red inalámbrica, por lo tanto esta debe ser protegida para mantener la confidencialidad, autenticidad o integridad de la información, como tampoco hay control al acceso a los archivos de los sistemas operacionales poniendo a si el riesgo de alteración de estos mismos, esto sumándole a que no existe ningún tipo de control y seguridad del software y la información del sistema

de aplicación, ya que esto puede ocasionar la alteración de los sistemas de información. Tampoco existe ninguna clase de revisión en cuanto a las nuevas actualizaciones y parches de seguridad a los sistemas, todo esto cambios son considerados esenciales, por lo tanto debe ser probados y documentados exhaustivamente de manera que puedan aplicarse nuevamente, a futuras actualizaciones, tampoco hay control de vulnerabilidad en los equipos de la organización, esto puede ocasionar que al momento que exista un ataque al sistema de información no se tenga ninguna solución pronta, y ningún Diagnóstico en general de lo ocurrido, causando perdida de la información.

En este momento se encuentra que existe seguridad en las aplicaciones.

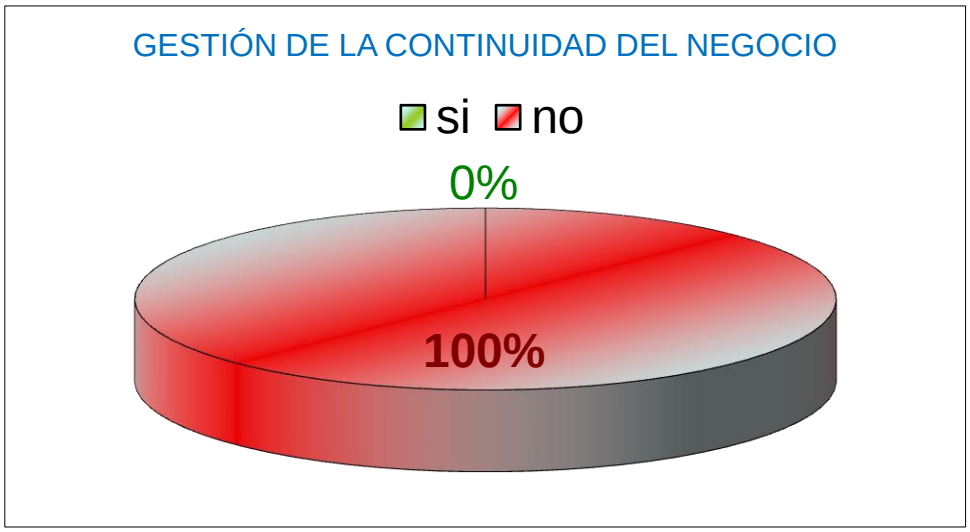
9. **Administración de incidentes**



Actualmente en la organización no están definidas las responsabilidades y debilidades antes un incidente y el procedimiento formal de respuesta.

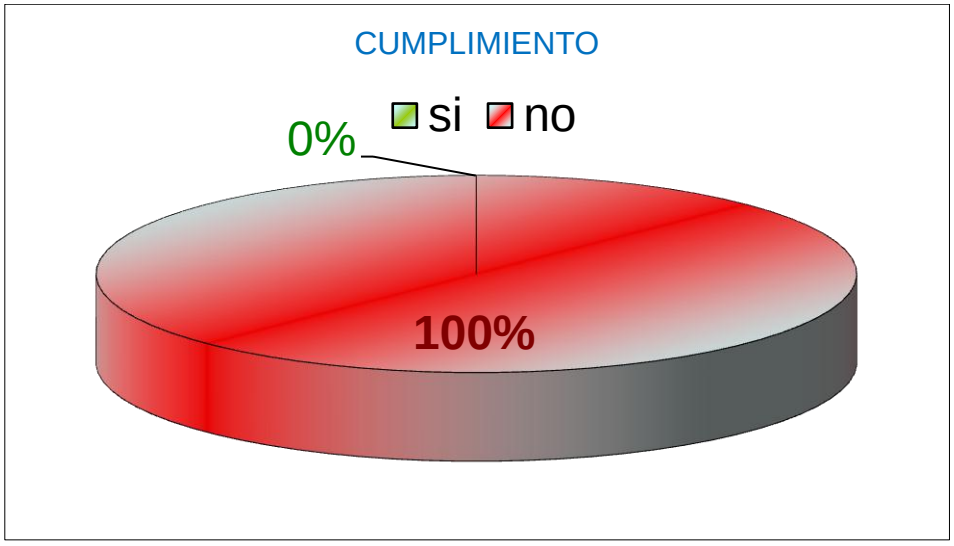
Aunque al momento de presentarse un incidente es atendido por el personal de servicios.

10. **Gestión de la continuidad del negocio**



No se ha implementado un proceso de administración de la continuidad de los negocios para reducir la discontinuidad ocasionada por fallas de seguridad y desastres naturales, accidentes, fallas en el equipamiento y acciones deliberadas mediante la combinación de controles preventivos y de recuperación, como tampoco se tiene analizado ni implementado planes de contingencia para garantizar que los procesos de negocios puedan restablecerse dentro de los plazos requeridos, dichos planes deben mantenerse en vigencias y transformarse en una parte integral del resto de los procesos de administración y gestión, como también se debe incluir controles destinados a identificar y reducir riesgos, atenuar las consecuencias de los incidentes perjudiciales, fallas de seguridad, interrupciones de servicios con el propósito que se pueda asegurar la reanudación oportuna de las operaciones indispensables.

11. **Cumplimiento**



No se tiene definido ni documentado todos los resquicitos legales, normativos y contractuales pertinentes para cada sistema de información, como también los controles específicos y las responsabilidades individuales, del mismo modo no se tiene implementado los procedimientos adecuados para garantizar el cumplimiento de las restricciones legales al uso del material respecto del cual puede existir derechos de propiedad intelectual, derechos de diseño o marcas registradas. Se debe garantizar que se lleven a cabo correctamente todos los procedimientos de seguridad dentro el área de responsabilidad, asimismo se debe considerar la implementación de una revisión periódica de todas la áreas de la organización para garantizar el cumplimiento de las políticas y estándares de seguridad. Se debe verificar periódicamente la compatibilidad de los sistemas de información con los estándares de implementación de la seguridad; esto comprende la revisión de los sistemas operacionales a fin de garantizar que los controles de hardware y software hayan sido correctamente implementados. No existe controles que protejan los sistemas de operaciones y las herramientas de auditoria en el transcurso de las auditoria de sistemas, asimismo, se requiere una protección

adecuada para salvaguardar la integridad y evitar el uso inadecuado de las herramientas de auditoria.

4. Amenazas y vulnerabilidades

4.1. Definición

Las amenazas son agentes capaces de explotar los fallos de seguridad, que denominamos puntos débiles y, como consecuencia de ello, causar pérdidas o daños a los activos de una empresa, afectando a sus negocios.

En las organizaciones, los activos de información están sujetos a distintas formas de amenazas. Una amenaza puede causar un incidente no deseado que puede generar daño a la organización y a sus activos.

“Una amenaza es la indicación de un potencial evento no deseado” (Albert y Dorofee, 2003). En conclusión, se podría decir que una amenaza es “Una indicación de un evento desagradable con el potencial de causar daño”.

Para poder implantar contramedidas de seguridad adecuadas, en primer lugar se debe comprender cuales son las amenazas a que una red está expuesta y cual son las vulnerabilidades de red explotadas por los ataques.

Para una empresa, las amenazas pueden ser de distintos tipos con base a si origen.

4.2. Clasificación

Cuando una organización inicia la identificación de activo de amenazas que pudiesen afectar sus activos, se conviene clasificarla, para facilitar su ubicación. A continuación mostramos los seis tipos de amenazas y factores aleatorios que desempeñan en relación con su casualidad.

1. **Amenazas naturales (**inundaciones, tsunamis o maremotos, tornados, huracanes, sismos, tormentas, incendio forestales **)**
2. **Amenazas a Instalaciones (**fuego, explosión, caída de energía, daño de agua, perdida de acceso, fallas mecánicas **)**
3. **Amenazas humanas (**huelgas, epidemia, materiales peligrosos, problemas de transporte, perdida de personal clave**)**
4. **Amenazas tecnológica (**virus, hacking, perdida de datos, fallas de hardware, fallas de software, fallas en la red, fallas en las líneas telefónicas**)**
5. **Amenazas operacionales (**crisis financiera, perdida de suplidores, fallas en los equipos, aspectos regulatorio, mala publicidad**)**
6. **Amenazas sociales (**motines, protesta, sabotaje, vandalismo, bombas, violencia laboral, terrorismo**)**

Como se nota, las amenazas se pueden originar de fuentes o eventos accidentales o deliberados.

Para que una amenaza cause daño a algún activo de información tendría que explotar una o más vulnerabilidades del sistema, aplicaciones o servicios usados por la organización a efecto de poder ser exitosa en su intención de hacer daño.

4.3. Identificación de amenazas

A Continuación conoceremos una lista de amenazas posibles de las que pueden ser víctimas los activos del Departamento de Sistemas del Tecnológico de Comfenalco**.** Se entiende por amenaza a la posible ocurrencia de todo hecho que pueda causar daños a los diferentes tipos de activos de la organización.

[N] Desastres Naturales

Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.

[N.1] Fuego	
Tipos de activos: • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [SI] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** **1. [D] disponibilidad**
Descripción: **Incendios:** posibilidad de que el fuego acabe con recursos del sistema de información del Departamento de Sistemas**,** en el laboratorio de sistemas solo se cuenta con un solo extinguidor, además técnicos no están capacitados en caso de emergencia como utilizar estos equipos.	

[N.2] Daños por agua	
Tipos de activos: • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [SI] soportes de información • [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad

• [L] instalaciones	
Descripción: **Inundaciones**: **posibilidad de que el agua acabe con los recursos del sistema,** dado que puedan presentarse Inundaciones por causa de lluvia en las instalaciones del Departamento de Sistemas**,** esto sumándole que hay varios equipos ubicados en el piso sin que estos estén protegidos con ninguna base ni defensa física, pudiendo ocasionar daños ceberos a estos. Además no existe un control donde se tenga un diseño de protecciones físicas contra daño por incendio, inundación, terremoto, explosión, manifestaciones sociales y otras formas de desastre natural o artificial.	

[N.*] Desastres naturales	
Tipos de activos: • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [SI] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: **Incidentes que se producen sin intervención humana**: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras, entre otros desastres naturales que causen avería y daños a las instalaciones del Departamento de Sistemas. Además no existe un control donde se tenga un diseño de protecciones físicas contra daño por incendio, inundación, terremoto, explosión, manifestaciones sociales y otras formas de desastre natural o artificial.	

[I] De origen industrial

Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.

[I.1] Fuego	
Tipos de activos: • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [SI] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: **Incendio:** posibilidad de que el fuego acabe con los recursos del sistema, dado que las instalaciones del Departamento de Sistemas cuenta con laboratorios que utilizan material inflamable. Pudimos observar que cuenta con un solo extinguidor, además los técnicos no están capacitados en caso de emergencia, ya que unas de las formas de evitar emergencia es saber utilizar el extinguidor de incendio, antes de verse en la situación de apagar el incendio, además de esto, deben saber la clasificación de los extintores. Asimismo no existe un control donde se tenga un diseño de protecciones físicas contra daño por incendio, inundación, terremoto, explosión, manifestaciones sociales y otras formas de desastre natural o artificial.	

[I.*] ***Desastres industriales***	
Tipos de activos: • [HW] equipos informáticos (hardware)	**Dimensiones:** **1. [D] disponibilidad**

• [COM] redes de comunicaciones • [SI] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	
Descripción: Otros **desastres debidos a la actividad humana**: explosiones, derrumbes, contaminación química, sobrecarga eléctrica, fluctuaciones eléctricas, accidentes de tráfico ya que en cualquier momento, la informática de la organización puede quebrar total o parcialmente como consecuencia de un siniestro fortuito, para seguir con la continuidad del negocio se debe planificar ciertas contramedidas. Además no existe un control donde se tenga un diseño de protecciones físicas contra daño por incendio, inundación, terremoto, explosión, manifestaciones sociales y otras formas de desastre natural o artificial.	

[I.5] ***Avería de origen físico o lógico***	
Tipos de activos: • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [SI] soportes de información • [AUX] equipamiento auxiliar	**Dimensiones:** **1. [D] disponibilidad**
Descripción: **Fallos en los equipos y/o fallos en los programas**. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema. En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es	

físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante. Se puede averiar cualquiera de los servidores que prestan servicios a toda la organización, ya sea por falta de mantenimiento o por algún evento que suceda como fluctuación de energía, que afecte desconfigurando de los programas.

[I.6] ***Corte del suministro eléctrico***	
Tipos de activos: • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [SI] soportes de información (electrónicos) • [AUX] equipamiento auxiliar	**Dimensiones:** **1. [D] disponibilidad**
Descripción: **Cese de la alimentación de potencia:** la organización dispone de unos Inversores, la cual es la que da soporte a todo los servidores.	

[I.7] ***Condiciones inadecuadas de temperatura y/o humedad***	
Tipos de activos: • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [SI] soportes de información • [AUX] equipamiento auxiliar	**Dimensiones:** **1. [D] disponibilidad**
Descripción: **Deficiencias en la aclimatación de los locales,** Existe una equipo de aire que mide	

correctamente la temperatura, variando la temperatura de acuerdo este se encuentra.

[I.8] ***Fallo de servicios de comunicaciones***	
Tipos de activos: • [COM] redes de comunicaciones	**Dimensiones:** **1. [D] disponibilidad**
Descripción: **Cese de la capacidad de transmitir datos de un sitio a otro.** Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente. Como también los fallos del proveedor de servicio de internet o daños en los dispositivos de comunicaciones de la red. Como es sabido se debe tener toda la esquema de la red de datos de la organización de la forma más optimizada con el fin de que cuando ocurra algún fallo de los servicios de comunicación poder llegar de la forma más rápida y precisa al evento ocasionado, logrando así una pronta solución	

[I.10] ***Degradación de los soportes de almacenamiento de la información***	
Tipos de activos: • [SI] soportes de información	**Dimensiones:** **1. [D] disponibilidad**
Descripción: Otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, tóner, refrigerante. Esta amenaza se da como consecuencia del paso del tiempo. Esta amenaza solo de identifica sobre soporte de almacenamiento de información y de los datos en general, pues cuando la información está en algún soporte informático hay amenazas específicas. Esta se presenta por que no existen medidas diseñadas para brindar protección a los	

soportes informáticos. También porque no existen políticas de procedimientos para el aseguramientos de los datos.

[E] Errores y fallos no intencionados

[E.1] ***Errores de los usuarios***	
Tipos de activos: • [S] servicios • [D] datos / información • [SW] aplicaciones (software)	**Dimensiones:** **1. [I] integridad** **2. [D] disponibilidad**
Descripción: **Equivocaciones de las personas cuando usan los servicios, datos, etc.** Este se presenta cuando no se le da la capacitación necesaria al personal que va a utilizar los sistemas de información de la organización y también por la falta de políticas y procedimientos para el uso de estos activos, además no se cuenta con los manuales de procedimientos necesarios para cuando un evento por error de usuario ocurra. Asimismo no existe algún control donde se comente que todos los empleados de la organización y, cuando se pertinente, los contratista y los usuarios de terceras partes deben recibir información adecuada en concientización y actualizaciones regulares sobre las políticas y los procedimientos de la organización, según sea pertinente para sus funciones laborales.	

[E.2] ***Errores del administrador***	
Tipos de activos: • [S] servicios	**Dimensiones:** **1. [D] disponibilidad**

• [D] datos / información • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones	**2. [I] integridad** **3. [C] confidencialidad** **4. [A_S] autenticidad**
Descripción: **Equivocaciones de personas con responsabilidades de instalación y operación,** en la parte administrativa, como en el desarrollo de las aplicaciones, y en el mantenimiento de los equipos; una mala instalación y operación de algunos de estos activos genera un mal funcionamiento en el cual repercutirá sobre los servicios que ofrece la Departamento de Sistemas, además también se presenta cuando no se le da la capacitación necesaria al personal que va a utilizar los sistemas de información, instalación, configuración.	

[E.4] ***Errores de configuración***	
Tipos de activos: • [S] servicios • [D] datos / información • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones	**Dimensiones:** **1. [D] disponibilidad** **2. [I] integridad** **3. [C] confidencialidad** **4. [A_S] autenticidad del servicio** **5. [A_D] autenticidad de los datos**
Descripción: **Introducción de datos de configuración erróneos,** prácticamente todos los activos	

dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc. Cuando se presenta una mala configuración en los recursos de sistemas, se presenta el riesgo de que los activos sean vulnerables a ataques externos.

[E.8] *Difusión de software dañino*	
Tipos de activos: • [SW] aplicaciones (software)	**Dimensiones:** **1. [D] disponibilidad** **2. [I] integridad** **3. [C] confidencialidad** **4. [A_S] autenticidad del servicio** **5. [A_D] autenticidad de los datos**
Descripción: **Propagación inocente de virus, espías *(spyware)*, gusanos, troyanos, bombas lógicas, etc.** Se presenta por falta de antivirus (Software, Hardware), o por la no actualización de este. Además no existe controles de código malicioso, ya que se debe tener implementado controles de detección, prevención y recuperación para proteger contra condigo maliciosos, así como procedimientos apropiados de concientización de los usuarios.	

[E.15] *Alteración de la información*	
Tipos de activos:	**Dimensiones:**

• [D] datos / información	**1. [I] integridad**
Descripción: **Alteración accidental de la información.** Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas. El departamento no tiene medidas de protección diseñadas para los soportes informáticos. También se da por que no existen políticas de procedimientos para el aseguramiento de los datos, es por eso que se deben hacer copias de respaldo de la información y del software, y se deben poner a pruebas con regularidad de acuerdo con la política de respaldo acordada.	

[E.16] ***Introducción de información incorrecta***	
Tipos de activos: • [D] datos / información	**Dimensiones:** **1. [I] integridad**
Descripción: **Inserción accidental de información incorrecta.** Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas. Es por eso que se deben hacer copias de respaldo de la información y del software, y se deben poner a pruebas con regularidad de acuerdo con la política de respaldo acordada. También se da porque no existe políticas de procedimientos para el aseguramiento de las datos	

[E.17] ***Degradación de la información***	
Tipos de activos:	**Dimensiones:**

• [D] datos / información	**1. [I] integridad**

Descripción:

Degradación accidental de la información, esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.

Esta se presenta por que no existen medidas diseñadas para brindar protección a los soportes informáticos. Es por eso que se deben hacer copias de respaldo de la información y del software, y se deben poner a pruebas con regularidad de acuerdo con la política de respaldo acordada También se da por que no existen políticas de procedimientos para los aseguramientos de los datos.

[E.18] ***Destrucción de información***	
Tipos de activos: • [D] datos / información	**Dimensiones:** **1. [D] disponibilidad**

Descripción:

Pérdida accidental de información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas. Es por eso que se debe hacer copias de respaldo de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldo acordada.

[E.19] ***Divulgación de información***	
Tipos de activos: • [D] datos / información	**Dimensiones:** **1. [C] confidencialidad**

Descripción: **Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel, etc**. No existe política o procedimientos para la divulgación de la información referente a los procesos que se realizan en la Organización, Además no existe un control donde se tenga establecido los procedimientos para el manejo de la información y almacenamiento de la información contra divulgación no autorizada uso inadecuado.

[E.20] Vulnerabilidades de los programas (software)	
Tipos de activos: • [SW] aplicaciones (software)	**Dimensiones:** **1. [I] integridad** **2. [D] disponibilidad** **3. [C] confidencialidad**
Descripción: Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar. Esto sucede cuando no se le hace un análisis exhaustivo sobre las vulnerabilidades que poseen en (los) software o los programas que adquiere la Organización. Además no se tiene establecido un control del vulnerabilidades técnica, donde se pueda obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información que están en uso, evaluar la exposición de la organización a fichas vulnerabilidades y tomar las acciones apropiadas para tratar los riesgos asociados.	

[E.23] ***Errores de mantenimiento / actualización de equipos (hardware)***

Tipos de activos:	Dimensiones:
• [HW] equipos informáticos (hardware)	**1. [D] disponibilidad**
Descripción: **Defectos en los procedimientos o controles de actualización de los equipos** que permiten que sigan utilizándose más allá del tiempo nominal de uso. Causando deterioros en ellos y el mal funcionamiento.	

[E.24] ***Caída del sistema por agotamiento de recursos***	
Tipos de activos: • [S] servicios • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones	**Dimensiones:** **1. [D] disponibilidad**
Descripción: **La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.** Esto se presenta cuando los activos existentes son saturados por falta de capacidad para procesar la información, debido a muchas peticiones de los usuarios a los activos.	

[A] Ataques intencionados

Fallos deliberados causados por las personas.

La numeración no es consecutiva para coordinarla con los errores no intencionados, muchas veces de naturaleza similar a los ataques deliberados, difiriendo únicamente en el propósito del sujeto.

[A.4] ***Manipulación de la configuración***

Tipos de activos: • [S] servicios • [D] datos / información • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones	**Dimensiones:** **1. [I] integridad** **2. [C] confidencialidad** **3. [A_S] autenticidad del servicio** **4. [A_D] autenticidad de los datos**
Descripción: Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc. Esto se presenta porque no hay un esquema de seguridad en la red administrativa, también para la detección de intrusos. Además no se tiene control de los registros de las actividades.	

[A.5] ***Suplantación de la identidad del usuario***	
Tipos de activos: • [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones	**Dimensiones:** **1. [C] confidencialidad** **2. [A_S] autenticidad del servicio** **3. [A_D] autenticidad de los datos** **4. [I] integridad**
Descripción: Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios.	

Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente. Esto se presenta porque no hay un esquema de seguridad, también para la detección de intrusos.

[A.6] *Abuso de privilegios de acceso*	
Tipos de activos: • [S] servicios • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones	**Dimensiones:** **1. [C] confidencialidad** **2. [I] integridad**
Descripción: Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, trae problemas y consecuencias.	

[A.11] *Acceso no autorizado*	
Tipos de activos: • [S] servicios • [D] datos / información • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [SI] soportes de información • [AUX] equipamiento auxiliar	**Dimensiones:** **1. [C] confidencialidad** **2. [I] integridad** **3. [A_S] autenticidad del servicio**

• [L] instalaciones	
Descripción: El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización. Esto se presenta por que se presentan ciertas vulnerabilidades que el atacante aprovecha para obtener un acceso no autorizado.	
[A.12] *Análisis de tráfico*	
Tipos de activos: • [COM] redes de comunicaciones	**Dimensiones:** **1. [C] confidencialidad**
Descripción: El atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios. A veces se denomina “monitorización de tráfico”. Se presenta por que la organización no cuenta ningún sistema de transmisión seguro que permita tener cierto grado de certidumbre de que los datos que se envían, sean los que se están recibiendo, tampoco se cuenta con un mecanismo que permita hacer uso del encriptamiento de la información.	

[A.14] *Interceptación de información (escucha)*	
Tipos de activos: • [D] datos / información • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones	**Dimensiones:** **1. [C] confidencialidad**
Descripción: El atacante llega a tener acceso a información que no le corresponde, sin que la	

información en sí misma se vea alterada.

[A.15] Modificación de la información	
Tipos de activos: • [D] datos / información	**Dimensiones:** **1. [I] integridad**
Descripción: Alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	

A.16] ***Introducción de falsa información***	
Tipos de activos: • [D] datos / información	**Dimensiones:** **1. [I] integridad**
Descripción: **Inserción interesada de información falsa,** con ánimo de obtener un beneficio o causar un perjuicio. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas. Esto se presenta por que no existe medidas de protección a los soporte o por que no existan políticas de procedimientos para la seguridad de los datos.	

[A.19] Divulgación de información	
Tipos de activos:	**Dimensiones:**

• [D] datos / información	**1. [C] confidencialidad**
Descripción: **Revelación de información,** se presenta por falta de programas detectores de intrusos como programas analizadores de red.	

[A.22] *Manipulación de programas*	
Tipos de activos: [SW] aplicaciones (software)	**Dimensiones:** **1. [C] confidencialidad** **2. [I] integridad** **3. [A_S] autenticidad del servicio** **4. [A_D] autenticidad de los datos**
Descripción: Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.	

[A.24] *Denegación de servicio*	
Tipos de activos: • [S] servicios • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones	**Dimensiones:** **1. [D] disponibilidad**
Descripción:	

La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.

[A.25] Robo	
Tipos de activos: • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [SI] soportes de información • [AUX] equipamiento auxiliar	**Dimensiones:** **1. [D] disponibilidad** **2. [C] confidencialidad**
Descripción: La sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales. El robo puede realizarlo personal interno, personas ajenas a la Organización o personas contratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.	
[A.28] *Indisponibilidad del personal*	
Tipos de activos: • [P] personal interno	**Dimensiones:** **1. [D] disponibilidad**
Descripción: Ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos.	

[A.30] *Ingeniería social*	
Tipos de activos: • [P] personal interno	**Dimensiones:** **1. [C] confidencialidad** **2. [I] integridad** **3. [A_S] autenticidad del servicio** **4. [A_D] autenticidad de los datos**
Descripción: Abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero. Esto se presenta por que no existe algún control donde se comente que todos los empleados de la organización y, cuando se pertinente, los contratista y los usuarios de terceras partes deben recibir información y capacitación adecuada en concientización y actualizaciones regulares sobre las políticas y los procedimientos de la organización, según sea pertinente para sus funciones laborales.	

4.4. VALORIZACION DE LAS AMENAZAS

Tabla de Frecuencia	
3	Alta
2	Media
1	Baja

		Dimensiones de seguridad			
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**
[SI_C_Elec] Servicio de Correo Electrónico					
[E.1] Errores de los usuarios	3	10%	50%	50%	60%
[E.2] Errores del administrador	2	90%			
[E.4] Errores de configuración	2	90%	30%	40%	30%
[E.14] Escapes de información	2	60%			
[E.19] Divulgación de información	2	40%	50%	70%	
[A.4] Manipulación de la configuración	2	30%	40%	60%	40%
[A.11] Acceso no autorizado	3	30%	60%	80%	
[A.14] Intercepción de información	1			90%	

(escucha)					
[A.19] Divulgación de información	2			80%	
[A.5] Suplantación de la identidad del usuario	2	30%	40%	80%	90%
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	100%			
[E.20] Vulnerabilidades de los programas (software)	2	70%	40%	60%	
[I.6] Corte del suministro eléctrico	3	90%			
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**
[HW_S_Domino] Servidor de Dominio					
[E.2] Errores del administrador	2	90%	40%	70%	70%
[E.4] Errores de configuración	1	90%	10%	10%	40%
[A.4] Manipulación de la configuración	1		70%	60%	70%
[A.11] Acceso no autorizado	1		90%	100%	80%
[A.25] Robo	1	100%		100%	
[A.24] Denegación de servicio	1	100%			

[A.14] Intercepción de información (escucha)	1			100%	
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	80%			
[I.6] Corte del suministro eléctrico	3	60%			
[E.24] Caída del sistema por agotamiento de recursos	1	80%			
[A.6] Abuso de privilegios de acceso	2		70%	80%	
[N.2] Daños por agua	2	80%			
[N.1] Fuego	1	100%			
[I.5] Avería de origen físico o lógico	2	90%			
[I.7] Condiciones inadecuadas de temperatura y/o humedad	2	80%			
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**
[HW_S_Arch] Servidor de Archivo					
[E.2] Errores del administrador	2	80%	80%	90%	70%
[E.4] Errores de configuración	1	90%	60%	10%	40%
[A.4] Manipulación de la configuración	1		70%	80%	70%
[A.11] Acceso no autorizado	1		90%	100%	80%

[A.25] Robo	1	100%		100%	
[A.24] Denegación de servicio	1	100%			
[A.14] Intercepción de información (escucha)	1			100%	
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	80%			
[I.6] Corte del suministro eléctrico	3	50%			
[E.24] Caída del sistema por agotamiento de recursos	1	80%			
[A.6] Abuso de privilegios de acceso	2		70%	80%	
[N.2] Daños por agua	2	80%			
[N.1] Fuego	1	100%			
[I.7] Condiciones inadecuadas de temperatura y/o humedad	2	80%			
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**
[HW_S_Arch] Servidor de Archivo					
[E.2] Errores del administrador	2	80%	80%	90%	70%
[E.4] Errores de configuración	1	90%	60%	10%	40%
[A.4] Manipulación de la configuración	1		70%	80%	70%

[A.11] Acceso no autorizado	1		90%	100%	80%
[A.25] Robo	1	100%		100%	
[A.24] Denegación de servicio	1	100%			
[A.14] Intercepción de información (escucha)	1			100%	
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	80%			
[I.6] Corte del suministro eléctrico	3	50%			
[E.24] Caída del sistema por agotamiento de recursos	1	80%			
[A.6] Abuso de privilegios de acceso	2		70%	80%	
[N.2] Daños por agua	2	80%			
[N.1] Fuego	1	100%			
[I.5] Avería de origen físico o lógico	2	90%			
[I.7] Condiciones inadecuadas de temperatura y/o humedad	2	80%			
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**
[HW_S_Proxy] Servidor Proxy					
[E.2] Errores del administrador	3	80%	30%	40%	70%
[E.4] Errores de configuración	1	90%	30%	10%	40%

[A.4] Manipulación de la configuración	1		70%	80%	70%
[A.11] Acceso no autorizado	1		40%	40%	30%
[A.25] Robo	2	100%		10%	
[A.24] Denegación de servicio	3	100%			
[A.14] Intercepción de información (escucha)	2			10%	
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	80%			
[I.6] Corte del suministro eléctrico	3	60%			
[E.24] Caída del sistema por agotamiento de recursos	1	80%			
[N.2] Daños por agua	2	80%			
[N.1] Fuego	1	100%			
[I.5] Avería de origen físico o lógico	2	90%			
[I.7] Condiciones inadecuadas de temperatura y/o humedad	2	80%			

Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**
[HW_Serv_PV] Servidor PV					
[E.2] Errores del administrador	1	80%	10%	40%	70%

[E.4] Errores de configuración	1	90%	30%	10%	40%
[A.4] Manipulación de la configuración	1		70%	40%	30%
[A.11] Acceso no autorizado	1		70%	60%	30%
[A.25] Robo	2	100%		40%	
[A.24] Denegación de servicio	3	100%			
[A.14] Intercepción de información (escucha)	2			40%	
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	80%			
[I.6] Corte del suministro eléctrico	3	60%			
[E.24] Caída del sistema por agotamiento de recursos	1	80%			
[A.6] Abuso de privilegios de acceso	2		40%	40%	
[N.2] Daños por agua	2	80%			
[N.1] Fuego	1	100%			
[I.5] Avería de origen físico o lógico	2	90%			
[I.7] Condiciones inadecuadas de temperatura y/o humedad	2	80%			
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**
[HW_Serv_CC] Servidor Cc					

[E.2] Errores del administrador	1	80%	30%	60%	70%
[E.4] Errores de configuración	1	90%	10%	60%	40%
[A.4] Manipulación de la configuración	1		70%	40%	30%
[A.11] Acceso no autorizado	1		70%	60%	30%
[A.25] Robo	1	100%		40%	
[A.24] Denegación de servicio	3	100%			
[A.14] Intercepción de información (escucha)	2			60%	
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	80%			
[I.6] Corte del suministro eléctrico	3	60%			
[E.24] Caída del sistema por agotamiento de recursos	1	80%			
[A.6] Abuso de privilegios de acceso	2		40%	40%	
[N.2] Daños por agua	2	80%			
[N.1] Fuego	1	100%			
[I.5] Avería de origen físico o lógico	2	90%			
[I.7] Condiciones inadecuadas de temperatura y/o humedad	2	80%			
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**

[HW_Serv_Ctgex] Servidor ctgexc					
[E.2] Errores del administrador	1	90%	50%	60%	70%
[E.4] Errores de configuración	1	90%	50%	60%	40%
[A.4] Manipulación de la configuración	1		80%	60%	50%
[A.11] Acceso no autorizado	1		80%	60%	30%
[A.25] Robo	1	100%		70%	
[A.24] Denegación de servicio	3	100%			
[A.14] Intercepción de información (escucha)	2			70%	
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	80%			
[I.6] Corte del suministro eléctrico	3	60%			
[E.24] Caída del sistema por agotamiento de recursos	1	80%			
[A.6] Abuso de privilegios de acceso	2		80%	70%	
[N.2] Daños por agua	2	90%			
[N.1] Fuego	1	100%			
[I.5] Avería de origen físico o lógico	2	90%			
[I.7] Condiciones inadecuadas de temperatura y/o humedad	2	80%			
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**

[HW_Serv_ISA] Servidor Isa					
[E.2] Errores del administrador	1	90%	60%	60%	80%
[E.4] Errores de configuración	1	90%	50%	60%	70%
[A.4] Manipulación de la configuración	1		80%	60%	70%
[A.11] Acceso no autorizado	1		80%	60%	30%
[A.25] Robo	1	100%		70%	
[A.24] Denegación de servicio	3	100%			
[A.14] Intercepción de información (escucha)	2			70%	
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	80%			
[I.6] Corte del suministro eléctrico	3	60%			
[E.24] Caída del sistema por agotamiento de recursos	1	80%			
[A.6] Abuso de privilegios de acceso	2		80%	70%	
[N.2] Daños por agua	2	90%			
[N.1] Fuego	1	100%			
[I.5] Avería de origen físico o lógico	2	90%			
[I.7] Condiciones inadecuadas de temperatura y/o humedad	2	80%			
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**

[HW_Serv_PV] Servidor Sp					
[E.2] Errores del administrador	1	90%	60%	60%	80%
[E.4] Errores de configuración	1	90%	50%	60%	70%
[A.4] Manipulación de la configuración	1		80%	60%	70%
[A.11] Acceso no autorizado	1		80%	60%	30%
[A.25] Robo	1	100%		70%	
[A.24] Denegación de servicio	3	100%			
[A.14] Intercepción de información (escucha)	2			70%	
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	80%			
[I.6] Corte del suministro eléctrico	3	60%			
[E.24] Caída del sistema por agotamiento de recursos	1	80%			
[A.6] Abuso de privilegios de acceso	2		80%	70%	
[N.2] Daños por agua	2	90%			
[N.1] Fuego	1	100%			
[I.5] Avería de origen físico o lógico	2	90%			
[I.7] Condiciones inadecuadas de temperatura y/o humedad	2	80%			
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**

[HW_Serv_DHCP] Servidor Dhcp					
[E.2] Errores del administrador	1	90%	30%	30%	
[E.4] Errores de configuración	1	90%	40%	30%	70%
[A.4] Manipulación de la configuración	1		80%	60%	70%
[A.11] Acceso no autorizado	1		80%	60%	30%
[A.25] Robo	1	100%		70%	
[A.24] Denegación de servicio	3	100%			
[A.14] Intercepción de información (escucha)	2			70%	
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	80%			
[I.6] Corte del suministro eléctrico	3	60%			
[E.24] Caída del sistema por agotamiento de recursos	1	80%			
[A.6] Abuso de privilegios de acceso	2		80%	70%	
[N.2] Daños por agua	2	90%			
[N.1] Fuego	1	100%			
[I.5] Avería de origen físico o lógico	2	90%			
[I.7] Condiciones inadecuadas de temperatura y/o humedad	2	80%			
Activo / Amenaza		**D**	**I**	**C**	**A_S**

	frecuencia				
[HW_Serv_RC] Servidor Rc					
[E.2] Errores del administrador	1	70%	30%	30%	
[E.4] Errores de configuración	1	90%	40%	30%	70%
[A.4] Manipulación de la configuración	1		80%	60%	70%
[A.11] Acceso no autorizado	1		80%	60%	30%
[A.25] Robo	1	100%		70%	
[A.24] Denegación de servicio	3	100%			
[A.14] Intercepción de información (escucha)	2			70%	
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	80%			
[I.6] Corte del suministro eléctrico	3	60%			
[E.24] Caída del sistema por agotamiento de recursos	1	80%			
[A.6] Abuso de privilegios de acceso	2		80%	70%	
[N.2] Daños por agua	2	90%			
[N.1] Fuego	1	100%			
[I.5] Avería de origen físico o lógico	2	90%			
[E.17] Degradación de la información					

Activo / Amenaza	frecuencia	D	I	C	A_S
[HW_Serv_Alma] Servidor Almacenamiento					
[E.2] Errores del administrador	1	90%	60%	60%	80%
[E.4] Errores de configuración	1	90%	80%	80%	80%
[A.4] Manipulación de la configuración	1		80%	60%	70%
[A.11] Acceso no autorizado	1		80%	60%	30%
[A.25] Robo	1	100%		70%	
[A.24] Denegación de servicio	2	100%			
[A.14] Intercepción de información (escucha)	2			80%	
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	80%			
[I.6] Corte del suministro eléctrico	3	60%			
[E.24] Caída del sistema por agotamiento de recursos	1	80%			
[A.6] Abuso de privilegios de acceso	2		80%	70%	
[N.2] Daños por agua	2	90%			
[N.1] Fuego	1	100%			
[I.5] Avería de origen físico o lógico	2	90%			

[I.7] Condiciones inadecuadas de temperatura y/o humedad	2	80%			
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**
[HW_Serv_Syne] Servidor Synersis					
[E.2] Errores del administrador	2	90%	80%	60%	80%
[E.4] Errores de configuración	1	90%	80%	70%	80%
[A.4] Manipulación de la configuración	1		80%	60%	70%
[A.11] Acceso no autorizado	1		80%	60%	70%
[A.25] Robo	1	100%		80%	
[A.24] Denegación de servicio	2	100%			
[A.14] Intercepción de información (escucha)	2			80%	
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	80%			
[I.6] Corte del suministro eléctrico	3	100%			
[E.24] Caída del sistema por agotamiento de recursos	1	80%			
[A.6] Abuso de privilegios de acceso	2		80%	70%	
[N.2] Daños por agua	2	90%			
[N.1] Fuego	1	100%			

[I.5] Avería de origen físico o lógico	2	90%			
[I.7] Condiciones inadecuadas de temperatura y/o humedad	2	80%			
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**
[HW_Mobile] Informática Móvil					
[E.2] Errores del administrador	1	80%	60%	60%	70%
[E.4] Errores de configuración	1	50%	40%	60%	70%
[A.4] Manipulación de la configuración	1		70%	60%	70%
[A.11] Acceso no autorizado	1		80%	60%	30%
[A.25] Robo	1	100%		80%	
[A.24] Denegación de servicio	2	100%			
[A.14] Intercepción de información (escucha)	2			80%	
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	80%			
[I.6] Corte del suministro eléctrico	3	30%			
[E.24] Caída del sistema por agotamiento de recursos	1	80%			
[A.6] Abuso de privilegios de acceso	2		80%	70%	
[N.2] Daños por agua	2	90%			

[N.1] Fuego	1	100%			
[I.5] Avería de origen físico o lógico	2	90%			
[I.7] Condiciones inadecuadas de temperatura y/o humedad	2	80%			
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**
[HW_Printer] Medios de Impresión y escáner					
[E.2] Errores del administrador	1	80%			
[E.4] Errores de configuración	1	90%			
[A.25] Robo	1	100%			
[A.14] Intercepción de información (escucha)	2			70%	
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	80%			
[I.6] Corte del suministro eléctrico	3	80%			
[E.24] Caída del sistema por agotamiento de recursos	1	80%			
[N.2] Daños por agua	2	90%			
[N.1] Fuego	1	100%			
[I.5] Avería de origen físico o lógico	2	90%			
[I.7] Condiciones inadecuadas de temperatura y/o humedad	2	80%			
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**

[HW_Acces_P] Access Point					
[E.2] Errores del administrador	1	90%			80%
[E.4] Errores de configuración	1	90%			80%
[A.4] Manipulación de la configuración	1				70%
[A.11] Acceso no autorizado	1				30%
[A.25] Robo	1	100%			
[A.24] Denegación de servicio	2	100%			
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	70%			
[I.6] Corte del suministro eléctrico	3	80%			
[E.24] Caída del sistema por agotamiento de recursos	1	80%			
[N.2] Daños por agua	2	90%			
[N.1] Fuego	1	100%			
[I.5] Avería de origen físico o lógico	2	90%			
[I.7] Condiciones inadecuadas de temperatura y/o humedad	2	80%			
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**

[HW_Arma] Armarios					
[E.2] Errores del administrador	1	90%			
[E.4] Errores de configuración					
[A.4] Manipulación de la configuración					
[A.11] Acceso no autorizado					
[A.25] Robo	1	100%			
[A.24] Denegación de servicio					
[A.14] Intercepción de información (escucha)					
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	60%			
[I.6] Corte del suministro eléctrico					
[E.24] Caída del sistema por agotamiento de recursos	1	30%			
[A.6] Abuso de privilegios de acceso					
[N.2] Daños por agua	2	80%			
[N.1] Fuego	1	100%			
[I.5] Avería de origen físico o lógico	2	80%			
[I.7] Condiciones inadecuadas de temperatura y/o humedad	2	40%			
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**
[HW_Swith] Conmutadores					
[E.2] Errores del administrador	2	90%			70%

[E.4] Errores de configuración	2	90%			70%
[A.4] Manipulación de la configuración	1				70%
[A.11] Acceso no autorizado	1				30%
[A.25] Robo	1	100%			
[A.24] Denegación de servicio	2	100%			
[A.14] Intercepción de información (escucha)					
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	80%			
[I.6] Corte del suministro eléctrico	3	80%			
[E.24] Caída del sistema por agotamiento de recursos	1	80%			
[N.2] Daños por agua	2	90%			
[N.1] Fuego	1	100%			
[I.5] Avería de origen físico o lógico	2	90%			
[I.7] Condiciones inadecuadas de temperatura y/o humedad	2	40%			
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**
[HW_Router] Encaminadores					
[E.2] Errores del administrador	2	90%			70%

[E.4] Errores de configuración	2	90%			70%
[A.4] Manipulación de la configuración	1				70%
[A.11] Acceso no autorizado	1				30%
[A.25] Robo	1	100%			
[A.24] Denegación de servicio	2	100%			
[A.14] Intercepción de información (escucha)					
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	80%			
[I.6] Corte del suministro eléctrico	3	80%			
[E.24] Caída del sistema por agotamiento de recursos	1	80%			
[A.6] Abuso de privilegios de acceso	2	80%			
[N.2] Daños por agua	1	90%			
[N.1] Fuego	2	100%			
[I.5] Avería de origen físico o lógico	2	90%			
[I.7] Condiciones inadecuadas de temperatura y/o humedad	1	40%			
[S_Internet] Servicio de Internet					
[E.1] Errores de los usuarios	2	60%	10%		
[E.2] Errores del administrador	1	80%	10%		10%
[E.4] Errores de configuración	1	70%	10%		10%

[E.9] Errores de [re-]encaminamiento	1		10%		70%
[E.24] Caída del sistema por agotamiento de recursos	2	80%			
[A.4] Manipulación de la configuración	2		70%		60%
[A.5] Suplantación de la identidad del usuario					
[A.6] Abuso de privilegios de acceso	2		80%		
[I.6] Corte del suministro eléctrico	2	40%			
[A.10] Alteración de secuencia	1		50%		
[A.7] Uso no previsto	3	40%			
[A.11] Acceso no autorizado	2	60%	70%		
[A.24] Denegación de servicio	2	90%			
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**
[S_Luz] Energía Empresarial					
[E.1] Errores de los usuarios	2	70%	60%		
[E.2] Errores del administrador	1	90%	40%		
[E.4] Errores de configuración					
[E.9] Errores de [re-]encaminamiento	1		30%		
[E.24] Caída del sistema por agotamiento de recursos	2	80%			

[A.4] Manipulación de la configuración	2		40%		
[A.5] Suplantación de la identidad del usuario	2		80%	30%	
[A.6] Abuso de privilegios de acceso	2		80%	20%	
[I.6] Corte del suministro eléctrico					
[A.10] Alteración de secuencia	1		80%		
[A.7] Uso no previsto	3	40%			
[A.11] Acceso no autorizado	2	60%	70%	80%	
[A.24] Denegación de servicio					
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**
[S_Comuni] Servicio de comunicaciones					
[E.1] Errores de los usuarios	2	70%	50%		
[E.2] Errores del administrador	1	70%	40%	90%	60%
[E.4] Errores de configuración	1	40%	70%	40%	70%
[E.9] Errores de [re-]encaminamiento	1		70%	70%	70%
[E.24] Caída del sistema por agotamiento de recursos	2	80%			
[A.4] Manipulación de la configuración	2		70%	70%	60%

[A.5] Suplantación de la identidad del usuario	2		80%	70%	70%
[A.6] Abuso de privilegios de acceso	2		80%	70%	
[A.10] Alteración de secuencia	1		80%		
[A.7] Uso no previsto	3	40%			
[I.6] Corte del suministro eléctrico	2	80%			
[A.11] Acceso no autorizado	2	60%	70%	80%	
[A.24] Denegación de servicio	2	90%			
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**
[S_Correo] Servicio Correo electrónico					
[E.1] Errores de los usuarios	2	70%	50%		
[E.2] Errores del administrador	1	70%	40%	90%	60%
[E.4] Errores de configuración	1	40%	70%	40%	70%
[E.9] Errores de [re-]encaminamiento	1		70%	60%	70%
[E.24] Caída del sistema por agotamiento de recursos	2	80%			
[A.4] Manipulación de la configuración	2		70%	70%	60%

[A.5] Suplantación de la identidad del usuario	2		80%	70%	70%
[A.6] Abuso de privilegios de acceso	2		80%	70%	
[A.10] Alteración de secuencia	1		80%		
[A.7] Uso no previsto	2	40%			
[I.6] Corte del suministro eléctrico	2	80%			
[A.11] Acceso no autorizado	2	60%	70%	80%	
[A.24] Denegación de servicio	2	70%			
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**
[S_Int_Inal] Servicio de Internet Inalámbrico					
[E.1] Errores de los usuarios	2	70%			
[E.2] Errores del administrador	1	70%	40%		60%
[E.4] Errores de configuración	1	40%	70%	40%	70%
[E.9] Errores de [re-]encaminamiento	1		70%	70%	70%
[E.24] Caída del sistema por agotamiento de recursos	2	80%			
[A.4] Manipulación de la configuración	2		70%	70%	60%

[A.5] Suplantación de la identidad del usuario	2		70%	60%	60%
[A.6] Abuso de privilegios de acceso	2		80%	70%	
[A.10] Alteración de secuencia	1		80%		
[A.7] Uso no previsto	3	40%			
[I.6] Corte del suministro eléctrico	2	80%			
[A.11] Acceso no autorizado	2	60%	70%	80%	
[A.24] Denegación de servicio	2	90%			
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**
[Técnico] Servicio Técnico					
[E.1] Errores de los usuarios	2	70%	50%		
[E.2] Errores del administrador	1	70%	40%	90%	60%
[E.4] Errores de configuración	1	70%	70%	40%	70%
[E.9] Errores de [re-]encaminamiento	1		70%	70%	70%
[E.24] Caída del sistema por agotamiento de recursos					
[A.4] Manipulación de la configuración	2		70%	70%	60%
[A.5] Suplantación de la identidad del usuario					

[A.6] Abuso de privilegios de acceso	2		80%	70%	
[A.10] Alteración de secuencia	1		80%		
[A.7] Uso no previsto	3	40%			
[I.6] Corte del suministro eléctrico					
[A.11] Acceso no autorizado	2	60%	70%	80%	
[A.24] Denegación de servicio	2	90%			
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**
[Backup] Servicio de Backup					
[E.1] Errores de los usuarios	2	40%	50%		
[E.2] Errores del administrador	1	70%	40%	90%	60%
[E.4] Errores de configuración	1	40%	60%	40%	70%
[E.9] Errores de [re-]encaminamiento	1		70%	70%	70%
[E.24] Caída del sistema por agotamiento de recursos	2	80%			
[A.4] Manipulación de la configuración	2		70%	60%	60%
[A.5] Suplantación de la identidad del usuario					
[A.6] Abuso de privilegios de acceso					

[A.10] Alteración de secuencia	1		80%		
[A.7] Uso no previsto	2	40%			
[I.6] Corte del suministro eléctrico		80%			
[A.11] Acceso no autorizado	2	60%	70%	80%	
[A.24] Denegación de servicio					
[D_R] Datos Reservados					
[N.1] Fuego	1	100%	80%		
[E.2] Errores del administrador	1	40%			70%
[E.4] Errores de configuración	1	80%	70%	50%	80%
[E.14] Escapes de información	1		80%	80%	70%
[E.15] Alteración de la información	2	80%			
[E.16] Introducción de información incorrecta	2		90%	70%	
[E.17] Degradación de la información	2		90%	80%	
[E.18] Destrucción de información	2		80%	70%	
[E.19] Divulgación de información	1		80%		
[A.4] Manipulación de la configuración	2	90%			
[A.11] Acceso no autorizado	1	90%			
[A.14] Interceptación de información (escucha)	2	100%	80%	80%	
[A.15] Modificación de la información	1	80%	70%		
[A.16] Introducción de falsa información	2	90%	80%		

[N.2] Daños por agua	1	90%	80%		
[A.17] Corrupción de la información	1	80%	70%		
[A.19] Divulgación de información	1	90%	80%	80%	
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**
[D_C] Datos Confidencial					
[N.1] Fuego	1	100%	90%		
[E.2] Errores del administrador	1	80%	70%		70%
[E.4] Errores de configuración	1	90%	90%	100%	70%
[E.14] Escapes de información	1		100%	100%	90%
[E.15] Alteración de la información	2	90%			
[E.16] Introducción de información incorrecta	2		90%	100%	
[E.17] Degradación de la información	2		100 %	90%	
[E.18] Destrucción de información	2		100 %	90%	
[E.19] Divulgación de información	1	60%	100 %		
[A.4] Manipulación de la configuración	2	60%			

[A.11] Acceso no autorizado	1	70%			
[A.14] Interceptación de información (escucha)	2	60%	80%	100%	
[A.15] Modificación de la información	1	50%	90%		
[A.16] Introducción de falsa información	2	70%	100 %		
[N.2] Daños por agua	1	90%			
[A.17] Corrupción de la información	1	30%	90%		
[A.19] Divulgación de información	1	30%	100 %	100%	
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**
[D_SC] Datos sin clasificar					
[N.1] Fuego	1	100%	80%		
[E.2] Errores del administrador					
[E.4] Errores de configuración	1	80%	70%	40%	70%
[E.14] Escapes de información	1		70%	70%	70%
[E.15] Alteración de la información	2	80%			
[E.16] Introducción de información incorrecta	2		70%	70%	
[E.17] Degradación de la información	2		80%	70%	

[E.18] Destrucción de información	2		80%	70%	
[E.19] Divulgación de información	1	60%	100 %		
[A.4] Manipulación de la configuración	2	60%			
[A.11] Acceso no autorizado	1	70%			
[A.14] Interceptación de información (escucha)	2	60%	80%	100%	
[A.15] Modificación de la información	1	50%	90%		
[A.16] Introducción de falsa información	2	70%	100 %		
[N.2] Daños por agua	1	90%			
[A.17] Corrupción de la información	1	30%	90%		
[A.19] Divulgación de información	1	30%	100 %	100%	
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**
[D_Printed] Material Impreso					
[N.1] Fuego	1	100%	70%		
[E.2] Errores del administrador					
[E.4] Errores de configuración					
[E.14] Escapes de información	1		70%	60%	70%
[E.15] Alteración de la información	2	80%			

[E.16] Introducción de información incorrecta	2		70%	70%	
[E.17] Degradación de la información	2		80%	70%	
[E.18] Destrucción de información	2		80%	70%	
[E.19] Divulgación de información	1		80%		
[A.4] Manipulación de la configuración	2	60%			
[A.11] Acceso no autorizado	1	70%			
[A.14] Interceptación de información (escucha)	2	60%	70%	60%	
[A.15] Modificación de la información	1	30%	60%		
[A.16] Introducción de falsa información	2	80%	60%		
[N.2] Daños por agua	1	90%			
[A.17] Corrupción de la información	1	30%	40%		
[A.19] Divulgación de información	1	30%	60%	80%	
[D_Info] Archivos datos Informático					
[N.1] Fuego	1	100%	90%		
[E.2] Errores del administrador	1	80%	70%		70%
[E.4] Errores de configuración	1	90%	90%	100%	70%
[E.14] Escapes de información	1		100%	100%	90%
[E.15] Alteración de la información	2	90%			
[E.16] Introducción de información incorrecta	2		90%	100%	

[E.17] Degradación de la información	2		100 %	90%	
[E.18] Destrucción de información	2		100 %	90%	
[E.19] Divulgación de información	1	60%	100 %		
[A.4] Manipulación de la configuración	2	60%			
[A.11] Acceso no autorizado	1	70%			
[A.14] Interceptación de información (escucha)	2	60%	80%	100%	
[A.15] Modificación de la información	1	50%	90%		
[A.16] Introducción de falsa información	2	70%	100 %		
[N.2] Daños por agua	1	90%			
[A.17] Corrupción de la información	1	30%	90%		
[A.19] Divulgación de información	1	30%	100 %	100%	
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**
[D_Finan_Con] datos Financiero y contable					
[N.1] Fuego	1	100%	90%		
[E.2] Errores del administrador	1	80%	70%		70%

[E.4] Errores de configuración	1	90%	90%	100%	70%
[E.14] Escapes de información	1		100%	100%	90%
[E.15] Alteración de la información	2	90%			
[E.16] Introducción de información incorrecta	2		90%	100%	
[E.17] Degradación de la información	2		100 %	90%	
[E.18] Destrucción de información	2		100 %	90%	
[E.19] Divulgación de información	1	60%	100 %		
[A.4] Manipulación de la configuración	2	60%			
[A.11] Acceso no autorizado	1	70%			
[A.14] Interceptación de información (escucha)	2	60%	80%	100%	
[A.15] Modificación de la información	1	50%	90%		
[A.16] Introducción de falsa información	2	70%	100 %		
[N.2] Daños por agua	1	90%			
[A.17] Corrupción de la información	1	30%	90%		
[A.19] Divulgación de información	1	30%	100 %	100%	
Activo / Amenaza		**D**	**I**	**C**	**A_S**

	frecuencia				
[SW_Anti] Antivirus					
[I.5] Avería de origen físico o lógico	1	80%			
[E.1] Errores de los usuarios	2	70%			
[E.2] Errores del administrador	1	80%			20%
[E.4] Errores de configuración	1				70%
[E.8] Difusión de software dañino	2	80%			
[E.9] Errores de [re-]encaminamiento					
[E.14] Escapes de información					
[E.20] Vulnerabilidades de los programas (software)					
[E.21] Errores de mantenimiento / actualización de programas (software)	1	60%			
[A.4] Manipulación de la configuración	2	60%			
[A.5] Suplantación de la identidad del usuario	1	10%			
[A.6] Abuso de privilegios de acceso	2	60%			
[A.7] Uso no previsto	1	30%			
[A.10] Alteración de secuencia	2	80%			
[A.11] Acceso no autorizado					
[A.14] Interceptación de información (escucha)	1	10%			

[A.22] Manipulación de programas	1	30%			
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**
[SW_SO] Sistemas Operativos					
[I.5] Avería de origen físico o lógico	1	90%			
[E.1] Errores de los usuarios	2	80%			
[E.2] Errores del administrador	1	80%			60%
[E.4] Errores de configuración	1				70%
[E.8] Difusión de software dañino	2	80%			
[E.9] Errores de [re-]encaminamiento					
[E.14] Escapes de información					
[E.20] Vulnerabilidades de los programas (software)					
[E.21] Errores de mantenimiento / actualización de programas (software)	1	60%			
[A.4] Manipulación de la configuración	2	60%			
[A.5] Suplantación de la identidad del usuario	1	40%			
[A.6] Abuso de privilegios de acceso	2	60%			
[A.7] Uso no previsto	1	30%			
[A.10] Alteración de secuencia	2	80%			
[A.11] Acceso no autorizado					

[A.14] Interceptación de información (escucha)	1	10%			
[A.22] Manipulación de programas	1	30%			
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**
[SW_Office] Ofimáticas					
[I.5] Avería de origen físico o lógico	1	90%			
[E.1] Errores de los usuarios	2	80%			
[E.2] Errores del administrador	1	80%			60%
[E.4] Errores de configuración	1				70%
[E.8] Difusión de software dañino	2	80%			
[E.9] Errores de [re-]encaminamiento					
[E.14] Escapes de información					
[E.20] Vulnerabilidades de los programas					
[E.21] Errores de mantenimiento / actualización de programas (software)	1	60%			
[A.4] Manipulación de la configuración	2	60%			
[A.5] Suplantación de la identidad del usuario	1	40%			
[A.6] Abuso de privilegios de acceso	2	60%			
[A.7] Uso no previsto	1	30%			
[A.10] Alteración de secuencia	2	80%			

[A.11] Acceso no autorizado					
[A.14] Interceptación de información (escucha)	1	10%			
[A.22] Manipulación de programas	1	30%			
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**
[SW_Browser] Navegador					
[I.5] Avería de origen físico o lógico	1	60%			
[E.1] Errores de los usuarios	2	40%			
[E.2] Errores del administrador	1	60%			20%
[E.4] Errores de configuración	1				70%
[E.8] Difusión de software dañino	2	60%			
[E.9] Errores de [re-]encaminamiento					
[E.14] Escapes de información					
[E.20] Vulnerabilidades de los programas (software)					
[E.21] Errores de mantenimiento / actualización de programas (software)	1	30%			
[A.4] Manipulación de la configuración	2	40%			
[A.5] Suplantación de la identidad del usuario	1	10%			
[A.6] Abuso de privilegios de acceso	2	30%			

[A.7] Uso no previsto	1	30%			
[A.10] Alteración de secuencia	2	20%			
[A.11] Acceso no autorizado					
[A.14] Interceptación de información (escucha)	1	10%			
[A.22] Manipulación de programas	1	30%			
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**
[SW_Sap] SAP Nomina					
[I.5] Avería de origen físico o lógico	1	90%			90%
[E.1] Errores de los usuarios	2	80%	80%		
[E.2] Errores del administrador	1	90%	80%		90%
[E.4] Errores de configuración	1	100%			
[E.8] Difusión de software dañino	2	80%			
[E.9] Errores de [re-]encaminamiento	1	80%			
[E.14] Escapes de información	1		80%		
[E.20] Vulnerabilidades de los programas (software)	1	80%			
[E.21] Errores de mantenimiento / actualización de programas (software)	1	80%			

[A.4] Manipulación de la configuración	2	60%			
[A.5] Suplantación de la identidad del usuario	1	90%	90%		
[A.6] Abuso de privilegios de acceso	2	80%			
[A.7] Uso no previsto	1	80%			
[A.10] Alteración de secuencia	2	90%			
[A.11] Acceso no autorizado	1	90%	80%		
[A.14] Interceptación de información (escucha)	1	90%	70%		
[A.22] Manipulación de programas	1	80%			

Activo / Amenaza	frecuencia	D	I	C	A_S
[SW_Dbms] Sistemas gestión bases de datos					
[I.5] Avería de origen físico o lógico	1	80%			20%
[E.1] Errores de los usuarios	2	70%			
[E.2] Errores del administrador	1	90%			10%
[E.4] Errores de configuración	1	100%			

[E.8] Difusión de software dañino	2	80%			
[E.9] Errores de [re-]encaminamiento	1	80%			
[E.14] Escapes de información					
[E.20] Vulnerabilidades de los programas (software)	1	70%			
[E.21] Errores de mantenimiento / actualización de programas (software)	1	70%			
[A.4] Manipulación de la configuración	2	60%			
[A.5] Suplantación de la identidad del usuario	1	10%			
[A.6] Abuso de privilegios de acceso	2	40%			
[A.7] Uso no previsto	1	40%			
[A.10] Alteración de secuencia	2	20%			
[A.11] Acceso no autorizado	1	30%	80%		
[A.14] Interceptación de información (escucha)	1	90%	70%		
[A.22] Manipulación de programas	1	80%			
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**
[SW_Len_pro] Plataforma de Programación					
[I.5] Avería de origen físico o lógico	1	80%			20%

[E.1] Errores de los usuarios	2	70%			
[E.2] Errores del administrador	1	90%			10%
[E.4] Errores de configuración	1	100%			
[E.8] Difusión de software dañino	2	80%			
[E.9] Errores de [re-]encaminamiento	1	80%			
[E.14] Escapes de información					
[E.20] Vulnerabilidades de los programas (software)	1	70%			
[E.21] Errores de mantenimiento / actualización de programas (software)	1	70%			
[A.4] Manipulación de la configuración	2	60%			
[A.5] Suplantación de la identidad del usuario	1	10%			
[A.6] Abuso de privilegios de acceso	2	40%			
[A.7] Uso no previsto	1	40%			
[A.10] Alteración de secuencia	2	20%			
[A.11] Acceso no autorizado	1	30%	80%		
[A.14] Interceptación de información (escucha)	1	90%	70%		
[A.22] Manipulación de programas	1	80%			
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**

[SW_email] Outlook					
[I.5] Avería de origen físico o lógico	1	90%			90%
[E.1] Errores de los usuarios	2	80%	80%		
[E.2] Errores del administrador	1	90%	80%		90%
[E.4] Errores de configuración	1	100%			
[E.8] Difusión de software dañino	2	80%			
[E.9] Errores de [re-]encaminamiento	1	80%			
[E.14] Escapes de información	1		80%		
[E.20] Vulnerabilidades de los programas (software)	1	80%			
[E.21] Errores de mantenimiento / actualización de programas (software)	1	80%			
[A.4] Manipulación de la configuración	2	60%			
[A.5] Suplantación de la identidad del usuario	1	90%	90%		
[A.6] Abuso de privilegios de acceso	2	80%			
[A.7] Uso no previsto	1	80%			
[A.10] Alteración de secuencia	2	90%			
[A.11] Acceso no autorizado	1	90%	80%		
[A.14] Interceptación de información (escucha)	1	90%	70%		
[A.22] Manipulación de programas	1	80%			

Activo / Amenaza	frecuencia	D	I	C	A_S
[SW_Synersis] Synersis					
[I.5] Avería de origen físico o lógico	1	90%			90%
[E.1] Errores de los usuarios	2	80%	80%		
[E.2] Errores del administrador	1	90%	80%		90%
[E.4] Errores de configuración	1	100%			
[E.8] Difusión de software dañino	2	80%			
[E.9] Errores de [re-]encaminamiento	1	80%			
[E.14] Escapes de información	1		80%		90%
[E.20] Vulnerabilidades de los programas (software)	1	80%			
[E.21] Errores de mantenimiento / actualización de programas (software)	1	80%			
[A.4] Manipulación de la configuración	2	60%			
[A.5] Suplantación de la identidad del usuario	1	90%	90%		
[A.6] Abuso de privilegios de acceso	2	80%			
[A.7] Uso no previsto	1	80%			
[A.10] Alteración de secuencia	2	90%			

[A.11] Acceso no autorizado	1	90%	80%		
[A.14] Interceptación de información (escucha)	1	90%	70%		
[A.22] Manipulación de programas	1	80%			
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**
[SW_Backup] Sistemas de Backup					
[I.5] Avería de origen físico o lógico	1	80%			20%
[E.1] Errores de los usuarios	2	70%	80%	90%	
[E.2] Errores del administrador	1	90%			10%
[E.4] Errores de configuración	1	100%			
[E.8] Difusión de software dañino	2	80%			
[E.9] Errores de [re-]encaminamiento	1	80%			60%
[E.14] Escapes de información	1		80%	90%	
[E.20] Vulnerabilidades de los programas (software)	1	70%			
[E.21] Errores de mantenimiento / actualización de programas (software)	1	70%			
[A.4] Manipulación de la configuración	2	60%			

[A.5] Suplantación de la identidad del usuario	1	90%			
[A.6] Abuso de privilegios de acceso	2	70%			
[A.7] Uso no previsto	1	80%			
[A.10] Alteración de secuencia	2	80%			
[A.11] Acceso no autorizado	1	90%	80%	80 %	90%
[A.14] Interceptación de información (escucha)	1	90%	70%		
[A.22] Manipulación de programas	1	80%			
[COM_Pstn] Red Telefónica	1				
[I.5] Avería de origen físico o lógico	2			40%	30%
[E.1] Errores de los usuarios	1	70%	80%		
[E.2] Errores del administrador	1			10%	10%
[E.4] Errores de configuración	2				
[E.8] Difusión de software dañino	1				
[E.9] Errores de [re-]encaminamiento	1			60 %	80%

[E.14] Escapes de información	1	80%	90%		
[E.20] Vulnerabilidades de los programas (software)	1				
[E.21] Errores de mantenimiento / actualización de programas (software)	2				
[A.4] Manipulación de la configuración	1	60%	60%	70 %	70%
[A.5] Suplantación de la identidad del usuario	2	70%	40%	80 %	70%
[A.6] Abuso de privilegios de acceso	1	70%	50%		
[A.7] Uso no previsto	2				
[A.10] Alteración de secuencia	1	80%			
[A.11] Acceso no autorizado	1	80%	80%	90%	
[A.14] Interceptación de información (escucha)	1	70%			30%
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**
[COM_Micro] Microondas					
[I.5] Avería de origen físico o lógico	1	80%			20%
[E.1] Errores de los usuarios	2	70%	80%	90%	

[E.2] Errores del administrador	1	90%			10%
[E.4] Errores de configuración	1	100%			
[E.8] Difusión de software dañino	2	80%			
[E.9] Errores de [re-]encaminamiento	1	80%			60%
[E.14] Escapes de información	1		80%	90%	
[E.20] Vulnerabilidades de los programas (software)	1	70%			
[E.21] Errores de mantenimiento / actualización de programas (software)	1	80%			
[A.4] Manipulación de la configuración	2	60%	60%	70 %	70%
[A.5] Suplantación de la identidad del usuario	1	70%	40%	80 %	70%
[A.6] Abuso de privilegios de acceso	2	70%	50%		
[A.7] Uso no previsto	1				
[A.10] Alteración de secuencia	2	80%			
[A.11] Acceso no autorizado	1	80%	80%	90%	
[A.14] Interceptación de información (escucha)	1	70%			30%
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**

[COM_Pstn] Red Telefónica					
[I.5] Avería de origen físico o lógico	1	80%			20%
[E.1] Errores de los usuarios	2	70%	80%	90%	
[E.2] Errores del administrador	1	90%			10%
[E.4] Errores de configuración	1	100%			
[E.8] Difusión de software dañino	2	80%			
[E.9] Errores de [re-]encaminamiento	1	80%			60%
[E.14] Escapes de información	1		80%	90%	
[E.20] Vulnerabilidades de los programas (software)	1	70%			
[E.21] Errores de mantenimiento / actualización de programas (software)	1	80%			
[A.4] Manipulación de la configuración	2	60%	60%	70 %	70%
[A.5] Suplantación de la identidad del usuario	1	70%	40%	80 %	70%
[A.6] Abuso de privilegios de acceso	2	70%	50%		
[A.7] Uso no previsto	1				
[A.10] Alteración de secuencia	2	80%			

[A.11] Acceso no autorizado	1	80%	80%	90%	
[A.14] Interceptación de información (escucha)	1	70%			30%
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**
[COM_Micro] Microondas					
[I.5] Avería de origen físico o lógico	1	80%			20%
[E.1] Errores de los usuarios	2	70%	80%	90%	
[E.2] Errores del administrador	1	90%			10%
[E.4] Errores de configuración	1	100%			
[E.8] Difusión de software dañino	2	80%			
[E.9] Errores de [re-]encaminamiento	1	80%			60%
[E.14] Escapes de información	1		80%	90%	
[E.20] Vulnerabilidades de los programas	1	70%			
[E.21] Errores de mantenimiento / actualización de programas (software)	1	80%			
[A.4] Manipulación de la configuración	2	60%	60%	70 %	70%
[A.5] Suplantación de la identidad del usuario	1	70%	40%	80 %	70%

[A.6] Abuso de privilegios de acceso	2	70%	50%		
[A.7] Uso no previsto	1				
[A.10] Alteración de secuencia	2	80%			
[A.11] Acceso no autorizado	1	80%	80%	90%	
[A.14] Interceptación de información (escucha)	1	70%			30%
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**
[COM_Lan] Red Local					
[I.5] Avería de origen físico o lógico	1	80%			20%
[E.1] Errores de los usuarios	2	70%	80%	90%	
[E.2] Errores del administrador	1	90%			10%
[E.4] Errores de configuración	1	100%			
[E.8] Difusión de software dañino	2	80%			
[E.9] Errores de [re-]encaminamiento	1	80%			60%
[E.14] Escapes de información	1		80%	90%	
[E.20] Vulnerabilidades de los programas (software)	1	70%			

[E.21] Errores de mantenimiento / actualización de programas (software)	1	80%			
[A.4] Manipulación de la configuración	2	60%	60%	70 %	70%
[A.5] Suplantación de la identidad del usuario	1	70%	40%	80 %	70%
[A.6] Abuso de privilegios de acceso	2	70%	50%		
[A.7] Uso no previsto	1				
[A.10] Alteración de secuencia	2	80%			
[A.11] Acceso no autorizado	1	80%	80%	90%	
[A.14] Interceptación de información (escucha)	1	70%			30%
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**
[COM_Internet] Internet					
[I.5] Avería de origen físico o lógico	1	80%			20%
[E.1] Errores de los usuarios	2	70%	80%	90%	
[E.2] Errores del administrador	1	90%			10%
[E.4] Errores de configuración	1	100%			
[E.8] Difusión de software dañino	2	80%			

[E.9] Errores de [re-]encaminamiento	1	80%			60%
[E.14] Escapes de información	1		80%	90%	
[E.20] Vulnerabilidades de los programas (software)	1	70%			
[E.21] Errores de mantenimiento / actualización de programas (software)	1	80%			
[A.4] Manipulación de la configuración	2	60%	60%	70 %	70%
[A.5] Suplantación de la identidad del usuario	1	70%	40%	80 %	70%
[A.6] Abuso de privilegios de acceso	2	70%	50%		
[A.7] Uso no previsto	1				
[A.10] Alteración de secuencia	2	80%			
[A.11] Acceso no autorizado	1	80%	80%	90%	
[A.14] Interceptación de información (escucha)	1	70%			30%
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**
[COM_Boqui] Radios Boquitoqui					
[I.5] Avería de origen físico o lógico	1	50%			10%

[E.1] Errores de los usuarios	2	40%			
[E.2] Errores del administrador	1	40%			10%
[E.4] Errores de configuración	1	50%			
[E.8] Difusión de software dañino					
[E.9] Errores de [re-]encaminamiento	1	60%			20%
[E.14] Escapes de información	1		40%	60%	
[E.20] Vulnerabilidades de los programas (software)					
[E.21] Errores de mantenimiento / actualización de programas (software)	1	30%			
[A.4] Manipulación de la configuración	2	60%	60%	70 %	70%
[A.5] Suplantación de la identidad del usuario	1	40%	40%	40 %	30%
[A.6] Abuso de privilegios de acceso	2	40%	10%		
[A.7] Uso no previsto	1				
[A.10] Alteración de secuencia	2	20%			
[A.11] Acceso no autorizado	1	20%	40%	30%	
[A.14] Interceptación de información (escucha)	1	30%			30%
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**

[SI_Usb] Dispositivos USB					
[N.1] Fuego	1	100%			
[N.2] Daños por agua	2	70%			
[N.*] Desastres naturales	1	90%			
[I.5] Avería de origen físico o lógico	1	90%			
[I.6] Corte del suministro eléctrico	2	100%			
[I.7] Condiciones inadecuadas de temperatura y/o humedad	1	80%			
[I.10] Degradación de los soportes de almacenamiento de la información	1	70%			
[A.7] Uso no previsto	1	70%			
[A.11] Acceso no autorizado	1	80%			
[A.25] Robo	2	100 %			
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**
[SI_Dvd] Dvd / Cd´s					
[N.1] Fuego	1	100%			
[N.2] Daños por agua	2	60%			
[N.*] Desastres naturales	1	90%			
[I.5] Avería de origen físico o lógico	1	80%			

[I.6] Corte del suministro eléctrico	2				
[I.7] Condiciones inadecuadas de temperatura y/o humedad	1	80%			
[I.10] Degradación de los soportes de almacenamiento de la información	1	60%			
[A.7] Uso no previsto	1	50%			
[A.11] Acceso no autorizado	1	70%			
[A.25] Robo	2	100 %			
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**
[SI_Tape] Cintas Magnéticas					
[N.1] Fuego	1	100%			
[N.2] Daños por agua	2	70%			
[N.*] Desastres naturales	1	90%			
[I.5] Avería de origen físico o lógico	1	90%			
[I.6] Corte del suministro eléctrico	2	100%			
[I.7] Condiciones inadecuadas de temperatura y/o humedad	1	80%			
[I.10] Degradación de los soportes de almacenamiento de la información	1	70%			
[A.7] Uso no previsto	1	70%			
[A.11] Acceso no autorizado	1	80%			
[A.25] Robo	2	100			

		%			
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**
[SI_Disk] Discos Duros					
[N.1] Fuego	1	100%			
[N.2] Daños por agua	2	80%			
[N.*] Desastres naturales	1	90%			
[I.5] Avería de origen físico o lógico	1	90%			
[I.6] Corte del suministro eléctrico	2	100%			
[I.7] Condiciones inadecuadas de temperatura y/o humedad	1	80%			
[I.10] Degradación de los soportes de almacenamiento de la información	1	70%			
[A.7] Uso no previsto	1	70%			
[A.11] Acceso no autorizado	1	80%			
[A.25] Robo	2	100 %			
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**
[AUX_Ups] Sistema Alimentación Interrumpida					
[N.1] Fuego	1	100%			

[N.2] Daños por agua	2	90%			
[N.*] Desastres naturales	1	100%			
[I.5] Avería de origen físico o lógico	1	90%			
[I.6] Corte del suministro eléctrico	2	80%			
[I.7] Condiciones inadecuadas de temperatura y/o humedad	1	80%			
[A.7] Uso no previsto	1	70%			
[A.11] Acceso no autorizado	1	80%			
[A.25] Robo	2	100 %			
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**
[AUX_Gen] Generadores Eléctricos					
[N.1] Fuego	1	100%			
[N.2] Daños por agua	2	90%			
[N.*] Desastres naturales	1	100%			
[I.5] Avería de origen físico o lógico	1	90%			
[I.6] Corte del suministro eléctrico	2	80%			
[I.7] Condiciones inadecuadas de temperatura y/o humedad	1	80%			
[A.7] Uso no previsto	1	70%			
[A.11] Acceso no autorizado	1	70%			
[A.25] Robo	2	100			

		%			
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**
[AUX_Ac] Equipos de Climatización					
[N.1] Fuego	1	100%			
[N.2] Daños por agua	2	90%			
[N.*] Desastres naturales	1	100%			
[I.5] Avería de origen físico o lógico	1	90%			
[I.6] Corte del suministro eléctrico	2	80%			
[I.7] Condiciones inadecuadas de temperatura y/o humedad	1	80%			
[A.7] Uso no previsto	1	70%			
[A.11] Acceso no autorizado	1	80%			
[A.25] Robo	2	100 %			
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**
[AUX_Cabling] Cableado					
[N.1] Fuego	1	100%			
[N.2] Daños por agua	2	30%			
[N.*] Desastres naturales	1	80%			

[I.5] Avería de origen físico o lógico	1	90%			
[I.6] Corte del suministro eléctrico	2	80%			
[I.7] Condiciones inadecuadas de temperatura y/o humedad	1	40%			
[A.7] Uso no previsto	1	70%			
[A.11] Acceso no autorizado	1	60%			
[A.25] Robo	2	100 %			
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**
[P_Adm] Administrador del Sistemas					
[A.28] Indisponibilidad del personal	1	90%			
[A.30] Ingeniería social	2		100 %	100%	90%
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**
[P_Tec] Técnico de Sistemas					
[A.28] Indisponibilidad del personal	1	90%			
[A.30] Ingeniería social	2		100 %	100%	90%
Activo / Amenaza		**D**	**I**	**C**	**A_S**

	frecuencia				
[P_Adm] Administrador del Sistemas					
[A.28] Indisponibilidad del personal	1	90%			
[A.30] Ingeniería social	2		100 %	100%	90%
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**
[P_Dba] Administrador de bases de datos					
[A.28] Indisponibilidad del personal	1	90%			
[A.30] Ingeniería social	2		100 %	100%	90%
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**
[P_Adm] Administrador del Sistemas					
[A.28] Indisponibilidad del personal	1	90%			
[A.30] Ingeniería social	2		100 %	100%	90%
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**

[P_Desa] Desarrolladores					
[A.28] Indisponibilidad del personal	1	90%			
[A.30] Ingeniería social	2		100 %	100%	90%
Activo / Amenaza	**frecuencia**	**D**	**I**	**C**	**A_S**
[P_Adm] Coordinador de proyectos					
[A.28] Indisponibilidad del personal	1	90%			
[A.30] Ingeniería social	2		100 %	100%	90%

6. Políticas de Seguridad

	Fundación Universitaria Tecnológico Comfenalco	Versión: 1.0	Página 1
Responsable:	**Política de Seguridad de la Información - General**	Fecha: 21/11/2010	Fecha de divulgación:

Las políticas de seguridad informática son importantes y diferencian una empresa de otra ya que no todas tienen protegidos sus recursos ni utilizan buenas prácticas para la protección de estos. Es importante que los principios de la Política de Seguridad sean parte de la cultura organizacional.

Para esto, se asegura un compromiso manifiesto de la Dirección de la institución y de Unidades Organizativas para la difusión, consolidación y cumplimiento de la presente Política.

1. Objeto.

Proteger los recursos de información del Organismo y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

2. Alcance

Esta Política solo es aplicable al Departamento de Sistemas y por ende a sus recursos y a la totalidad de los procesos, ya sean internos o externos vinculados a cada una de ellas.

Además, se encuentra a disposición del público que la solicite y es revisada cuando así lo estima necesario.

1. Objetivo.

Definir las pautas generales para asegurar una adecuada protección de la información de los virus informáticos.

2. Responsables del cumplimiento:

Todo el personal de la organización y los terceros que interactúan de manera habitual u ocasional que acceda a información sensible, y/o a los recursos informáticos en el desarrollo de sus tareas habituales.

3. Definiciones

- Se debe implementar un sistema automático de control de antivirus para prevenir y eliminar las consecuencias de la acción de los virus informáticos.

- Estos programas deben ser instalados por el área de sistemas en los equipos centralizados de procesamiento y en las estaciones de trabajo.

- Mantener actualizado el software de manera periódica con las últimas versiones de estos, o en dado caso si hay una versión disponible más actualizada antes del

periodo estipulado para hacer la actualización descargarla e instalarla inmediatamente.

- Nunca descargar archivos de páginas con contenido o fuentes sospechosas.

- Siempre escanear unidades de disquete o USB antes de usarla, ya que estos son fuentes de virus.

- Hacer un back up de información importante para la empresa o la división, que contenga configuración del sistema, y guardar este en un lugar seguro.

- Deben utilizarse programas que monitoreen el accionar de los virus informáticos tanto para los mensajes como para los archivos adjuntos previamente a su ejecución

1. **Objetivo.**

   Definir las pautas generales para asegurar una adecuada protección de la información de la institución en el uso de los servicios de correo electrónico.

2. **Responsables del cumplimiento:**

   Todo el personal de la organización y los terceros que interactúan de manera habitual u ocasional que acceda a información sensible, y/o a los recursos informáticos en el desarrollo de sus tareas habituales.

3. **Contenido**

   - El usuario de correo electrónico debe utilizar este servicio con criterios de racionalidad, seguridad, para las labores propias de su función y en beneficio de la institución.
     Este no debe utilizarse para ningún otro fin.

   - Cada persona es responsable del contenido del mensaje enviado como de cualquier otra información adjunta al mismo.

- El contenido de los mensajes de correo debe ser considerado confidencial; solo se pierde este carácter en casos de investigaciones legales o análisis de incidentes relacionados con seguridad informática.

- Debe limitarse a los usuarios el acceso a sitios que pudieran perjudicar los intereses y la reputación de la compañía, específicamente no deben accederse a aquellos sitios que contienen información pornográfica, racismo, violencia o material potencialmente ofensivo contrario a los intereses de la institución.

- Todos los accesos pueden ser objetos de monitoreo y conservación permanente por parte de la compañía.

1. Objetivo.

Definir las pautas generales para asegurar una adecuada recuperación de la información en caso de ser necesario, a través de la metodología definida para efectuar copias de respaldo.

2. Responsables del cumplimiento.

El personal del área de sistema que sea responsable de la generación y restauración de las copias de respaldo.

3. Contenido

- Es responsabilidad de los operadores de los sistemas para efectuar los procesos de generación y restauración de copias de respaldo para los equipos de procesamiento centralizado.
- Se deberá efectuar la generación de la copia de respaldo para el total de la información de los equipos centrales de procesamiento en forma diaria, conservando adicionalmente una copia extra en edificio externo semanalmente.
- Se debe analizar y definir los soportes magnéticos más adecuados sobre los que se deben efectuar Las copias de respaldo, como son unidades ópticas, discos ópticos o similares.
- Se debe realizar pruebas periódicas de recuperación desde los soportes físicos, para verificar la correcta recuperación de la información.

- Se debe llevar en forma permanente un inventario de los soportes existentes, su contenido y el lugar donde están almacenado.

1. **Objetivo.**

   Definir las pautas que permiten asegurar que todos los usuarios tienen exclusivamente el acceso necesario a la información para el desarrollo de sus tareas habituales en la institución**.**

2. **Responsables del cumplimiento.**

   El personal de sistema delegado para dar de alta o de baja o modificación de los perfiles de un usuario.

3. **Contenido.**

   - La creación modificación y la baja de un perfil de usuario debe ser tarea del administrador de sistema.
   - Los usuarios no deben tener acceso a todos los recurso, solo deben acceder a lo que estén autorizado.
   - Los accesos deben seguir el principio de “camino forzoso “permitiendo a el usuario acceder exclusivamente a los recursos para los cuales tiene permisos sin acceder por la misma vía a otros recursos.
   - La solicitud de accesos puede ser realizada por cualquier usuario a través de un formulario especifico en papel o utilizando el correo electrónico.

- El administrador de sistema debe efectuar el análisis correspondiente y proceder a la definición técnica de los permisos solicitados a los recursos informáticos.

- Cada persona debe tener una cuenta personal de usuario para acceder a los recursos de la institución y es responsable por su correcto uso.

- El usuario debe definir una clave personal que se utilizara para comprobar la autenticidad de la persona responsable de cada cuenta de usuario.

1. **Objetivo**

   Definir las pautas generales para asegurar una adecuada protección física de los equipos y soportes de procesamiento, transmisión y conservación de la información de la compañía.

2. **Responsable del cumplimiento**

   Personal del área de sistema responsable de la seguridad de los centros de cómputos.

3. **Contenido**

- El acceso físico a los ambientes donde se encuentre los equipos debe ser limitado solo a personal autorizado.
- Se deberán utilizar dispositivos automáticos con calves de acceso para el ingreso a los centros de cómputo principales (cuarto de servidores, centro de telecomunicaciones).
- Se debe registrar en forma específica los ingresos de usuarios que no realicen tareas operativas habituales.
- Se debe evaluar el uso de sistema de monitoreo a través de cámara de video para el centro de cómputo.

- No deben ubicarse dentro de los centros de cómputos recursos de uso habitual por parte del personal (impresoras, suministros informáticos).
- Los equipos deben contar con unidades de suministro continuo de energía y estabilizadores de tensión.

- La división de sistema debe mantener los inventarios detallados de los recursos de hardware instalados dentro y fuera del centro de cómputo.

- Las copias de respaldo deben conservarse en armarios ignífugos y de acceso restringido y con la respectiva identificación.

1. Objetivo

Definir las pautas generales para que todo software que sea utilizado por el personal de la institución en el desarrollo de sus tareas tenga la licencia de uso legal correspondiente.

2. Responsable del cumplimiento

Todo el personal de la organización y los terceros que interactúan de manera habitual u ocasional que acceda a información sensible, y/o a los recursos informáticos en el desarrollo de sus tareas habituales.

3. Contenido

- Todo software que se utilice en los equipos informáticos debe ser adquirido a nombre de la compañía, y debe contar obligatoriamente con una licencia legal para su utilización excepto aquellos que sean de uso libre.

- El área de sistemas es responsable de la homologación inicial, instalación o eliminación de cualquier tipo de software en los equipos centralizados de procesamiento, o en cualquiera de los equipos conectados o no a la red de la institución.
- Los usuarios no deben instalar ningún software en cualquiera de los equipos informáticos de la institución, que estén o no conectados a las redes bajo ningún concepto, sin la autorización específica del área de sistemas, a pesar que sea de uso libre.

- En las donaciones de equipos informáticos deben identificarse detalladamente en la documentación respiratoria, todos los recursos de software que se incluyen en la operación.

- Debe existir un inventario actualizado permanente de las versiones de software instaladas en todos los equipos informáticos de la institución.

1. **Objetivo**

   Definir las pautas generales para asegurar una adecuada protección de la información en los procesos de transmisión y recepción de datos en las redes internas y externas de la institución.

2. **Responsables del cumplimiento**

   Todo el personal de la organización y los terceros que interactúan de manera habitual u ocasional que acceda a información sensible, y/o a los recursos informáticos en el desarrollo de sus tareas habituales.

3. **Contenido**

   - Verificar que exista adecuados mecanismo de encriptación para la información sensible propia de los sistemas (contraseñas, base de datos de seguridad o similares).
   - Utilizar sistemas de detección de intrusos que permitan la detección de posibles ataques y tomen acciones automáticas para prevenirlos.
   - Asegurarse que todas las conexiones externas con la red interna de la compañía se realicen a través de puntos adecuadamente controlados.
   - El origen de todas las conexione remotas deben ser autenticadas utilizando un nivel aceptado de autenticación.

- Los accesos externos deben ser registrados a fin de determinar posibles intentos de accesos no autorizados.
- Debe incluirse en los contratos con los proveedores la utilización de otra ruta alternativa ante interrupción en los servicios de comunicaciones.

1. **Objetivo**

   Definir las pautas generales para asegurar un adecuado manejo de los activos al momento de hacer una adquisición, cambio o actualización de sus partes.

2. **Responsables del cumplimiento**

   El personal de la organización responsable de adquirir los equipos de hardware y la manipulación técnica de estos.

3. **Contenido**

   - Cualquier cambio que se requiera realizar en los equipos de cómputo de la entidad (cambios de procesador, adición de memoria o tarjetas) debe tener previamente una evaluación técnica y autorización del área responsable.
   - La reparación técnica de los equipos, que implique la apertura de los mismos, únicamente puede ser realizada por el personal autorizado.
   - Los equipos de microcomputadores (PC, servidores, LAN etc.) no deben moverse o reubicarse sin la aprobación previa del administrador, jefe o coordinador del área involucrada.

- Los empleados deben reportar a los entes pertinentes de la entidad, sobre daños o pérdida del equipo que tengan a su cuidado y sea propiedad de la entidad. La intervención directa para reparar el equipo debe estar expresamente prohibida. La entidad debe proporcionar personal interno o externo para la solución del problema reportado.

1. **Objetivo**

   Definir las pautas generales para asegurar un adecuado manejo de los activos al momento de realizar eventos, y asegurar el bienestar del personal.

2. **Responsables del cumplimiento**

   El personal de la organización responsable de realizar las reuniones o capacitaciones en la institución.

3. **Contenido**

- Los visitantes deben permanecer escoltados y portar un distintivo o escarapela claramente visible, y las personas que laboran para la entidad que requieran ingresar a áreas críticas también deben permanecer escoltados, además, tanto los visitantes como los empleados mencionados únicamente deben tener a la información y recursos necesarios para el desarrollo de sus actividades.
- En el evento que los funcionarios dejen de tener vínculos laborales con la entidad todos sus códigos de acceso deben ser cambiados o desactivados, Además, en caso de pérdida de la escarapela o tarjeta de acceso también deben desactivarse dichos códigos.
- Se debe mantener el registro de acceso del personal autorizado y de ingresos con el objeto de facilitar procesos de investigación.

- Como mecanismo de prevención todos los empleados y visitantes no deben comer, fumar o beber en el centro de cómputo o instalaciones con equipos tecnológicos, al hacerlo estarían exponiendo los equipos a daños eléctricos como a riesgos de contaminación sobre los dispositivos de almacenamiento.
- Todos los sistemas de control de acceso deben ser monitoreados permanentemente.

7. CONTROLES

A continuación se enuncian los controles a aplicar en cada una de las políticas de seguridad diseñadas a la **Fundación Universitaria Tecnológico Comfenalco**.

Para ver la guía de controles puede dirigirse al Anexo. **ACTIVO**	**AMENAZA**	**CONTROL**
Datos	**[E1]**	**A.8.2** Que todos los empleados, contratistas y usuarios de terceros conozcan las amenazas y problemas de seguridad de la información, así como sus responsabilidades y obligaciones, y estén capacitados para apoyar la política de seguridad de la organización en el curso de su trabajo normal, y reducir el riesgo de error humano. **A.10.10.5 Registros de fallas** Las fallas deberán registrarse, analizarse y deberán tomarse las medidas adecuadas. **A.10.10.1 Registros de auditoria** Los registros de auditoría que graban las actividades, excepciones, y eventos de seguridad de la información de los usuarios deberán existir y mantenerse durante un período convenido para asistir futuras investigaciones y en el monitoreo de control de acceso.
	[E2]	**A.10.10.1 Registros de auditoria** Los registros de auditoría que graban las actividades, excepciones, y eventos de seguridad de la información de los usuarios deberán existir y mantenerse durante un período convenido para asistir futuras investigaciones y en el monitoreo de control de acceso. **A.13.2.1 Responsabilidades y procedimientos** Deberán establecerse responsabilidades y procedimientos de gerencia para asegurar la respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información. **A.13.2.2 Aprendiendo de los incidentes de seguridad de la información** Deberán existir mecanismos en ejecución que permitan cuantificar y monitorear los tipos, volúmenes, y costos de los incidentes de

		seguridad de la información. **A.13.2.3 Recolección de evidencia** Cuando la acción de seguimiento contra una persona u organización después de un incidente de seguridad de la información involucre medidas legales (ya sea civil o penal), deberá recolectarse, retenerse y presentarse evidencia de conformidad con las reglas de prueba establecidas en la legislación pertinente. **A.14.1.1 Incluir seguridad de la información en el proceso de gestión de la continuidad de negocios** Deberá desarrollarse y mantenerse un proceso gestionado de continuidad del negocio en toda la organización, que se encargue de los requerimientos de seguridad de la información necesarios para la continuidad del negocio de la organización. **A.14.1.2 Continuidad de negocios y evaluación de riesgos** Deberá identificarse los eventos que pueden causar interrupciones a los procesos de negocios, junto con la probabilidad e impacto de tales interrupciones y sus consecuencias para la seguridad de la información. **A.14.1.3 Desarrollo e implementación de planes de continuidad incluyendo seguridad de la información**. Deberá prepararse e implementarse planes para mantener o restaurar las operaciones y asegurar la disponibilidad de información al nivel requerido y en las escalas de tiempo requeridas luego de la interrupción o falla de procesos de negocios críticos. **A.14.1.4 Marco de planeamiento de la continuidad de los negocios** Deberá mantenerse un solo marco de planes de continuidad de negocios para asegurar que todos los planes sean concordantes, para enfocar de modo uniforme los requerimientos de seguridad de la información, y para identificar prioridades de prueba y mantenimiento. **A.14.1.5 Prueba, mantenimiento y reevaluación de planes de continuidad de los negocios** Los planes de continuidad de los negocios deberán probarse y actualizarse regularmente para asegurar que estén al día y sean efectivos. **A.10.1.2 Monitoreo del uso del sistema** Deberán establecerse procedimientos para monitorear el uso de las instalaciones de procesamiento de información, y los resultados de las actividades de monitoreo deberán revisarse regularmente. **A.10.1.3 Separación de deberes** Los deberes y áreas de responsabilidad deberán separarse para reducir las oportunidades de modificación no autorizada o inadvertida o mal uso de los activos de la organización. **A.10.1.4 Separación de instalaciones de desarrollo, prueba y**

		operaciones Las instalaciones de desarrollo, prueba y operaciones deberán separarse para reducirlos riesgos de acceso o cambios no autorizados al sistema operativo. **A.10.2.1 Entrega de servicios** Se deberá asegurar que los controles de seguridad, definiciones de servicio y niveles de entrega incluidos en el convenio de servicios por terceros, sean implementados, operados y mantenidos por el tercero. **A.10.2.2 Monitoreo y revisión de servicios de terceros** Los servicios, informes y registros suministrados por terceros deberán monitorearse y revisarse periódicamente, y efectuarse auditorias regularmente. **A.10.2.3 Gestión de cambios en terceros** Deberá gestionarse los cambios en la provisión de servicios, incluyendo el mantenimiento y mejora de las políticas, procedimientos y controles de seguridad de información existentes, tomando en cuenta la criticabilidad de los sistemas y procesos de negocios involucrados y la reevaluación de los riesgos **A.10.3.1 Gestión de la capacidad** El uso de los recursos debe monitorearse y refinarse, y deben hacerse proyecciones de las necesidades de capacidad futuras para asegurar el desempeño requerido del sistema. **A.10.3.2 Aceptación de sistemas** Deberán establecerse criterios de aceptación de nuevos sistemas de información, actualizaciones y nuevas versiones, y realizarse pruebas adecuadas de los sistemas durante el desarrollo y antes de la aceptación. **A.10.4.1 Controles contra código malicioso** Deberá implementarse controles de detección, prevención y recuperación para protegerse contra código malicioso así como procedimientos adecuados de concientización de usuarios. **A.10.4.2 Controles contra código móvil** Cuando el uso de código móvil está autorizado, la configuración deberá asegurar que el código móvil autorizado opere según una política de seguridad claramente definida, y se impedirá la ejecución de código móvil no autorizado **A.10.5 Respaldo** Objetivo: Mantener la integridad y disponibilidad de la información y de las instalaciones de procesamiento de información **A.10.5.1 Respaldo de la información** Deberán hacerse copias de respaldo de la información y el “software”,

		y probarse periódicamente según la política de respaldo convenida. **A.10.6 Gestión de seguridad de redes** Objetivo: Asegurar la protección de la información en redes y la protección de la infraestructura de soporte **A.10.6.1** Controles de redes **A.10.6.2** Las redes deberán manejarse y controlarse debidamente, a fin de protegerse de amenazas, y mantener la seguridad de los sistemas y aplicaciones que usan la red, incluyendo la información en tránsito. **A.10.7.3 Procedimientos de manipulación de información** Deberán establecerse procedimientos para la manipulación y almacenamiento de información, a fin de protegerla de la divulgación no autorizada o del mal uso.
	[E4]	**A.10.1.1 Procedimientos operativos** Los procedimientos operativos deberán documentarse, mantenerse y ponerse a disposición de todos los usuarios que los necesiten. **A.13.2.1 Responsabilidades y procedimientos** Deberán establecerse responsabilidades y procedimientos de gerencia para asegurar la respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información. **A.10.10.5 Registro de fallas** Las fallas deberán registrarse, analizarse y deberán tomarse las medidas
	[E15] **[E16]**	**A.11.6.1 Restricción del acceso a la información** El acceso por los usuarios a las funciones del sistema de información y aplicaciones deberá restringirse según la política de control de acceso definida. **A.12.2.1 Validación de datos de entrada** Los datos de entrada para aplicaciones deberán validarse para asegurar que estos datos son correctos y adecuados. **A.12.2.3 Integridad del mensaje** Deberán identificarse los requerimientos para asegurar la autenticidad y proteger la integridad del mensaje en las aplicaciones, así como identificarse e implementarse los controles apropiados. **A.6.1.5 Convenios de confidencialidad** Los requerimientos de convenios de confidencialidad o de no divulgación n que reflejen las necesidades de la organización n para protección de la información deberán ser identificados y revisados periódicamente.

		A.8.2.3 Proceso disciplinario Habrá un proceso disciplinario formal para los empleados que hayan cometido una violación de seguridad. **A.10.1.1 Procedimientos operativos** Los procedimientos operativos deberán documentarse, mantenerse y ponerse a disposición de todos los usuarios que los necesiten.
	[E17]	**A.10.5 Respaldo** Objetivo: Mantener la integridad y disponibilidad de la información y de las instalaciones de procesamiento de información **[A.10.5.1]** Respaldo de la información Deberán hacerse copias de respaldo de la información y el "software", y probarse periódicamente según la política de respaldo convenida. **A.12.3 Controles criptográficos** Objetivo: Proteger la confidencialidad, autenticidad o integridad de la información por medios criptográficos. **[A.12.3]** Política sobre el uso de controles criptográficos Deberá prepararse e implementarse una política sobre el uso de controles criptográficos para protección de la información. **A.10.1 Procedimientos y responsabilidades operativas** Objetivo: Asegurar la correcta y segura operación de los recursos de procesamiento de información. **[A.10.1.1]** Procedimientos operativos documentados Los procedimientos operativos deberán documentarse, mantenerse y ponerse a disposición de todos los usuarios que los necesiten. **[A.8.2.3]** Proceso disciplinario Habrá un proceso disciplinario formal para los empleados que hayan cometido una violación de seguridad.
	[E19]	**A.15.1 Cumplimiento de requisitos legales** Objetivo: Evitar violaciones de cualquier ley u obligación estatutaria, de regulación o contractual, y de cualquier requisito de seguridad. **[A.15.1.4] Protección de datos y privacidad de la información personal** La protección y privacidad de los datos deberá asegurarse como sea necesario mediante la legislación y reglamentos pertinentes y, si corresponde, mediante las cláusulas contractuales. **[A.6.1.5] Convenios de confidencialidad** Los requerimientos de convenios de confidencialidad o de no divulgación que reflejen

		Las necesidades de la organización para protección de la información deberán ser identificadas y revisadas periódicamente.
	[A11]	**A.9.1 Áreas aseguradas** Objetivo: Impedir el acceso físico no autorizado, daños e interferencias en los locales y la información de la organización. **[A.9.1.2] Controles de ingreso físico** Las áreas seguras deberán protegerse mediante controles de ingreso adecuados para asegurar que sólo se permita el acceso del personal autorizado. **[A.9.1.5] Trabajo en áreas aseguradas** Las áreas seguras deberán protegerse mediante controles de ingreso adecuados para asegurar que sólo se permita el acceso del personal autorizado. **[A.9.1.1] Perímetro de seguridad físico** Perímetros de seguridad (barreras tales como muros, puertas controladas por tarjeta o recepcionistas) deberán utilizarse para proteger las áreas que contienen información y las instalaciones de procesamiento de información. **[A.10.1.4] Separación de instalaciones de desarrollo, prueba y operaciones** Las instalaciones de desarrollo, prueba y operaciones deberán separarse para reducirlos riesgos de acceso o cambios no autorizados al sistema operativo. **A.11.2 Gestión del acceso de usuarios** Objetivo: Asegurar el acceso de usuarios autorizados e impedir el acceso no autorizado a los sistemas de información. **[A.11.2.1] Inscripción de usuarios** Deberá haber un procedimiento formal de inscripción y des-inscripción de usuarios para otorgar y revocar el acceso a todos los sistemas y servicios de información. **[A.11.1.1] Política de control del acceso** Se deberá establecer, documentar, y revisar una política de control del acceso basada en los requisitos de negocios y de seguridad para el acceso. **A.11.4 Control del acceso a redes** Objetivo: Prevenir el acceso no autorizado a los servicios de redes. **[A.11.4.1]** Política sobre uso de servicios de redes A los usuarios sólo deberá dárseles acceso a los servicios que están específicamente autorizados para usar. **A.11.6 Control del acceso a aplicación e información** Objetivo: Impedir el acceso no autorizado a la información contenida en los sistemas de aplicaciones

		[A.11.6.1] Restricción del acceso a la información El acceso por los usuarios a las funciones del sistema de información y aplicaciones deberá restringirse según la política de control de acceso definida. **A.10.1 Procedimientos y responsabilidades operativas** Objetivo: Asegurar la correcta y segura operación de los recursos de procesamiento de información. **[A.10.1.1]Procedimientos operativos documentados** Los procedimientos operativos deberán documentarse, mantenerse y ponerse a disposición de todos los usuarios que los necesiten. **A.10.10 Monitoreo** Objetivo: Detectar actividades de procesamiento de información no autorizadas **[A.10.10.1]** Registros de auditoria Los registros de auditoría que graban las actividades, excepciones, y eventos de seguridad de la información de los usuarios deberán existir y mantenerse durante un período convenido para asistir futuras investigaciones y en el monitoreo de control de acceso. **[A.10.10.4]** Registros de Administrador y operador Se deberán registrar las actividades del administrador del sistema y del operador del sistema. **[A.10.10.6]** Sincronización de reloj Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o dominio de seguridad, deberán sincronizarse con una fuente de tiempo exacto convenida. **A.12.1 Requisitos de seguridad para sistemas de información** Objetivo: Exigir que la seguridad sea parte integral de los sistemas de información **A.12.4 Seguridad de archivos del sistema** Objetivo: Establecer la seguridad de los archivos del sistema **[A.12.4.3]** Control del acceso a código fuente de programas Deberá restringirse el acceso al código fuente de programas. **A.12.1 Requisitos de seguridad para sistemas de información** Objetivo: Exigir que la seguridad sea parte integral de los sistemas de información Los enunciados de requisitos de negocios para nuevos sistemas de información, o para mejoras de sistemas de información existentes, deberán especificar los requisitos para controles de seguridad.

		[A.12.2.1] Análisis y especificación de requisitos de seguridad Los enunciados de requisitos de negocios para nuevos sistemas de información, o para mejoras de sistemas de información existentes, deberán especificar los requisitos para controles de seguridad. **[A.8.3] Terminación o cambio de empleo** Objetivo: Asegurar que los empleados, contratistas y usuarios de terceros salgan de una organización o cambien de empleo en forma ordenada. **A.13.2 Gestión de incidentes y mejoras de seguridad de la información** Objetivo: Verificar que se aplique un enfoque uniforme y efectivo a la gestión de la seguridad de la información. **[A.13.2.3] Recolección de evidencia** Cuando la acción de seguimiento contra una persona u organización después de un incidente de seguridad de la información involucre medidas legales (ya sea civil o penal), deberá recolectarse, retenerse y presentarse evidencia de conformidad con las reglas de prueba establecidas en la legislación pertinente. **A.15.1 Cumplimiento de requisitos legales** Objetivo: Evitar violaciones de cualquier ley u obligación estatutaria, de regulación o contractual, y de cualquier requisito de seguridad. **[A.15.1.1] Identificación de la legislación aplicable** Deberá definirse, documentarse y mantenerse al día explícitamente todos los requisitos estatutarios, de regulación y contractuales pertinentes y el enfoque de la organización para cumplirlos, para cada sistema de información en la organización.
	[A15] **[A16]** **[A17]**	**A.11.6 Control del acceso a aplicación e información** Objetivo: Impedir el acceso no autorizado a la información contenida en los sistemas de aplicaciones **[A.11.6.1]** El acceso por los usuarios a las funciones del sistema de información y aplicaciones deberá restringirse según la política de control de acceso definida. **[A.10.7.4]** Seguridad de la documentación del sistema Deberá protegerse la documentación del sistema contra el acceso no autorizado **[A.10.8.3]** Medios físicos en tránsito Los medios que contengan información deberán protegerse contra el acceso no autorizado, el mal uso o corrupción durante su transporte más allá de los límites físicos de una organización. **A.10.10 Monitoreo**

		Objetivo: Detectar actividades de procesamiento de información no autorizadas **[A.10.10.3]** Protección de la información de registro Las instalaciones de registro y la información de registro deberán protegerse contra las alteraciones y el acceso no autorizado. **A.11.4 Control del acceso a redes** Objetivo: Prevenir el acceso no autorizado a los servicios de redes. **[A.11.4.1]** Política sobre uso de servicios de redes A los usuarios sólo deberá dárseles acceso a los servicios que están específicamente autorizados para usar. **A.10.5 Respaldo** Objetivo: Mantener la integridad y disponibilidad de la información y de las instalaciones de procesamiento de información **[A.10.5.1] Respaldo de la información** Deberán hacerse copias de respaldo de la información y el "software", y probarse periódicamente según la política de respaldo convenida. **A.6.1 Organización interna** Objetivo: Gestionar la seguridad de la información dentro de la organización. **[A.6.1.5]** Convenios de confidencialidad Los requerimientos de convenios de confidencialidad o de no divulgación que reflejen Las necesidades de la organización para protección de la información deberán ser identificadas y revisadas periódicamente. **A.10.1 Procedimientos y responsabilidades operativas** Objetivo: Asegurar la correcta y segura operación de los recursos de procesamiento de información. **[A.10.1.1]** Procedimientos operativos documentados Los procedimientos operativos deberán documentarse, mantenerse y ponerse a disposición de todos los usuarios que los necesiten. **[A.12.3] Controles criptográficos** Objetivo: Proteger la confidencialidad, autenticidad o integridad de la información por medios criptográficos.
	[E18]	**A.12.2 Procesamiento correcto en aplicaciones** Objetivo: Prevenir errores, pérdidas, modificación no autorizada o mal uso de la información en aplicaciones **[A.12.2.1]** Validación de datos de entrada

		Los datos de entrada para aplicaciones deberán validarse para asegurar que estos datos son correctos y adecuados. **[A.6.1.5] Convenios de confidencialidad** Los requerimientos de convenios de confidencialidad o de no divulgación que reflejen Las necesidades de la organización para protección de la información deberán ser identificadas y revisadas periódicamente. **A.10.1 Procedimientos y responsabilidades operativas** Objetivo: Asegurar la correcta y segura operación de los recursos de procesamiento de información. **[A.10.1.1] Procedimientos operativos documentados** Los procedimientos operativos deberán documentarse, mantenerse y ponerse a disposición de todos los usuarios que los necesiten. **A.7.2 Clasificación de la información** Objetivo: Asegurar que la información reciba el nivel de protección adecuado. **[A.10.7.2]** Rotulación y manipulación de la información Deberá prepararse e implementarse un conjunto de procedimientos adecuados para la rotulación y manipulación de la información, de acuerdo al esquema de clasificación adoptado por la organización. **A.10.1 Procedimientos y responsabilidades operativas** Objetivo: Asegurar la correcta y segura operación de los recursos de procesamiento de información. **[A.10.1.1] Procedimientos operativos documentados** Los procedimientos operativos deberán documentarse, mantenerse y ponerse a disposición de todos los usuarios que los necesiten. **A.13.2 Gestión de incidentes y mejoras de seguridad de la información** Objetivo: Verificar que se aplique un enfoque uniforme y efectivo a la gestión de la seguridad de la información. **[A.13.2.3] Responsabilidades y procedimientos** Deberán establecerse responsabilidades y procedimientos de gerencia para asegurar la respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.
		[A.15.1.4] Protección de datos y privacidad de la información

	[A19]	La protección y privacidad de los datos deberá asegurarse como sea necesario mediante la legislación y reglamentos pertinentes y, si corresponde, mediante las cláusulas contractuales **[A.6.1.5] Convenios de confidencialidad** Los requerimientos de convenios de confidencialidad o de no divulgación que reflejen las necesidades de la organización para protección de la información deberán ser identificados y revisados periódicamente.
ACTIVO	**AMENAZA**	**CONTROL**
Soporte de Información		
	[I.10] **[A.11]**	**- [A.12.2.3] Integridad del mensaje** Deberán identificarse los requerimientos para asegurar la autenticidad y proteger la integridad del mensaje en las aplicaciones, así como identificarse e implementarse los controles apropiados. **-[A.6.1.5] Convenios de confidencialidad** Los requerimientos de convenios de confidencialidad o de no divulgación que reflejen las necesidades de la organización para protección de la información deberán ser identificados y revisados periódicamente. **- [A.10.1.1] Procedimientos operativos documentados** Los procedimientos operativos deberán documentarse, mantenerse y ponerse a disposición de todos los usuarios que los necesiten. **- [A.9.2.4] Mantenimiento del equipo** El equipo deberá mantenerse correctamente para asegurar su continua disponibilidad e integridad.
	[A.25]	**- [A.9.1.1] Perímetro de seguridad físico** Perímetros de seguridad (barreras tales como muros, puertas controladas por tarjeta o recepcionistas) deberán utilizarse para proteger las áreas que contienen información y las instalaciones de procesamiento de información.

		- [A.9.1.3] Aseguramiento de oficinas, cuartos e instalaciones Deberá diseñarse y aplicarse seguridad física para las oficinas, cuartos e instalaciones **- [A.9.1.5] Trabajo en áreas aseguradas** Las áreas seguras deberán protegerse mediante controles de ingreso adecuados para asegurar que s lo se permita el acceso del personal autorizado. **- [A.9.1.6] Acceso público, áreas de entrega y carga** Los puntos de acceso tales como las áreas de entrega y carga y otros puntos donde personas no autorizadas pueden ingresar a los locales deberán controlarse y, de ser posible, aislarse de las instalaciones de procesamiento de información para evitar el acceso no autorizado. **- [A.10.1.1] Procedimientos operativos documentados** Los procedimientos operativos deberán documentarse, mantenerse y ponerse a disposición de todos los usuarios que los necesiten. **- [A.8.2.3] Proceso disciplinario** Habrá un proceso disciplinario formal para los empleados que hayan cometido una violación de seguridad.
	[N.1] [N.2] [I.1]	**- [A.10.1.1] Procedimientos operativos documentados** Los procedimientos operativos deberán documentarse, mantenerse y ponerse a disposición de todos los usuarios que los necesiten. **- [A.15.2.1] Cumplimiento de las políticas y normas de seguridad** Los gerentes deberán asegurar que todos los procedimientos de seguridad dentro de sus áreas de responsabilidad se efectúan correctamente para lograr el cumplimiento de las políticas y normas de seguridad. **- [A.14.1] Aspectos de seguridad de la información en la gestión de la continuidad de negocios**

		Objetivo: Contrarrestar las interrupciones de las actividades de negocios y proteger los procesos de negocio críticos de los efectos de fallas o desastres mayores de los sistemas de información, y asegurar su oportuna reanudación. **- [A.9.1.4] Protección contra amenazas exteriores y ambientales** Deberá diseñarse y aplicarse protección física contra daños por incendio, inundación, terremoto, explosión, desorden civil, y otras formas de desastres.
	[I.6]	**- [A.9.2.2] Servicios de soporte** El equipo deberá estar protegido contra cortes de energía y otros trastornos ocasionados por fallas en los servicios de soporte. **- [A.10.1.1] Procedimientos operativos documentados** Los procedimientos operativos deberán documentarse, mantenerse y ponerse a disposición de todos los usuarios que los necesiten.
	[A.7]	**- [A.7.1.3] Uso aceptable de los activos** Deberán identificarse, documentarse e implementarse reglas para el uso aceptable de la información y de los activos relacionados con las instalaciones de procesamiento de información. **- [A.9.2.2] Servicios de soporte** El equipo deberá estar protegido contra cortes de energía y otros trastornos ocasionados por fallas en los servicios de soporte. **- [A.15.1.5] Prevención del mal uso de las instalaciones de procesamiento de información** A los usuarios se les deberá disuadir de utilizar las instalaciones de procesamiento de información para fines no autorizados.
		- [A.9.1.2] Controles de ingreso físico

	[A.11]	Las áreas seguras deberán protegerse mediante controles de ingreso adecuados para asegurar que s lo se permita el acceso del personal autorizado. **- [A.9.1.5] Trabajo en áreas aseguradas** Las áreas seguras deberán protegerse mediante controles de ingreso adecuados para asegurar que s lo se permita el acceso del personal autorizado. **- [A.9.1.1] Perímetro de seguridad físico** Perímetros de seguridad (barreras tales como muros, puertas controladas por tarjeta o recepcionistas) deberán utilizarse para proteger las áreas que contienen información y las instalaciones de procesamiento de información. **- [A.9.1.4] Protección contra amenazas exteriores y ambientales** Deberá diseñarse y aplicarse protección física contra daños por incendio, inundación, terremoto, explosión, desorden civil, y otras formas de desastres. **- [A.10.1.4] Separación de instalaciones de desarrollo, prueba y operaciones** Las instalaciones de desarrollo, prueba y operaciones deberán separarse para reducirlos riesgos de acceso o cambios no autorizados al sistema operativo. **- [A.11.4.1] Política sobre uso de servicios de redes** A los usuarios s lo deberá dárseles acceso a los servicios que están específicamente autorizados para usar. **-[A.8.3] Terminación o cambio de empleo** Objetivo: Asegurar que los empleados, contratistas y usuarios de terceros salgan de una organización o cambien de empleo en forma **- [A.13.2.3] Recolección de evidencia** Cuando la acción de seguimiento contra una persona u

		organización después de un incidente de seguridad de la información involucre medidas legales (ya sea civil o penal), deberá recolectarse, retenerse y presentarse evidencia de conformidad con las reglas de prueba establecidas en la legislación pertinente. **-[A.15.1] Cumplimiento de requisitos legales** Objetivo: Evitar violaciones de cualquier ley u obligación estatutaria, de regulación o contractual, y de cualquier requisito. **-[A.13]** Gestión de incidentes de seguridad de la información **- [A.9.1.5] Trabajo en áreas aseguradas** Las áreas seguras deberán protegerse mediante controles de ingreso adecuados para asegurar que s lo se permita el acceso del personal autorizado. **- [A.9.1.6] Acceso público, áreas de entrega y carga** Los puntos de acceso tales como las áreas de entrega y carga y otros puntos donde personas no autorizadas pueden ingresar a los locales deberán controlarse y, de ser posible, aislarse de las instalaciones de procesamiento de información para evitar el acceso no autorizado. **- [A.10.1.1] Procedimientos operativos documentados** Los procedimientos operativos deberán documentarse, mantenerse y ponerse a disposición de todos los usuarios que los necesiten. **- [A.8.2.3] Proceso disciplinario** Habrá un proceso disciplinario formal para los empleados que hayan cometido una violación de seguridad.
	[A.25]	**- [A.9.1.1] Perímetro de seguridad físico** Perímetros de seguridad (barreras tales como muros, puertas controladas por tarjeta o recepcionistas) deberán utilizarse para proteger las áreas que contienen información y las instalaciones de procesamiento de información. **- [A.9.1.2] Controles de ingreso físico**

		Las áreas seguras deberán protegerse mediante controles de ingreso adecuados para asegurar que s lo se permita el acceso del personal autorizado. **- [A.9.1.3] Aseguramiento de oficinas, cuartos e instalaciones** Deberá diseñarse y aplicarse seguridad física para las oficinas, cuartos e instalaciones **- [A.9.1.5] Trabajo en áreas aseguradas** Las áreas seguras deberán protegerse mediante controles de ingreso adecuados para asegurar que s lo se permita el acceso del personal autorizado. **- [A.9.1.6] Acceso público, áreas de entrega y carga** Los puntos de acceso tales como las áreas de entrega y carga y otros puntos donde personas no autorizadas pueden ingresar a los locales deberán controlarse y, de ser posible, aislarse de las instalaciones de procesamiento de información para evitar el acceso no autorizado. **- [A.10.1.1] Procedimientos operativos documentados** Los procedimientos operativos deberán documentarse, mantenerse y ponerse a disposición de todos los usuarios que los necesiten. **- [A.8.2.3] Proceso disciplinario** Habrá un proceso disciplinario formal para los empleados que hayan cometido una violación de seguridad.
ACTIVO	**AMENAZA**	**CONTROL**
Equipamiento Auxiliar		
	[I.6]	**A.9.2 Seguridad del equipo** Objetivo: Impedir la pérdida, daño, robo o compromiso de activos así como interrupción de las actividades de la organización. **- [A.9.2.2]** El equipo deberá estar protegido contra cortes de energía y otros trastornos ocasionados por fallas en los servicios de soporte. **A.10.1Procedimientos y responsabilidades operativas**

		Objetivo: Asegurar la correcta y segura operación de los recursos de procesamiento de información. **- [A.10.1.1]** Los procedimientos operativos deberán documentarse, mantenerse y ponerse a disposición de todos los usuarios que los necesiten.
	[N.1] **[I.2]** **[N.2]** **[I.*]** **[I.1]** **[N.*]**	**- [A.10.1.1]** Los procedimientos operativos deberán documentarse, mantenerse y ponerse a disposición de todos los usuarios que los necesiten. **A.15.2 Cumplimiento de las políticas y normas de seguridad, y cumplimiento técnico** Objetivo: Asegurar que los sistemas cumplan con las políticas y normas de seguridad de la organización **- [A.15.2.1]** Los gerentes deberán asegurar que todos los procedimientos de seguridad dentro de sus áreas de responsabilidad se efectúan correctamente para lograr el cumplimiento de las políticas y normas de seguridad. **- [A.14.1] Aspectos de seguridad de la información en la gestión de la continuidad de negocios** Objetivo: Contrarrestar las interrupciones de las actividades de negocios y proteger los procesos de negocio críticos de los efectos de fallas o desastres mayores de los sistemas de información, y asegurar su oportuna reanudación. **- [A.9.1.4]** Deberá diseñarse y aplicarse protección física contra daños por incendio, inundación, terremoto, explosión, desorden civil, y otras formas de desastres naturales o artificiales.
	[I.5]	**- [A.10.10.5]** Las fallas deberán registrarse, analizarse y deberán tomarse las medidas adecuadas. **- [A.9.2.4]** El equipo deberá mantenerse correctamente para asegurar su continua disponibilidad e integridad. **- [A.10.1.1]** Los procedimientos operativos deberán

		documentarse, mantenerse y ponerse a disposición de todos los usuarios que los necesiten.
	[I.7]	**- [A.9.2.1]** El equipo deberá ubicarse y protegerse para reducir los riesgos de amenazas y peligros ambientales, y las oportunidades de acceso no autorizado.
	[A.25]	**- [A.9.1.1]** Perímetros de seguridad (barreras tales como muros, puertas controladas por tarjeta o recepcionistas) deberán utilizarse para proteger las áreas que contienen información y las instalaciones de procesamiento de información. **- [A.9.1.2]** Las áreas seguras deberán protegerse mediante controles de ingreso adecuados para asegurar que sólo se permita el acceso del personal autorizado. **- [A.9.1.3]** Deberá diseñarse y aplicarse seguridad física para las oficinas, cuartos e instalaciones. **- [A.9.1.5]** Las áreas seguras deberán protegerse mediante controles de ingreso adecuados para asegurar que sólo se permita el acceso del personal autorizado. **- [A.9.1.6]** Los puntos de acceso tales como las áreas de entrega y carga y otros puntos donde personas no autorizadas pueden ingresar a los locales deberán controlarse y, de ser posible, aislarse de las instalaciones de procesamiento de información para evitar el acceso no autorizado. **- [A.10.1.1]** Los procedimientos operativos deberán documentarse, mantenerse y ponerse a disposición de todos los usuarios que los necesiten. **- [A.8.2.3]** Habrá un proceso disciplinario formal para los empleados que hayan cometido una violación de seguridad
ACTIVO	**AMENAZA**	**CONTROL**
Equipos de comunicación		
	[N.1] [I.2] [N.2] [I.*] [I.1] [N.*]	**- [A.10.1.1]** Los procedimientos operativos deberán documentarse, mantenerse y ponerse a disposición de todos

		los usuarios que los necesiten. **- [A.15.2.1]** Los gerentes deberán asegurar que todos los procedimientos de seguridad dentro de sus áreas de responsabilidad se efectúan correctamente para lograr el cumplimiento de las políticas y normas de seguridad. **- [A.14.1] Aspectos de seguridad de la información en la gestión de la continuidad de negocios** Objetivo: Contrarrestar las interrupciones de las actividades de negocios y proteger los procesos de negocio críticos de los efectos de fallas o desastres mayores de los sistemas de información, y asegurar su oportuna reanudación. **- [A.9.1.4]** Deberá diseñarse y aplicarse protección física contra daños por incendio, inundación, terremoto, explosión, desorden civil, y otras formas de desastres naturales o artificiales.
	[I.5]	**- [A.10.10.5]** Las fallas deberán registrarse, analizarse y deberán tomarse las medidas adecuadas. **- [A.9.2.4]** El equipo deberá mantenerse correctamente para asegurar su continua disponibilidad e integridad. **- [A.10.1.1]** Los procedimientos operativos deberán documentarse, mantenerse y ponerse a disposición de todos los usuarios que los necesiten.
	[I.6]	**- [A.9.2.2]** El equipo deberá estar protegido contra cortes de energía y otros trastornos ocasionados por fallas en los servicios de soporte. **- [A.10.1.1]** Los procedimientos operativos deberán documentarse, mantenerse y ponerse a disposición de todos los usuarios que los necesiten.
	[I.7]	**- [A.9.2.1]** El equipo deberá ubicarse y protegerse para reducir los riesgos de amenazas y peligros ambientales, y las oportunidades de acceso no autorizado.

	[A.24]	**- [A.10.3] Planeamiento y aceptación de sistemas** Objetivo: Minimizar el riesgo de fallas de sistemas. **- [A.9.2.2]** El equipo deberá estar protegido contra cortes de energía y otros trastornos ocasionados por fallas en los servicios de soporte. **- [A.14.1.3]** Deberá prepararse e implementarse planes para mantener o restaurar las operaciones y asegurar la disponibilidad de información al nivel requerido y en las escalas de tiempo requeridas luego de la interrupción o falla de procesos de negocios críticos. **- [A.10.10.1]** Los registros de auditoria que graban las actividades, excepciones, y eventos de seguridad de la información de los usuarios deberán existir y mantenerse durante un período convenido para asistir futuras investigaciones y en el monitoreo de control de acceso. **- [A.13.2] Gestión de incidentes y mejoras de seguridad de la información** Objetivo: Verificar que se aplique un enfoque uniforme y efectivo a la gestión de la seguridad de la información. **- [A.10.10.5]** Las fallas deberán registrarse, analizarse y deberán tomarse las medidas adecuadas. **- [A.10.1.1]** Los procedimientos operativos deberán documentarse, mantenerse y ponerse a disposición de todos los usuarios que los necesiten.
	[E.2]	**- [A.10.10.1]** Los registros de auditoria que graban las actividades, excepciones, y eventos de seguridad de la información de los usuarios deberán existir y mantenerse durante un período convenido para asistir futuras investigaciones y en el monitoreo de control de acceso. **- [A.13.2] Gestión de incidentes y mejoras de seguridad de la información** Objetivo: Verificar que se aplique un enfoque uniforme y efectivo a la gestión de la seguridad de la información.

		- [A.14.1] Deberá desarrollarse y mantenerse un proceso gestionado de continuidad del negocio en toda la organización, que se encargue de los requerimientos de seguridad de la información necesarios para la continuidad del negocio de la organización.
	[A.25]	**- [A.9.1.1]** Perímetros de seguridad (barreras tales como muros, puertas controladas por tarjeta o recepcionistas) deberán utilizarse para proteger las áreas que contienen información y las instalaciones de procesamiento de información. **- [A.9.1.2]** Las áreas seguras deberán protegerse mediante controles de ingreso adecuados para asegurar que sólo se permita el acceso del personal autorizado. **- [A.9.1.3]** Deberá diseñarse y aplicarse seguridad física para las oficinas, cuartos e instalaciones. **- [A.9.1.5]** Las áreas seguras deberán protegerse mediante controles de ingreso adecuados para asegurar que sólo se permita el acceso del personal autorizado. **- [A.9.1.6]** Los puntos de acceso tales como las áreas de entrega y carga y otros puntos donde personas no autorizadas pueden ingresar a los locales deberán controlarse y, de ser posible, aislarse de las instalaciones de procesamiento de información para evitar el acceso no autorizado. **- [A.10.1.1]** Los procedimientos operativos deberán documentarse, mantenerse y ponerse a disposición de todos los usuarios que los necesiten.
	[E.4]	**- [A.10.10.1]** Los registros de auditoria que graban las actividades, excepciones, y eventos de seguridad de la información de los usuarios deberán existir y mantenerse durante un período convenido para asistir futuras investigaciones y en el monitoreo de control de acceso. **- [A.10.10.2]** Deberán establecerse procedimientos para monitorear el uso de las instalaciones de procesamiento de información, y los resultados de las actividades de monitoreo deberán revisarse regularmente.

		- [A.11.2.2] Deberá restringirse y controlarse la asignación y uso de privilegios. **- [A.11.4.1]** A los usuarios sólo deberá dárseles acceso a los servicios que están específicamente autorizados para usar. **- [A.11.4.1]** A los usuarios sólo deberá dárseles acceso a los servicios que están específicamente autorizados para usar. **- [A.11.5.2]** Todos los usuarios deberán tener un código de id organización único para uso personal solamente, y deberá seleccionarse una técnica de autenticación apropiada para fundamentar la id organización reclamada por un usuario. **- [A.11.5.2]** Todos los usuarios deberán tener un código de id organización único para uso personal solamente, y deberá seleccionarse una técnica de autenticación apropiada para fundamentar la id organización reclamada por un usuario. **- [A.11.6.1]** El acceso por los usuarios a las funciones del sistema de información y aplicaciones deberá restringirse según la política de control de acceso definida. **- [A.10.10.4]** Se deberán registrar las actividades del administrador del sistema y del operador del sistema. **- [A.10.1.1]** Los procedimientos operativos deberán documentarse, mantenerse y ponerse a disposición de todos los usuarios que los necesiten. **- [A.14.1.4]** Deberá mantenerse un solo marco de planes de continuidad de negocios para asegurar que todos los planes sean concordantes, para enfocar de modo uniforme los requerimientos de seguridad de la información, y para identificar prioridades de prueba y mantenimiento. **- [A.11.2.2]** Deberá restringirse y controlarse la asignación y uso de privilegios.
ACTIVO	**AMENAZA**	**CONTROL**
Equipamiento informático		
	[I.5]	**- [A.10.10.5]** Las fallas deberán registrarse, analizarse y

		deberán tomarse las medidas adecuadas. **- [A.9.2.4]** El equipo deberá mantenerse correctamente para asegurar su continua disponibilidad e integridad. **- [A.10.1.1]** Los procedimientos operativos deberán documentarse, mantenerse y ponerse a disposición de todos los usuarios que los necesiten.
	[I.6]	**- [A.9.2.2]** El equipo deberá estar protegido contra cortes de energía y otros trastornos ocasionados por fallas en los servicios de soporte. **- [A.10.1.1]** Los procedimientos operativos deberán documentarse, mantenerse y ponerse a disposición de todos los usuarios que los necesiten.
	[I.7]	**- [A.9.2.1]** El equipo deberá ubicarse y protegerse para reducir los riesgos de amenazas y peligros ambientales, y las oportunidades de acceso no autorizado.
	[A.24]	**- [A.10.3] Planeamiento y aceptación de sistemas** Objetivo: Minimizar el riesgo de fallas de sistemas. **- [A.9.2.2]** El equipo deberá estar protegido contra cortes de energía y otros trastornos ocasionados por fallas en los servicios de soporte. **- [A.14.1.3]** Deberá prepararse e implementarse planes para mantener o restaurar las operaciones y asegurar la disponibilidad de información al nivel requerido y en las escalas de tiempo requeridas luego de la interrupción o falla de procesos de negocios críticos. **- [A.10.10.1]** Los registros de auditoria que graban las actividades, excepciones, y eventos de seguridad de la información de los usuarios deberán existir y mantenerse durante un período convenido para asistir futuras investigaciones y en el monitoreo de control de acceso.

		- [A.13.2] Gestión de incidentes y mejoras de seguridad de la información Objetivo: Verificar que se aplique un enfoque uniforme y efectivo a la gestión de la seguridad de la información. **- [A.10.10.5]** Las fallas deberán registrarse, analizarse y deberán tomarse las medidas adecuadas. **- [A.10.1.1]** Los procedimientos operativos deberán documentarse, mantenerse y ponerse a disposición de todos los usuarios que los necesiten.
	[A.25]	**- [A.9.1.1]** Perímetros de seguridad (barreras tales como muros, puertas controladas por tarjeta o recepcionistas) deberán utilizarse para proteger las áreas que contienen información y las instalaciones de procesamiento de información. **- [A.9.1.3]** Deberá diseñarse y aplicarse seguridad física para las oficinas, cuartos e instalaciones. **- [A.9.1.5]** Las áreas seguras deberán protegerse mediante controles de ingreso adecuados para asegurar que sólo se permita el acceso del personal autorizado. **- [A.9.1.6]** Los puntos de acceso tales como las áreas de entrega y carga y otros puntos donde personas no autorizadas pueden ingresar a los locales deberán controlarse y, de ser posible, aislarse de las instalaciones de procesamiento de información para evitar el acceso no autorizado. **- [A.10.1.1]** Los procedimientos operativos deberán documentarse, mantenerse y ponerse a disposición de todos los usuarios que los necesiten. **- [A.9.1.2]** Las áreas seguras deberán protegerse mediante controles de ingreso adecuados para asegurar que sólo se permita el acceso del personal autorizado.
	[N.1] [I.2] [N.2] [I.*] [I.1] [N.*]	**- [A.10.1.1]** Los procedimientos operativos deberán documentarse, mantenerse y ponerse a disposición de todos los usuarios que los necesiten.

		- [A.15.2.1] Los gerentes deberán asegurar que todos los procedimientos de seguridad dentro de sus áreas de responsabilidad se efectúan correctamente para lograr el cumplimiento de las políticas y normas de seguridad. **- [A.14.1] Aspectos de seguridad de la información en la gestión de la continuidad de negocios** Objetivo: Contrarrestar las interrupciones de las actividades de negocios y proteger los procesos de negocio críticos de los efectos de fallas o desastres mayores de los sistemas de información, y asegurar su oportuna reanudación. **- [A.9.1.4]** Deberá diseñarse y aplicarse protección física contra daños por incendio, inundación, terremoto, explosión, desorden civil, y otras formas de desastres naturales o artificiales.
	[A.4]	**- [A.10.10.1]** Los registros de auditoria que graban las actividades, excepciones, y eventos de seguridad de la información de los usuarios deberán existir y mantenerse durante un período convenido para asistir futuras investigaciones y en el monitoreo de control de acceso. **- [A.10.1.1]** Los procedimientos operativos deberán documentarse, mantenerse y ponerse a disposición de todos los usuarios que los necesiten. **- [A.10.10.2]** Deberán establecerse procedimientos para monitorear el uso de las instalaciones de procesamiento de información, y los resultados de las actividades de monitoreo deberán revisarse regularmente. **- [A.14.1.4]** Deberá mantenerse un solo marco de planes de continuidad de negocios para asegurar que todos los planes sean concordantes, para enfocar de modo uniforme los requerimientos de seguridad de la información, y para identificar prioridades de prueba y mantenimiento. **- [A.8.2.3]** Habrá un proceso disciplinario formal para los empleados que hayan cometido una violación de seguridad. **- [A.10.10.4]** Se deberán registrar las actividades del administrador del sistema y del operador del sistema.

	[E.2]	**- [A.10.1.1]** Los procedimientos operativos deberán documentarse, mantenerse y ponerse a disposición de todos los usuarios que los necesiten. **- [A.13.2] Gestión de incidentes y mejoras de seguridad de la información** Objetivo: Verificar que se aplique un enfoque uniforme y efectivo a la gestión de la seguridad de la información. **- [A.13.2] Gestión de incidentes y mejoras de seguridad de la información** Objetivo: Verificar que se aplique un enfoque uniforme y efectivo a la gestión de la seguridad de la información. **- [A.14.1]** Deberá identificarse los eventos que pueden causar interrupciones a los procesos de negocios, junto con la probabilidad e impacto de tales interrupciones y sus consecuencias para la seguridad de la información. **- [A.10.10.4]** Se deberán registrar las actividades del administrador del sistema y del operador del sistema.
ACTIVO	**AMENAZA**	**CONTROL**
Personal		
	[E.28] - [E.28]	**- [A.8.1.3]** Como parte de su obligación contractual, los empleados, contratistas y usuarios de terceros deberán aceptar y firmar los términos y condiciones de su contrato de empleo, el cual deberá indicar sus responsabilidades de seguridad de la información así como las de la organización.
ACTIVO	**AMENAZA**	**CONTROL**
Instalaciones		
	[I.2] - [N.1] [N.2] - [I.*] [I.1] - [N.*]	**- [A.10.1.1]** Los procedimientos operativos deberán documentarse, mantenerse y ponerse a disposición de todos los usuarios que los necesiten. **- [A.15.2.1]** Los gerentes deberán asegurar que todos los procedimientos de seguridad dentro de sus áreas de responsabilidad se efectúan correctamente para lograr el

		cumplimiento de las políticas y normas de seguridad. **- [A.14.1] Aspectos de seguridad de la información en la gestión de la continuidad de negocios** Objetivo: Contrarrestar las interrupciones de las actividades de negocios y proteger los procesos de negocio críticos de los efectos de fallas o desastres mayores de los sistemas de información, y asegurar su oportuna reanudación. **- [A.9.1.4]** Deberá diseñarse y aplicarse protección física contra daños por incendio, inundación, terremoto, explosión, desorden civil, y otras formas de desastres naturales o artificiales.
ACTIVO	**AMENAZA**	**CONTROL**
Aplicaciones		
	[E.8] **[A.8]**	**- [A.10.4.1]** Deberá implementarse controles de detección, prevención y recuperación para protegerse contra código malicioso así como procedimientos adecuados de concientización de usuarios. **-[A.10.10.2]** Deberán establecerse procedimientos para monitorear el uso de las instalaciones de procesamiento de información, y los resultados de las actividades de monitoreo deberán revisarse regularmente. **- [A.12.4.1]** Deberán existir procedimientos para controlar la instalación de “software” en los sistemas operativos. **[A.12.4.1]** Deberán existir procedimientos para controlar la instalación de “software” en los sistemas operativos. **- [A.10.4.2]** Cuando el uso de código móvil está autorizado, la configuración deberá asegurar que el código móvil autorizado opere según una política de seguridad claramente definida, y se impedirá la ejecución de código móvil no autorizado **- [A.11.4.4]** Deberá controlarse el acceso físico y lógico a los puertos de diagnóstico y configuración **[A.10.1.1]** Los procedimientos operativos deberán documentarse, mantenerse y ponerse a disposición de todos los usuarios que los necesiten.

		[A.14.1.4] Deberá mantenerse un solo marco de planes de continuidad de negocios para asegurar que todos los planes sean concordantes, para enfocar de modo uniforme los requerimientos de seguridad de la información, y para identificar prioridades de prueba y mantenimiento. **[A.8.2.3]** Habrá un proceso disciplinario formal para los empleados que hayan cometido una violación de seguridad.
	[E.4] **[A.4]**	**- [A.10.10.1]** Los registros de auditoria que graban las actividades, excepciones, y eventos de seguridad de la información de los usuarios deberán existir y mantenerse durante un período convenido para asistir futuras investigaciones y en el monitoreo de control de acceso. **- [A.10.10.2]** Deberán establecerse procedimientos para monitorear el uso de las instalaciones de procesamiento de información, y los resultados de las actividades de monitoreo deberán revisarse regularmente **- [A.11.2.2]** Deberá restringirse y controlarse la asignación y uso de privilegios. **- [A.11.4.1]** A los usuarios sólo deberá dárseles acceso a los servicios que están específicamente autorizados para usar. **- [A.11.5.2]** Todos los usuarios deberán tener un código de id organización único para uso personal solamente, y deberá seleccionarse una técnica de autenticación apropiada para fundamentar la id organización reclamada por un usuario. **- [A.11.6.1]** El acceso por los usuarios a las funciones del sistema de información y aplicaciones deberá restringirse según la política de control de acceso definida. **- [A.10.1.1]** Los procedimientos operativos deberán documentarse, mantenerse y ponerse a disposición de todos los usuarios que los necesiten. **- [A.14.1.4]** Deberá mantenerse un solo marco de planes de continuidad de negocios para asegurar que todos los planes sean concordantes, para enfocar de modo uniforme los requerimientos de seguridad de la información, y para

		identificar prioridades de prueba y mantenimiento. **- [A.11.2.2]** Deberá restringirse y controlarse la asignación y uso de privilegios. **- [A.8.2.3]** Habrá un proceso disciplinario formal para los empleados que hayan cometido una violación de seguridad.
	[E.21]	**- [A.9.2.4]** El equipo deberá mantenerse correctamente para asegurar su continua disponibilidad e integridad. **- [A.10.3.2]** Deberán establecerse criterios de aceptación de nuevos sistemas de información, actualizaciones y nuevas versiones, y realizarse pruebas adecuadas de los sistemas durante el desarrollo y antes de la aceptación. **- [A.11.2.2]** Deberá restringirse y controlarse la asignación y uso de privilegios. **- [A.11.4.1]** A los usuarios sólo deberá dárseles acceso a los servicios que están específicamente autorizados para usar.
	[E.20]	**- [A.12.2] Procesamiento correcto en aplicaciones** Objetivo: Prevenir errores, pérdidas, modificación no autorizada o mal uso de la información en aplicaciones **- [A.12.5] Seguridad en los procesos de desarrollo y soporte** Objetivo: Mantener la seguridad del “software” e información del sistema de aplicaciones **- [A.12.6.1]** Deberá obtenerse información oportuna sobre las vulnerabilidades técnicas de los sistemas de información en uso, evaluarse la exposición de la organización a esas vulnerabilidades, y tomarse medidas adecuadas para resolver el riesgo relacionado. **- [A.10.4]** Deberá implementarse controles de detección, prevención y recuperación para protegerse contra código malicioso así como procedimientos adecuados de concientización de usuarios.

		- [A.12.2.1] Los datos de entrada para aplicaciones deberán validarse para asegurar que estos datos son correctos y adecuados. **- [A.10.4.2]** Cuando el uso de código móvil está autorizado, la configuración deberá asegurar que el código móvil autorizado opere según una política de seguridad claramente definida, y se impedirá la ejecución de código móvil no autorizado **- [A.11.4.4]** Deberá controlarse el acceso físico y lógico a los puertos de diagnóstico y configuración **- [A.12.4.1]** Deberán existir procedimientos para controlar la instalación de "software" en los sistemas operativos. **- [A.8.2.3]** Habrá un proceso disciplinario formal para los empleados que hayan cometido una violación de seguridad.
	[A.5]	**- [A.11.5.2]** Todos los usuarios deberán tener un código de id organización único para uso personal solamente, y deberá seleccionarse una técnica de autenticación apropiada para fundamentar la id organización reclamada por un usuario. **- [A.11.5.3]** Los sistemas de manejo de contraseñas deberán ser interactivos y deberán asegurar contraseñas de calidad. **- [A.11.3.1]** Se deberá exigir a los usuarios que sigan buenas prácticas de seguridad en la selección y uso de las contraseñas. **- [A.12.2.1]** Los datos de entrada para aplicaciones deberán validarse para asegurar que estos datos son correctos y adecuados. **- [A.11.3.1]** Se deberá exigir a los usuarios que sigan buenas prácticas de seguridad en la selección y uso de las contraseñas. **- [A.12.2.1]** Los datos de entrada para aplicaciones deberán validarse para asegurar que estos datos son correctos y adecuados. **- [A.11.3.2]** Los usuarios deberán asegurar que el equipo no atendido tenga protección adecuada.

		- [A.8.3.3] Los derechos de acceso de todos los empleados, contratistas y usuarios de terceros a la información y a las instalaciones de procesamiento de información deberán retirarse al terminar su empleo, contrato o convenio, o modificarse según el cambio. **- [A.8.2.3]** Habrá un proceso disciplinario formal para los empleados que hayan cometido una violación de seguridad. **- [A.10.1.1]** Los procedimientos operativos deberán documentarse, mantenerse y ponerse a disposición de todos los usuarios que los necesiten. **- [A.10.1.2]** Se controlarán los cambios en las instalaciones y sistemas de procesamiento de información.
	[A.11]	**- [A.9.1.2]** Las áreas seguras deberán protegerse mediante controles de ingreso adecuados para asegurar que sólo se permita el acceso del personal autorizado. **- [A.9.1.5]** Las áreas seguras deberán protegerse mediante controles de ingreso adecuados para asegurar que sólo se permita el acceso del personal autorizado. **- [A.9.1.1]** Perímetros de seguridad (barreras tales como muros, puertas controladas por tarjeta o recepcionistas) deberán utilizarse para proteger las áreas que contienen información y las instalaciones de procesamiento de información. **- [A.10.1.4]** Las instalaciones de desarrollo, prueba y operaciones deberán separarse para reducirlos riesgos de acceso o cambios no autorizados al sistema operativo. **- [A.11.2.1]** Deberá haber un procedimiento formal de inscripción y des-inscripción de usuarios para otorgar y revocar el acceso a todos los sistemas y servicios de información. **- [A.9.1.1]** Perímetros de seguridad (barreras tales como muros, puertas controladas por tarjeta o recepcionistas) deberán utilizarse para proteger las áreas que contienen información y las instalaciones de procesamiento de información.

		- [A.9.1.4] Deberá diseñarse y aplicarse protección física contra daños por incendio, inundación, terremoto, explosión, desorden civil, y otras formas de desastres naturales o artificiales. **- [A.10.1.4]** Las instalaciones de desarrollo, prueba y operaciones deberán separarse para reducirlos riesgos de acceso o cambios no autorizados al sistema operativo **- [A.11.4.1]** A los usuarios sólo deberá dárseles acceso a los servicios que están específicamente autorizados para usar. **- [A.8.3] Terminación o cambio de empleo** Objetivo: Asegurar que los empleados, contratistas y usuarios de terceros salgan de una organización o cambien de empleo en forma ordenada. **- [A.13.2.3]** Cuando la acción de seguimiento contra una persona o organización después de un incidente de seguridad de la información involucre medidas legales (ya sea civiles o penales), deberá recolectarse, retenerse y presentarse evidencia de conformidad con las reglas de prueba establecidas en la legislación pertinente. **- [A.15.1] Cumplimiento de requisitos legales** Objetivo: Evitar violaciones de cualquier ley u obligación estatutaria, de regulación o contractual, y de cualquier requisito de seguridad. **- [A.13] Gestión de incidentes de seguridad de la información** **- [A.9.1.5]** Las áreas seguras deberán protegerse mediante controles de ingreso adecuados para asegurar que sólo se permita el acceso del personal autorizado. **- [A.9.1.6]** Los puntos de acceso tales como las áreas de entrega y carga y otros puntos donde personas no autorizadas pueden ingresar a los locales deberán controlarse y, de ser posible, aislarse de las instalaciones de procesamiento de información para evitar el acceso no autorizado. **- [A.12.2.1]** Los datos de entrada para aplicaciones deberán validarse para asegurar que estos datos son correctos y

		adecuados. **- [A.10.1.4]** Las instalaciones de desarrollo, prueba y operaciones deberán separarse para reducirlos riesgos de acceso o cambios no autorizados al sistema operativo. **- [A.9.1.1]** Perímetros de seguridad (barreras tales como muros, puertas controladas por tarjeta o recepcionistas) deberán utilizarse para proteger las áreas que contienen información y las instalaciones de procesamiento de información. **- [A.10.1.1]** Los procedimientos operativos deberán documentarse, mantenerse y ponerse a disposición de todos los usuarios que los necesiten.
ACTIVO	**AMENAZA**	**CONTROL**
Servicios		
	[E.24]	**- [A.10.3] Planeamiento y aceptación de sistemas** Objetivo: Minimizar el riesgo de fallas de sistemas. **- [A.9.2.2]** El equipo deberá estar protegido contra cortes de energía y otros trastornos ocasionados por fallas en los servicios de soporte. **- [A.14.1.3]** Deberá prepararse e implementarse planes para mantener o restaurar las operaciones y asegurar la disponibilidad de información al nivel requerido y en las escalas de tiempo requeridas luego de la interrupción o falla de procesos de negocios críticos. **- [A.10.10.1]** Los registros de auditoria que graban las actividades, excepciones, y eventos de seguridad de la información de los usuarios deberán existir y mantenerse durante un período convenido para asistir futuras investigaciones y en el monitoreo de control de acceso. **- [A.13.2] Gestión de incidentes y mejoras de seguridad de la información** Objetivo: Verificar que se aplique un enfoque uniforme y efectivo a la gestión de la seguridad de la información.

		- [A.10.10.5] Las fallas deberán registrarse, analizarse y deberán tomarse las medidas adecuadas. **- [A.10.1.1]** Los procedimientos operativos deberán documentarse, mantenerse y ponerse a disposición de todos los usuarios que los necesiten.
	[E.1]	**[A.8.2] Durante el empleo** Objetivo: Asegurar que todos los empleados, contratistas y usuarios de terceros conozcan las amenazas y problemas de seguridad de la información, así como sus responsabilidades y obligaciones, y estén capacitados para apoyar la política de seguridad de la organización en el curso de su trabajo normal, y reducir el riesgo de error humano. **[A.10.10.5]** Las fallas deberán registrarse, analizarse y deberán tomarse las medidas adecuadas. **[A.10.10.1]** Los registros de auditoria que graban las actividades, excepciones, y eventos de seguridad de la información de los usuarios deberán existir y mantenerse durante un período convenido para asistir futuras investigaciones y en el monitoreo de control de acceso.
	[E.4] **[A.4]**	**- [A.10.10.1]** Los registros de auditoria que graban las actividades, excepciones, y eventos de seguridad de la información de los usuarios deberán existir y mantenerse durante un período convenido para asistir futuras investigaciones y en el monitoreo de control de acceso. **- [A.10.10.2]** Deberán establecerse procedimientos para monitorear el uso de las instalaciones de procesamiento de información, y los resultados de las actividades de monitoreo deberán revisarse regularmente. **- [A.11.2.2]** Deberá restringirse y controlarse la asignación y uso de privilegios. **- [A.11.4.1]** A los usuarios sólo deberá dárseles acceso a los servicios que están específicamente autorizados para usar. **- [A.11.5.2]** Todos los usuarios deberán tener un código de id organización único para uso personal solamente, y deberá seleccionarse una técnica de autenticación apropiada para fundamentar la id organización reclamada por un usuario.

		- [A.11.6.1] El acceso por los usuarios a las funciones del sistema de información y aplicaciones deberá restringirse según la política de control de acceso definida. **- [A.10.1.1]** Los procedimientos operativos deberán documentarse, mantenerse y ponerse a disposición de todos los usuarios que los necesiten. **- [A.14.1.4]** Deberá mantenerse un solo marco de planes de continuidad de negocios para asegurar que todos los planes sean concordantes, para enfocar de modo uniforme los requerimientos de seguridad de la información, y para identificar prioridades de prueba y mantenimiento. **- [A.11.2.2]** Deberá restringirse y controlarse la asignación y uso de privilegios. **- [A.8.2.3]** Habrá un proceso disciplinario formal para los empleados que hayan cometido una violación de seguridad.
	[E.5]	**- [A.11.5.2]** Todos los usuarios deberán tener un código de id organización único para uso personal solamente, y deberá seleccionarse una técnica de autenticación apropiada para fundamentar la id organización reclamada por un usuario. **- [A.11.5.3]** Los sistemas de manejo de contraseñas deberán ser interactivos y deberán asegurar contraseñas de calidad. **- [A.11.3.1]** Se deberá exigir a los usuarios que sigan buenas prácticas de seguridad en la selección y uso de las contraseñas. **- [A.12.2.1]** Los datos de entrada para aplicaciones deberán validarse para asegurar que estos datos son correctos y adecuados. **- [A.11.3.1]** Se deberá exigir a los usuarios que sigan buenas prácticas de seguridad en la selección y uso de las contraseñas. **- [A.12.2.1]** Los datos de entrada para aplicaciones deberán validarse para asegurar que estos datos son correctos y adecuados.

		- [A.11.3.2] Los usuarios deberán asegurar que el equipo no atendido tenga protección adecuada. **- [A.8.3.3]** Los derechos de acceso de todos los empleados, contratistas y usuarios de terceros a la información y a las instalaciones de procesamiento de información deberán retirarse al terminar su empleo, contrato o convenio, o modificarse según el cambio. **- [A.8.2.3]** Habrá un proceso disciplinario formal para los empleados que hayan cometido una violación de seguridad. **- [A.10.1.1]** Los procedimientos operativos deberán documentarse, mantenerse y ponerse a disposición de todos los usuarios que los necesiten. **- [A.10.1.2]** Se controlarán los cambios en las instalaciones y sistemas de procesamiento de información.
	[E.2]	**-[A.10.1.1]** Los procedimientos operativos deberán documentarse, mantenerse y ponerse a disposición de todos los usuarios que los necesiten. **- [A.13.2.1]** Deberán establecerse responsabilidades y procedimientos de gerencia para asegurar la respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información. **-[A.14.1] Aspectos de seguridad de la información en la gestión de la continuidad de negocios** Objetivo: Contrarrestar las interrupciones de las actividades de negocios y proteger los procesos de negocio críticos de los efectos de fallas o desastres mayores de los sistemas de información, y asegurar su oportuna reanudación. **- [A.10.1.1]** Los procedimientos operativos deberán documentarse, mantenerse y ponerse a disposición de todos los usuarios que los necesiten. **- [A.13.2] Gestión de incidentes y mejoras de seguridad de la información** Objetivo: Verificar que se aplique un enfoque uniforme y efectivo a la gestión de la seguridad de la información.

	[E.7]	**- [A.7.1.3]** Deberán identificarse, documentarse e implementarse reglas para el uso aceptable de la información y de los activos relacionados con las instalaciones de procesamiento de información. **- [A.8.2.2]** Todo el personal de la organización y, cuando sea pertinente, los contratistas y usuarios de terceros, deberán recibir el entrenamiento de concientización adecuado y actualizaciones periódicas de políticas y procedimientos de la organización, según corresponda a sus funciones de trabajo. **- [A.8.1.1]** Las funciones y responsabilidades de seguridad de los empleados, contratistas y usuarios de terceros deberán definirse y documentarse de acuerdo a la política de seguridad de información de la organización. **- [A.8.2.3]** Habrá un proceso disciplinario formal para los empleados que hayan cometido una violación de seguridad.

8. Recomendaciones

Como parte del diseño del sistema de gestión de seguridad se recomienda entre otras actividades a realizar:

- Este diseño solo se podrá implementar en el Departamento de Sistemas de la Fundación Universitaria Tecnológico Comfenalco, ya que ese fue nuestro objeto de estudio, por lo tanto el esquema solo puede ser ejecutado en el sistemas de gestión informática que actualmente se allí se lleva acabo.

- El estudio que se realizó en esta importante organización fue realizada en las fechas del 24 de Mayo hasta el 27 de Septiembre del presente año; por su alto crecimiento de la Universidad, su infraestructura tecnológica del departamento de sistemas ha ido creciendo, por lo tanto solo se diseñó los controles y políticas de seguridad y todo el análisis realizados a los activos adquiridos en esas fechas.

  Se recomienda que para una implementación actual se deba identificar los activos adquiridos con el fin de aplicar todas las fases que indica la Norma Iso 27001 como también la metodología de análisis de riesgo Magerit V2 y las herramientas relacionadas con estas.

- Se recomienda que para un futuro análisis de este documento al momento de ser implementado se abarque en la etapa de determinación de la brecha el punto de manejo de presupuesto y diseño del cronograma, así como todas las etapas subsiguientes a la elaboración del plan de gestión de continuidad.

- En relación a los resultados de la investigación se recomienda que la implementación de este diseño, solo se lleve a cabo por personas que dominen bien la Norma Iso 27001 SGSI y todos los elementos relacionados con esta, como también la conozcan la Metodología de análisis de riesgo Magerit V2.

9. Conclusiones

Como conclusión podemos decir que el Departamento de Sistemas de Tecnológico Comfenalco cuenta con unos mecanismos de control para asegurar la confidencialidad, integridad y disponibilidad de la información, estos mecanismos han sido implantados a través de herramientas como: Windows 2003 Server e ISA Server entre otros, en donde se tienen configurados diferentes parámetros que permiten establecer controles de acceso por parte de los usuarios a diferentes tipos de información, estos mecanismos no son suficientes, por lo que es necesario realizar la evaluación de riesgos sobre todos los activos de la organización, incluyendo hardware, software, documentación, personal, proveedores, socios, etc. y escoger los controles adecuados para disminuir esos riesgos. Por lo que la ISO 27001 nos ofrece 133 controles que los podemos encontrar en el anexo 3, además debe apoyarse en la metodología y análisis de gestión de riesgos como lo es MAGERIT V2, que les permitirá saber cuánto valor está en juego y les ayudará a protegerlo. Conocer el riesgo al que están sometidos los elementos de trabajo y es simplemente imprescindible para poder gestionarlos. Con MAGERIT se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

En el diseño del sistema de gestión de seguridad de información, que se realizado para el Departamento de Sistemas**,** se llevó un procedimiento el cual cubre varias etapas las cuales comienza con el entendimiento de los requerimientos del modelo, en donde se hizo necesario y preciso manejar técnicas de recolección de información como fueron entrevistas al personal encargado, observación y los registros, los cuales nos abrieron las puertas para que se pudiera desarrollar la investigación plenamente en la institución. Como primera medida *conocimiento del departamento:* En este se procede a conocer las funciones de cada uno de los que laboran en esta área, además de esto se solicitó los manuales de procedimientos en los cuales están redactados las tareas y actividades que debe realizar estrictamente. *Identificación de los activos*: en este se pidió el inventario de activo actualizado, con el fin de identificar los activos con que cuenta el Departamento de

Sistemas, además de esto también se indago acerca de la importancia de cada activo, de que tan indispensable era para la división y la institución si alguno de estos hiciera falta. *Valoración de Activos:* En esta etapa es donde empezamos a darlos valor a cada activos teniendo en cuenta lo parametrizado en Magerit V2, teniendo en cuenta la disponibilidad, integridad de los datos, confidencialidad de los datos, autenticidad de los usuarios y autenticidad de el origen de los datos. *Determinación de la brecha*: En esta etapa lo que se trata de determinar que tanto se tiene implementado en el Departamento de Sistemas, como los son controles y políticas para la seguridad de la información teniendo en cuenta lo parametrizado en la norma ISO 27001, entre los ítem que se comparan están los 11 puntos de políticas de seguridad; para realizar esta etapa tuvimos que implementar una actividad que en los sistemas de seguridad de información se le conoce como análisis GAP, el cual es una herramienta metodológica que nos permite comparar dos prácticas distintas una de las practicas es aquella que está utilizando en el Departamento de Sistemas y la otra es aquella que establece un estándar que es aceptable mundialmente.

Un paso muy vital e importante el cual se convierte en otra etapa de nuestro proyecto es el de *análisis y evaluación de riesgo* para efectuar este hay que tener en cuenta los riesgos y amenazas posibles sobre los activos. Al ser capaces de reconocer las posible amenazas tendremos también la capacidad de crear contramedidas para estas, las cuales minimicen y en el mejor de los casos eviten que alguna de estas se lleve a cabo, este punto también es importante. Luego se prosigue con el *Cálculo del impacto acumulado***:** a esto se le dé domina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza, este se calcula por cada activo, cada amenaza y cada dimensión de valoración. El objetivo de este paso en la metodología es determinar las salvaguardas de que hay que dotar a los medios de trabajo.

Finalmente se diseña las políticas de seguridad y los controles aplicar a cada una de las amenazas de los activos informático del Departamento de Sistemas del Tecnológico Comfenalco.

De esta manera, las políticas de seguridad en informática emergen como el instrumento para concientizar a sus miembros acerca de la importancia y sensibilidad de la información y servicios críticos, de la superación de las fallas y de las debilidades, de tal forma que permiten a la institución cumplir con su misión

También podemos decir que por falta de tiempo no pudimos terminar las siguientes etapas, la cual se recomienda que para un futuro análisis de este documento al momento de ser implementado se abarque en la etapa de determinación de la brecha el punto de manejo de presupuesto y diseño del cronograma, así como todas las etapas subsiguientes a la elaboración del plan de gestión de continuidad.

10. Referencias Bibliográficas

- ✓ Alberto G. Alexander, Diseño De Un Sistema De Gestión De Seguridad De Información óptica ISO 27001:2005, 1 era Edición, Bogotá DC, 2007, ISBN 978-958-682-713-3.
- ✓ ISO/IEC FDIS 27001:2005(E), Norma internacional ISO/IEC FDIS 27001.
- ✓ Álvarez M. Gonzalo, Pérez G. Pedro Pablo Seguridad Informática Para Empresas y Particulares, 1 era Edición, 2004, ISBN 84-481-4297-7
- ✓ Instituto Argentino De Normalización, Iram-IsoIec 17799 Código De Practica Para La Administración De La Seguridad De La Información, 1 Era Edición, 2002.
- ✓ Alan Calder, Nueve Claves Para El Éxito, Una visión general de la implementación de la norma NTC-ISO/IEC 27001
- ✓ EL PORTAL DE ISO 27001 EN ESPAÑOL. Sistema de Gestión de la seguridad de la Información. <**http://www.iso27000.es/mapa**> **[** citado el 29 de Agosto de 2010**]**
- ✓ IMPLANTACIÓN ISO 27001:2005. Sistema de Gestión de la seguridad de la Información. <**http://www.gestion-calidad.com/implantacion-iso-27001.html**>**[** citado el 2 de Septiembre de 2010**]**
- ✓ SEGURIDAD DE LA INFORMACIÓN. Sistema de Gestión de la seguridad de la Información.<**http://seguinfcol.blogspot.com/2010/10/checklist-de-implementacion-de-iso.html**>**[** citado el 15 de Junio de 2010**]**

FUNDACIÓN UNIVERSITARIA
TECNOLÓGICO COMFENALCO
CARTAGENA

ANEXO

Anexo # 1

Formato de Entrevista

Cuestionario que se utilizó para tener conocimiento acerca del Departamento de Sistemas del Tecnológico.

Fundación Universitaria Tecnológico

Comfenalco

ISO 27001

Fecha_____ **División**_____

Jefe o Responsable_____

Identificación de las funciones que desempeña el departamento

Preguntas

1. ¿Qué actividades o funciones realiza este departamento?
2. ¿Hace cuánto está conformado?
3. ¿Para qué fue creado?
4. ¿Cuál es la misión y visión del área?
5. ¿Qué grupo de personas conforman el área?
6. ¿Con quién se relaciona este departamento?
7. ¿Para qué se relaciona este departamento con los demás?
8. ¿Cómo se manejan los procesos internos?

Anexo # 2

Formato Análisis GAP

Lista de chequeo que se utilizó para realizar el Análisis Gab.

FORMULARIO PARA AUTODIAGNÓSTICO
(ISO 27001)
POLÍTICAS DE SEGURIDAD

- ☐ •Existen documento(s) de políticas de seguridad de SI
- ☐ •Existe normativa relativa a la seguridad de los SI
- ☐ •Existen procedimientos relativos a la seguridad de SI
- ☐ •Existe un responsable de las políticas, normas y procedimientos
- ☐ •Existen mecanismos para la comunicación a los usuarios de las normas
- ☐ •Existen controles regulares para verificar la efectividad de las políticas

ORGANIZACIÓN DE LA SEGURIDAD

- ☐ •Existen roles y responsabilidades definidos para las personas implicadas en la seguridad
- ☐ •Existe un responsable encargado de evaluar la adquisición y cambios de SI
- ☐ La Dirección y las áreas de la Organización participa en temas de seguridad
- ☐ •Existen condiciones contractuales de seguridad con terceros y outsourcing
- ☐ •Existen criterios de seguridad en el manejo de terceras partes
- ☐ •Existen programas de formación en seguridad para los empleados, clientes y terceros
- ☐ •Existe un acuerdo de confidencialidad de la información que se acceso.
- ☐ •Se revisa la organización de la seguridad periódicamente por una empresa externa

ADMINISTRACIÓN DE ACTIVOS

- ☐ •Existen un inventario de activos actualizado
- ☐ •El Inventario contiene activos de datos, software, equipos y servicios
- ☐ •Se dispone de una clasificación de la información según la criticidad de la

misma

• Existe un responsable de los activos

•Existen procedimientos para clasificar la información

•Existen procedimientos de etiquetado de la información

SEGURIDAD DE LOS RRHH

•Se tienen definidas responsabilidades y roles de seguridad

•Se tiene en cuenta la seguridad en la selección y baja del personal

•Se plasman las condiciones de confidencialidad y responsabilidades en los contratos

•Se imparte la formación adecuada de seguridad y tratamiento de activos

•Existe un canal y procedimientos claros a seguir en caso de incidente de seguridad

•Se recogen los datos de los incidentes de forma detallada

•Informan los usuarios de las vulnerabilidades observadas o sospechadas

•Se informa a los usuarios de que no deben, bajo ninguna circunstancia, probar las vulnerabilidades

• Existe un proceso disciplinario de la seguridad de la información

SEGURIDAD FÍSICA Y DEL AMBIENTE

Existe perímetro de seguridad física(una pared, puerta con llave).

Existen controles de entrada para protegerse frente al acceso de personal no autorizado

Un área segura ha de estar cerrada, aislada y protegida de eventos naturales

En las áreas seguras existen controles adicionales al personal propio y ajeno

Las áreas de carga y expedición están aisladas de las áreas de SI

La ubicación de los equipos está de tal manera para minimizar accesos innecesarios.

Existen protecciones frente a fallos en la alimentación eléctrica

Existe seguridad en el cableado frente a daños e intercepciones

Se asegura la disponibilidad e integridad de todos los equipos

Existe algún tipo de seguridad para los equipos retirados o ubicados exteriormente

Se incluye la seguridad en equipos móviles

GESTIÓN DE COMUNICACIONES Y OPERACIONES

Todos los procedimientos operativos identificados en la política de seguridad han de estar documentados

Estan establecidas responsabilidades para controlar los cambios en equipos

Estan establecidas responsabilidades para asegurar una respuesta rápida, ordenada y efectiva frente a incidentes de seguridad

Existe algún método para reducir el mal uso accidental o deliberado de los Sistemas

Existe una separación de los entornos de desarrollo y producción

Existen contratistas externos para la gestión de los Sistemas de Información

Existe un Plan de Capacidad para asegurar la adecuada capacidad de proceso y de almacenamiento

Existen criterios de aceptación de nuevos SI, incluyendo actualizaciones y nuevas versiones

Controles contra software maligno

Realizar copias de backup de la información esencial para el negocio

Existen logs para las actividades realizadas por los operadores y administradores

Existen logs de los fallos detectados

Existen rastro de auditoría

Existe algún control en las redes

Hay establecidos controles para realizar la gestión de los medios informáticos.(cintas, discos, removibles, informes impresos)

Eliminación de los medios informáticos. Pueden disponer de información sensible

Existe seguridad de la documentación de los Sistemas

Existen acuerdos para intercambio de información y software

Existen medidas de seguridad de los medios en el tránsito

Existen medidas de seguridad en el comercio electrónico.

Se han establecido e implantado medidas para proteger la confidencialidad e integridad de información publicada

Existen medidas de seguridad en las transacciones en línea

Se monitorean las actividades relacionadas a la seguridad

CONTROL DE ACCESOS

Existe una política de control de accesos

Existe un procedimiento formal de registro y baja de accesos

Se controla y restringe la asignación y uso de privilegios en entornos multi-usuario

Existe una gestión de los password de usuarios

Existe una revisión de los derechos de acceso de los usuarios

Existe el uso del password

Se protege el acceso de los equipos desatendidos

Existen políticas de limpieza en el puesto de trabajo

Existe una política de uso de los servicios de red

Se asegura la ruta (path) desde el terminal al servicio

Existe una autenticación de usuarios en conexiones externas

Existe una autenticación de los nodos

Existe un control de la conexión de redes

Existe un control del routing de las redes

Existe una identificación única de usuario y una automática de terminales

Existen procedimientos de log-on al terminal

Se ha incorporado medidas de seguridad a la computación móvil

Está controlado el teletrabajo por la organización

DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS

Se asegura que la seguridad está implantada en los Sistemas de Información

Existe seguridad en las aplicaciones

Existen controles criptográficos.

Existe seguridad en los ficheros de los sistemas

Existe seguridad en los procesos de desarrollo, testing y soporte

Existen controles de seguridad para los resultados de los sistemas

Existe la gestión de los cambios en los SO.

Se controlan las vulnerabilidades de los equipos

ADMINISTRACIÓN DE INCIDENTES

Se comunican los eventos de seguridad

Se comunican los debilidadesde seguridad

Existe definidas las responsabilidades antes un incidente.

Existe un procedimiento formal de respuesta

Existe la gestión de incidentes

GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Existen procesos para la gestión de la continuidad.

Existe un plan de continuidad del negocio y análisis de impacto

Existe un diseño, redacción e implantación de planes de continuidad

Existe un marco de planificación para la continuidad del negocio

Existen prueba, mantenimiento y reevaluación de los planes de continuidad del negocio.

CUMPLIMIENTO

Se tiene en cuenta el cumplimiento con la legislación por parte de los sistemas

Existe el resguardo de la propiedad intelectual

Existe el resguardo de los registros de la organización

Existe una revisión de la política de seguridad y de la conformidad técnica

Existen consideraciones sobre las auditorías de los sistemas

Anexo # 3: Formato utilizado para el cálculo de las amenazas de los activos.

VALOR	CRITERIO
10	**[1]** Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística. **[2]** Probablemente cause daños excepcionalmente graves a misiones extremadamente importantes de inteligencia o información. **[3]** Seguridad: probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios. **[4]** Seguridad de las personas: probablemente suponga gran pérdida de vidas humanas. **[5]** Orden público: alteración sería del orden constitucional. **[6]** Probablemente cause un impacto excepcionalmente grave en las relaciones internacionales. **[7]** Datos clasificados como secretos.
	[1] Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones. **[2]** Administración y gestión: probablemente impediría seriamente la operación efectiva de la organización, pudiendo llegar a su cierre. **[3]** Probablemente causaría una publicidad negativa generalizada por afectar

	de forma excepcionalmente grave a las relaciones. **[3.1]** las relaciones con otras organizaciones. **[3.2]** las relaciones con el público en general. **[3.3]** las relaciones con otros países. **[4]** Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística.
9	**[5]** Probablemente cause serios daños a misiones muy importantes de inteligencia o información. **[6]** Intereses comerciales o económicos: **[6.1]** De muy elevado valor comercial. **[6.2]** Causa de pérdidas económicas excepcionalmente elevadas **[6.3]** Causa de muy significativas ganancias o ventajas para Individuos u organizaciones. **[7]** Obligaciones legales: probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación. **[8]** Seguridad: probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios. **[9]** Seguridad de las personas: probablemente suponga la muerte de uno o más individuos. **[10]** Orden público: alteración sería del orden público. **[11]** Probablemente cause un serio impacto en las relaciones internacionales. **[12]** Datos clasificados como reservados.

8	**[1]** Seguridad de las personas: probablemente cause daño a la seguridad o libertad individual (por ejemplo, es probable que llegue a amenazar la vida de uno o más individuos). **[2]** Impida la investigación de delitos graves o facilite su comisión. **[3]** Datos clasificados como confidenciales.
7	**[1]** Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones. **[2]** Administración y gestión: probablemente impediría la operación efectiva de la organización. **[3]** Probablemente causaría una publicidad negativa generalizada **[3.1]** por afectar gravemente a las relaciones con otras organizaciones **[3.2]** por afectar gravemente a las relaciones con el público en general **[3.3]** por afectar gravemente a las relaciones con otros países **[4]** Probablemente cause perjudique la eficacia o seguridad de la misión operativa o logística. **[5]** Probablemente cause serios daños a misiones importantes de inteligencia o información. **[6]** Intereses comerciales o económicos: **[6.1]** de alto interés para la competencia **[6.2]** de elevado valor comercial

	[6.3] causa de graves pérdidas económicas **[6.4]** proporciona ganancias o ventajas desmedidas a individuos u organizaciones **[6.5]** constituye un serio incumplimiento de obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros **[7]** Obligaciones legales: probablemente cause un incumplimiento grave de una ley o regulación. **[8]** Seguridad: probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves. **[9]** Seguridad de las personas: probablemente cause daños de cierta consideración a varios individuos. **[10]** Probablemente cause un impacto significativo en las relaciones internacionales. **[11]** Datos clasificados como confidenciales.
6	**[1]** Información personal: probablemente afecte gravemente a un grupo de individuos. **[2]** Información personal: probablemente quebrante seriamente la ley o algún reglamento de protección de información personal. **[3]** Seguridad de las personas: probablemente cause daños de cierta consideración, restringidos a un individuo. **[4]** Orden público: probablemente cause manifestaciones, o presiones

	significativas. **[5]** Datos clasificados como de difusión limitada
5	**[1]** Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones. **[2]** Administración y gestión: probablemente impediría la operación efectiva de más de una parte de la organización. **[3]** Probablemente sea causa una cierta publicidad negativa. **[3.1]** por afectar negativamente a las relaciones con otras organizaciones **[3.2]** por afectar negativamente a las relaciones con el público. **[4]** Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local. **[5]** Probablemente dañe a misiones importantes de inteligencia o información. **[6]** Información personal: probablemente afecte gravemente a un individuo. **[7]** Información personal: probablemente quebrante seriamente leyes o regulaciones. **[8]** Obligaciones legales: probablemente sea causa de incumplimiento de una ley o regulación. **[9]** Probablemente tenga impacto en las relaciones internacionales. **[10]** Datos clasificados como de difusión limitad.

4	**[1]** Información personal: probablemente afecte a un grupo de individuos. **[2]** Información personal: probablemente quebrante leyes o regulaciones. **[3]** Seguridad de las personas: probablemente cause daños menores a varios individuos. **[4]** Dificulte la investigación o facilite la comisión de delitos. **[5]** Datos clasificados como de difusión limitada.
3	**[1]** Probablemente cause la interrupción de actividades propias de la Organización. **[2]**] Administración y gestión: probablemente impediría la operación efectiva de una parte de la organización. **[3]** Probablemente afecte negativamente a las relaciones internas de la Organización. **[4]** Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local). **[5]** Probablemente cause algún daño menor a misiones importantes de inteligencia o información. **[6]** Intereses comerciales o económicos: **[6.1]** de cierto interés para la competencia **[6.2]** de cierto valor comercial **[6.3]** causa de pérdidas financieras o merma de ingresos

	[6.4] facilita ventajas desproporcionadas a individuos u organizaciones **[6.5]** constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la proporcionada por terceros. **[7]** Información personal: probablemente afecte a un individuo. **[8]** Información personal: probablemente suponga el incumplimiento de una ley o regulación. **[9]** Obligaciones legales: probablemente sea causa de incumplimiento leve o técnico de una ley o regulación. **[10]** Seguridad: probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente. **[11]** Seguridad de las personas: probablemente cause daños menores a un individuo. **[12]** Orden público: causa de protestas puntuales. **[13]** Probablemente cause un impacto leve en las relaciones internacionales. **[14]** Datos clasificados como de difusión limitada
	[1] Probablemente cause una pérdida menor de la confianza dentro de la Organización. **[2]** Intereses comerciales o económicos: **[2.1]** de bajo interés para la competencia **[2.2]** de bajo valor comercial

2	**[3]** Información personal: pudiera causar molestias a un individuo **[4]** Información personal: pudiera quebrantar de forma leve leyes o regulaciones. **[5]** Seguridad de las personas: pudiera causar daño menor a varios individuos. **[6]** Datos clasificados como sin clasificar
1	**[1]** Pudiera causar la interrupción de actividades propias de la Organización. **[2]** Administración y gestión: pudiera impedir la operación efectiva de una parte de la organización. **[3]** Pudiera causar una pérdida menor de la confianza dentro de la Organización. **[4]** Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local). **[5]** Pudiera causar algún daño menor a misiones importantes de inteligencia o información. **[6]** Intereses comerciales o económicos: **[6.1]** de pequeño interés para la competencia **[6.2]** de pequeño valor comercial **[7]** Información personal: pudiera causar molestias a un individuo. **[8]** Obligaciones legales: pudiera causar el incumplimiento leve o técnico de una ley o regulación. **[9]** Seguridad: pudiera causar una merma en la seguridad o dificultar la

	investigación de un incidente. **[10]** Seguridad de las personas: pudiera causar daños menores a un individuo. **[11]**] Orden público: pudiera causar protestas puntuales. **[12]** Pudiera tener un impacto leve en las relaciones internacionales. **[13]**Datos clasificados como sin clasificar
0	**[1]** No afectaría a la seguridad de las personas. **[2]** Sería causa de inconveniencias mínimas a las partes afectadas. **[3]** Supondría pérdidas económicas mínimas. **[4]** No supondría daño a la reputación o buena imagen de las personas u organizaciones.

Amenazas y vulnerabilidades

[D] Disponibilidad
Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran la información y sus activos asociados.
¿Qué importancia tendría que el activo no estuviera disponible para la **Fundación Universitaria Tecnológico Comfenalco**?
➢ Un activo tiene un gran valor desde el punto de vista de disponibilidad si una amenaza afectara a su disponibilidad, las consecuencias serían graves.

- Un activo carece de un valor apreciable desde el punto de vista de disponibilidad cuando puede no estar disponible frecuentemente y durante largos periodo de tiempo sin por ellos causar mayor daño.

- La disponibilidad es una característica que afecta a todo tipo de activos.

- A menudo la disponibilidad requiere un tratamiento por escalones pues el coste de la indisponibilidad aumenta de forma no lineal con la duración de la interrupción, desde breves interrupciones sin importancia, pasando por interrupciones que causan daños considerables y llegando a interrupciones que no admiten recuperación: la organización está acabada.

[I] Integridad
Garantía de la exactitud y completitud de la información y los métodos de su procesamiento.
¿Qué importancia tendría que los datos fueran modificados fuera de control?

[C] Confidencialidad de los datos
Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.
¿Qué importancia tendría que el dato fuera conocido por personas no autorizadas?

➢ Los datos reciben una alta valoración desde el punto de vista de confidencialidad cuando su revelación causaría graves daños a la organización. ➢ Los datos carecen de un valor apreciable desde el punto de vista de confidencialidad cuando su conocimiento por cualquiera no supone preocupación alguna.

[A_S] Autenticidad de los usuarios del servicio
Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.
Aseguramiento de la identidad u origen.
¿Qué importancia tendría que quien accede al servicio no sea realmente quien se cree?
La autenticidad de los usuarios de un servicio es lo contrario de la oportunidad de fraude o uso no autorizado de un servicio. ➢ Un servicio recibe una elevada valoración desde el punto de vista de autenticidad cuando su prestación a falsos usuarios supondría un grave perjuicio para la **Fundación Universitaria Tecnológico Comfenalco**. ➢ Un servicio carece de un valor apreciable desde el punto de vista de autenticidad cuando su acceso por cualquiera no supone preocupación alguna.

[A_D] Autenticidad del origen de los datos
Aseguramiento de la identidad u origen.
¿Qué importancia tendría que los datos no fueran realmente imputables a quien se cree?

- Los datos reciben una elevada valoración desde el punto de vista de autenticidad del origen cuando un defecto de imputación causaría graves quebrantos a la organización. Típicamente, se habilita la oportunidad de repudio.
- Los datos carecen de un valor apreciable desde el punto de vista de autenticidad del origen cuando ignorar la fuente es irrelevante.

Fuente: Consejo Superior de Administración Electrónica, “Magerit V2, Metodología”, P. 23