# ESTUDIO DEL ESTADO DE SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA TECNOVAL SYSTEM PARA DESARROLLAR POLÍTICAS DE SEGURIDAD.

**SANDRA JOHANA BORREGO PLATA**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA**
**ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA**
**VALLEDUPAR**
**2019**

# ESTUDIO DEL ESTADO DE SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA TECNOVAL SYSTEM PARA DESARROLLAR POLÍTICAS DE SEGURIDAD.

**SANDRA JOHANA BORREGO PLATA**

**TRABAJO DE GRADO**

**ASESOR**
**EDGAR ALONSO BOJACA GARAVITO**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA**
**ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA**
**VALLEDUPAR**
**2019**

**NOTAS DE ACEPTACION**

_____

**FIRMA DE JURADO**

## DEDICATORIA

El presente trabajo de grado va dedicado a Dios, quien como guía estuvo presente en el caminar de mi vida, bendiciéndome y dándome fuerzas para continuar con mis metas trazadas sin desfallecer. A mi esposo que, con su apoyo incondicional, amor y confianza permitió que lograra culminar mi especialización, a mis padres y todos mis familiares por estar siempre apoyándome en las diferentes etapas de este proceso.

A todas las personas especiales que me acompañaron en esta etapa, aportando a mi formación tanto profesional y como ser humano.

## AGRADECIMIENTOS

A Dios, por haberme permitido llegar hasta este punto y haberme dado salud para lograr mis objetivos, además de su infinita bondad y amor. A mi esposo Luis Enrique, por ser parte importante en el logro de mis metas profesionales. Gracias por haber sido mi fuente de inspiración en mi deseo de proseguir estudios. A mis padres por ser el pilar fundamental en todo lo que soy, en toda mi educación, tanto académica, como de la vida, por su incondicional apoyo perfectamente mantenido a través del tiempo. A mis familiares, A mi hermana Eloísa por ser un gran apoyo y estar en los momentos más difíciles de mi vida, Gracias a todos mis familiares y aquellos que participaron directa o indirectamente en esta especialización.

¡Gracias a ustedes!

**CONTENIDO**

pág.

## LISTA DE FIGURAS

pág.

## LISTA DE TABLAS

pág.

# INTRODUCCION

La presente monografía, tiene como fin la aplicación del modelo MAGERIT versión 2 -Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información-, para poder llegar al objetivo principal que sería, contribuir a que la empresa TECNOVAL SYSTEM posea un conocimiento claro sobre los riesgos que pueden presentarse en sus sistemas de información.

Siguiendo una serie de pasos, empezando por un análisis de riesgos para la empresa TECNOVAL SYSTEM con el fin de garantizar mayor efectividad y eficiencia dentro de cada uno de los procesos; teniendo en cuenta que al conocer las fortalezas y debilidades se mejoran los controles y administración de recursos tecnológicos acorde a los estándares nacionales e internacionales que buscan proporcionar mecanismos y herramientas para adoptar buenas prácticas. Esta monografía es muy importante para la empresa TECNOVAL SYSTEM, ya que se están realizando todas las adecuaciones tecnológicas y de infraestructura para el ajuste de procesos y restructuración de las distintas áreas brindando a cada uno de los departamentos de la empresa el control de los riesgos de información basándose en reglas y controles claros que definan el mantenimiento de estas, minimizando los riesgos lo menor posible; mejorando así los objetivos claros establecidos. Beneficiando así a los usuarios de la empresa.

# 1. PLANTEAMIENTO DEL PROBLEMA

En la actualidad las grandes empresas Colombianas son conscientes de que necesitan tener una infraestructura informática segura, para minimizar riesgos asociados con la seguridad y los costos de administración y operaciones, por lo que, para ellos, la seguridad se ha convertido en un elemento de vital importancia al interior de la organización, por lo que no escatiman en invertir en el desarrollo, implantación y mantenimiento de políticas de seguridad.

Al igual que las grandes empresas, las medianas y pequeñas también están expuestas a una serie de riesgos, y/o amenazas latentes, las perdidas pueden ser millonarias por la falta de protección o de mecanismos que le permitan identificar con claridad sus procesos críticos, fallas y debilidades.

Por la misma naturaleza de la falta de formación de los propietarios de las PYME en el manejo general o especifico de recursos tecnológicos, que pueden estar asociado con la falta de capacitación o de recursos iniciales suficientes, la gran mayoría no cuenta con políticas de seguridad informáticas que le permitan determinar de manera preventiva los riegos a los que se encuentra expuesta la información relacionada con la actividad de su razón social y que es manejada mediante el uso de computadores y dispositivos tecnológicos. Ellos solo atienden a sus equipos de cómputos cuando estos presentan una falla física o lógica, aún más de estos tipos de procesos no se llevan registros, todo el manejo de controles de riesgos quedan al azar.

La atención de estas fallas se la delegan a personal externo a la empresa, con perfil técnico y profesional en sistemas y electrónica, los cuales solo cumplen con la acción de poner en funcionamiento la máquina y salvaguardar la información en la medida de sus posibilidades. No hay específicamente quien los supervise.

TECNOVAL SYSTEM a pesar de ser una empresa que se dedica a comercializar elementos de seguridad tales como cámaras, alarmas comunitarias, ventas de computadores, impresoras y otros elementos informáticos carece de políticas o estrategias organizacionales que le permitan controlar la integralidad, disponibilidad y confiabilidad de su información, producto de la ejecución de las actividades propias de su razón social. Encontramos que su red de datos tiene una mínima seguridad en

la configuración de su cifrado, los dispositivos de interconexión de red se encuentran expuestos a terceros, entre otros.

¿De qué manera un estudio en la seguridad de la información de la empresa TECNOVAL SYSTEM ayudaría a identificar, aplicar y ejecutar una correcta política de seguridad en su información?

# 2. JUSTIFICACIÓN

En la actualidad las microempresas en Colombia constituyen la fuerza de trabajo que más mueve la economía, algunas de ellas invierten en tecnología para mejorar su perfil y ser más competitivas, sin embargo ante el manejo y control de la tecnología actúan de manera reactiva, quizás porque no cuentan con la asesoría necesaria que les haga ver lo importante que es trabajar de manera preventiva y con políticas de seguridad sobre tecnología, en aras de que esta le preste su servicio de forma óptima y le permita disminuir los riesgos a los que está expuesta su información, siempre que sea manipulada con dispositivos electrónicos.

Con los resultados de esta monografía se pretende crear una serie de pasos y recomendaciones que sirvan de guía a la empresa TECNOVAL SYSTEM para así minimizar los riesgos a los que están expuestas.

Las organizaciones vienen siendo objeto de incontables intentos a diario por hacerse a la información y control de sus equipos de cómputo por parte de los delincuentes informáticos. Para muchas de las empresas que han sido víctimas de ataques informáticos, no ha sido prioridad capacitar el personal y la indagación respecto a las posibles medidas de seguridad que deben tomarse para prevenirlos.

Por ende, el desarrollo de la presente monografía (Estudio del estado de Seguridad de la información de la empresa TECNOVAL SYSTEM para desarrollar políticas de seguridad) Se convierte en una necesidad de gran importancia la cual pretende indagar y poner en conocimiento las diferentes herramientas que se encuentran disponibles en pro de elevar el nivel de seguridad informática de la organización.

El desarrollo de esta monografía es muy importante para la empresa TECNOVAL SYSTEM, ya que se están realizando todas las adecuaciones tecnológicas y de infraestructura para el ajuste de procesos y restructuración de las distintas áreas brindando a cada uno de los departamentos de la empresa el control de los riesgos de información basándose en reglas y controles claros que definan el mantenimiento de los mismas, minimizando los riesgos lo menor posible; mejorando los objetivos claros establecidos. Beneficiando así a los usuarios de la empresa.

# 3. OBJETIVOS

## 3.1. OBJETIVO GENERAL

Desarrollar un análisis de seguridad de la información, de la empresa TECNOVAL SYSTEM para determinar políticas de seguridad de la información.

## 3.2. OBJETIVOS ESPECÍFICOS

- Analizar el estado actual de la infraestructura tecnológica de TECNOVAL SYSTEM.
- Identificar los riegos a los que se encuentra expuesta la infraestructura tecnológica de TECNOVAL SYSTEM
- Desarrollar políticas de seguridad informática para el manejo de la infraestructura de TECNOVAL SYSTEM.

# 4. MARCO REFERENCIAL

## 4.1. MARCO CONCEPTUAL

Partiendo de la necesidad de determinar el estado de seguridad de la información mediante un diagnóstico en TECNOVAL SYSTEM y en vista de que actualmente se tiene una infraestructura tecnológica en crecimiento, se plantea realizar el análisis de riesgos a partir de la revisión de algunos antecedentes.

Existen diferentes estándares que se desarrollaron para gestionar la seguridad de la información, algunos más generales, algunos centrados en la gestión de riesgos, y otros incluso tendientes a desarrollar un modelo de madurez de la seguridad de la información; sin embargo, en la especificación de estos no se afronta su aplicación a un grupo empresarial, lo cual requiere consideraciones adicionales.

Estos estándares varían de acuerdo con la aplicabilidad que se le puedan dar en los diferentes campos en que se estén desempeñando, por ejemplo, estándares ISO/IEC 27000 que integran un sistema de administración de seguridad de la información (information security management system ISMS) el cual está enfocado en la seguridad de la información bajo un explícito control administrativo de la misma.

El ISO 15408 es un estándar desarrollado en lo que se conoce como “Criterio Común” y que permite que muchas diferentes aplicaciones de software puedan ser integradas y probadas en una forma o manera segura.

El RFC 2196 es memorándum publicado por el Internet Engineering Task Force para el desarrollo de políticas y procedimientos de seguridad para sistemas de información conectados a Internet; proporciona una amplia y general visión de la seguridad de la información incluyendo la seguridad de la red, respuesta a incidentes o las políticas de seguridad. El documento es muy práctico y centrado en el día a día de las operaciones.[1] Muchos de los planteamientos y problemas en seguridad informática se encaminan a protegerse contra accesos no autorizados, pero este es un problema sencillo de resolver, ya que durante años se han desarrollado y perfeccionado

[1] Tomado de la página web: http://isamex.org/intechmx/index.php/2018/02/26/los-estandares-seguridad-informatica-aplica-a-la-industria-actual/

algoritmos matemáticos para el cifrado de datos, para el intercambio seguro de información. El problema va mucho más allá. La Seguridad Informática es un problema cultural, en el que el usuario juega un papel muy importante. La metodología para el aseguramiento de entornos informatizados - MAEI2, resalta la importancia de tener una metodología clara para realizar un análisis de riesgos e identificar claramente vulnerabilidades, riesgos y amenazas presentes en los activos de información, ser gestionados y que permita optimizar los procesos organizacionales.

## 4.2. MARCO TEORICO

### 4.2.1. Seguridad de la Información

Se podría definir como seguridad de la información a un estado específico de la misma sin importar su formato, que nos indica un nivel o un determinado grado de seguridad de información, por ejemplo, que está libre de peligro, daño o riesgo, o por el contrario que es vulnerable y puede ser objeto de materialización de una amenaza. Las vulnerabilidades, el peligro o el daño de la misma es todo aquello que pueda afectar su funcionamiento directo y la esencia en sí de la información, o en su defecto los resultados que se obtienen de la consulta, administración o procesamiento de ella.

Garantizar un nivel de protección total es virtualmente imposible[2], la seguridad de la información en la práctica a un nivel total o de completitud no es alcanzable porque no existe un sistema seguro al ciento por ciento. Para dar una solución a este inconveniente de no existir una protección total, no exacta, pero sí que nos ayude a hacerlo lo mejor posible, existe un planteamiento denominado [3]Desarrollo de una

[2] ISO 2700. Sistema de gestión de seguridad de la información. Términos de uso información iso27000.es ©, 2012

[3]

metodología para la auditoría de riesgos informáticos (físicos y lógicos) y su aplicación al departamento de informática de la dirección provincial de pichincha del consejo de la judicatura, donde se afirma que la información está expuesta a un mayor rango de amenazas y vulnerabilidades. La información adopta diversas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en video o hablada en cualquier tipo de conversación". Debería protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparta o almacene.

La seguridad de la información protege a una organización que la adopte como parte de su visión y misión de un amplio rango de amenazas para asegurar la continuidad del negocio, minimizar los posibles daños y maximizar el retorno de las inversiones y las oportunidades. La información digital o en papel y los procesos que la apoyan, los sistemas y redes son importantes activos de la organización.

Las organizaciones y sus sistemas de información se enfrentan, cada vez más, con riesgos e inseguridades procedentes de una amplia variedad de fuentes, incluyendo fraudes basados en informática, espionaje, sabotaje, vandalismo, incendios o inundaciones. Ciertas fuentes de daños como virus informáticos y ataques de intrusión o de negación de servicios se están volviendo cada vez más comunes, ambiciosos y sofisticados.

La seguridad de la información es importante en negocios tanto del sector público como del privado para proteger las infraestructuras críticas. En ambos sectores, la seguridad de información permitirá, lograr el gobierno electrónico o el comercio electrónico, evitando y reduciendo los riesgos relevantes. La interconexión de las redes públicas y privadas y el compartir los recursos de información aumentan la dificultad de lograr el control de los accesos.

Es necesario que exista seguridad en el activo más importante de la organización por las siguientes razones:

Gran variedad de Riesgos y Amenazas: Fraudes, espionaje, sabotaje, vandalismo, incendio, inundación, hacking, virus, denegación de servicio, etc; Provenientes de múltiples fuentes.

- Mayor vulnerabilidad a las amenazas por la dependencia de los sistemas y servicios de información interconectados.
- La mayoría de los sistemas de información no han sido diseñados para ser seguros.

### 4.2.2. Análisis de Riesgos Informáticos

Antes de definir lo que es el análisis de riesgos, tenemos que considerar lo que es un riesgo, se exponen las siguientes definiciones:

Según Fernando Izquierdo Duarte: “El Riesgo es un incidente o situación, que ocurre en un sitio concreto durante un intervalo de tiempo determinado, con consecuencias positivas o negativas que podrían afectar el cumplimiento de los objetivos”.

Según Martín Vilches Troncoso: “El Riesgo es cualquier variable importante de incertidumbre que interfiera con el logro de los objetivos y estrategias del negocio. Es decir, es la posibilidad de la ocurrencia de un hecho o suceso no deseado o el desacierto de uno deseado”.

Con base a estos significados, entonces, podemos referirnos a que el proceso de análisis de riesgos debe ser el más importante de la gestión de la seguridad de la información de una organización, de aquí parte la gestión de los riesgos, que es en últimas con la que se decide tomar la decisión de eliminarlos, ignorarlos, mitigarlos y controlarlos, es decir aplicar la gestión de riesgos basados en la compleja tarea de determinar, analizar, evaluar y clasificar los activos de información más importantes según la criticidad de los mismos.

Actualmente se han tratado de clasificar los diferentes tipos de riesgos para que sea más fácil la aplicación de un análisis de estos, entre los más comunes están los

riesgos de negocios, inherentes, de auditoría, operativos y de control, profesionales y de tecnología entre otros. Además, a nivel general se debe tener claro el objetivo del análisis de riesgo estableciendo a su vez una escala valorativa y con cierta regla de priorización de los mismos, luego de que se tiene una escala definida y los riesgos catalogados y organizados todo se debe condensar en una matriz que muestre realmente el nivel de impacto según nuestra escala de valoración, buscando establecer al final el estado actual en materia de seguridad de la información.

### 4.2.3. Herramienta P.I.L.A.R

PILAR, es el acrónimo de “Procedimiento Informático-Lógico para el Análisis de Riesgos” es una herramienta desarrollada por el Centro Nacional de Inteligencia de Madrid para soportar el Análisis de Riesgos de Sistemas de Información basado en la metodología MAGERIT.

Esta herramienta puede hacer todas las actividades que se realizan en el Análisis y Gestión de Riesgos:

- Determinación de Activos: Identificación, dependencias y valoración.
- Determinación de Amenazas
- Estimación de Impactos
- Determinación de los criterios de aceptación del riesgo
- Determinación de las medidas de seguridad necesarias o Salvaguardas.

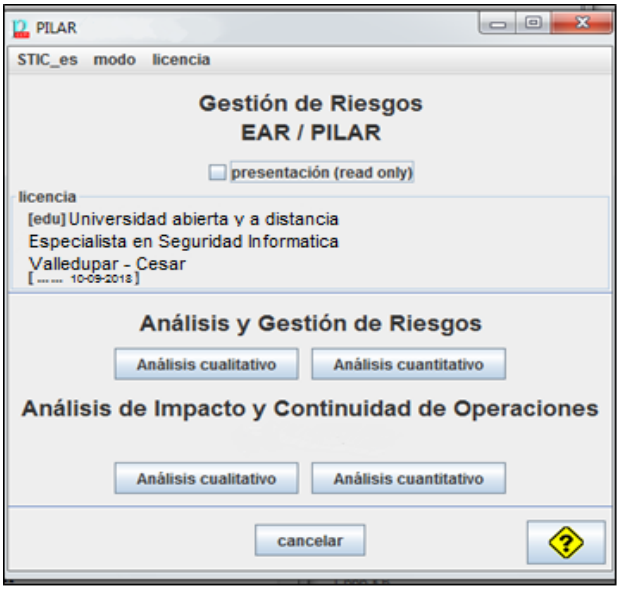
Este software permite hacer un Análisis de Riesgos sobre las dimensiones de valoración como son: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

Además nos ayuda con el cálculo del impacto y el riesgo, acumulado, repercutido, potencial y residual.

“Las salvaguardas se califican por fases, permitiendo la incorporación a un mismo modelo de diferentes situaciones temporales. Típicamente se puede incorporar el resultado de la diferente monografía de seguridad a lo largo de la ejecución del plan de seguridad, monitorizando la mejora del sistema.”[4]

PILAR puede hacer análisis cuantitativo y cualitativo.

Figura 1. Herramienta PILAR




Fuente: Autor a partir de herramienta

Los resultados se presentan en diversos formatos como son: gráficas y tablas donde se pueden incorporar hojas de cálculo.

### 4.3. MARCO CONTEXTUAL

TECNOVAL SYSTEM es una empresa dedicada a ofrecer soluciones tecnológicas, soporte técnico y desarrollo de dispositivos en el ámbito Electrónico, con ideal de brindar alternativas que mejoren la seguridad en el hogar, las empresas y en la comunidad, cuenta con un trato digno obrando siempre bien, para seguir creciendo y continuar desempeñando un papel importante en el logro de nuestra meta. Tratamos

[4] Magerit-versión 3 .0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro 1-Método, https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/ç, p. 125

siempre de ofrecer el mejor servicio, aplicando nuestras políticas empresariales como son respeto, honestidad y responsabilidad y así satisfacer al máximo las exigencias que este campo de desarrollo necesita y cumplirles a cabalidad a nuestros clientes.

Figura 2. Oficina comercial Tecnoval


Fuente: Archivos de Tecnoval System

Figura 3. Tecnoval System Ventas

Fuente: Archivos de Tecnoval System

### 4.3.1. Razón Social.

TECNOVAL SYSTEM

### 4.3.2. Ubicación.

Está ubicada en la Calle 12c # 19d - 2, en la ciudad de Valledupar, capital del departamento del Cesar, Colombia.

### 4.3.3. Breve reseña histórica.

La empresa “TECNOVAL SYSTEM” se encuentra ubicada en la ciudad de Valledupar, departamento del cesar, Colombia, es una mediana empresa que se dedica a ofrecer soluciones tecnológicas y de consultoría enfocada a ciberseguridad, La empresa fue fundada en Valledupar, con una variedad de productos para satisfacer las necesidades tecnológicas y de seguridad que están en el mercado. Cuenta con una sede. Su oferta de productos está respaldada por importantes marcas, lo que permite garantizar excelente calidad en el servicio, la atención y el asesoramiento técnico que los clientes requieren.

### 4.3.4. Objetivos institucionales.

Nuestro compromiso con nuestros clientes es brindar un servicio integral:

- A nuestros clientes de distribución les brindaremos el respaldo requerido para la venta de nuestros productos.
- A nuestros clientes les brindamos asesoría técnica y un servicio integral en la revisión, venta e instalación de todo tipo de Baterías en nuestras instalaciones y en servicio a domicilio.

En ambos casos, con un personal altamente capacitado y a un precio competitivo, cumpliendo y superando sus expectativas, mejorando continuamente el control de nuestros procesos por medio de un eficaz Sistema de Gestión de la Calidad para beneficio de la empresa, los clientes y colaboradores

### 4.3.5. Valores corporativos

- **Respeto**: Escuchamos, entendemos y valoramos al otro, buscando armonía en las relaciones interpersonales, laborales y comerciales.
- **Equidad**: Facilitamos el desarrollo integral del asociado, mediante la distribución justa e imparcial.
- **Honestidad**: realizamos todas las operaciones con trasparencia y rectitud.
- **Responsabilidad**: Obramos con seriedad, en consecuencia, con nuestros deberes y derechos como empresa.
- **Integridad**: Actuamos con firmeza, rectitud, honestidad, coherencia y sinceridad.

### 4.3.6. Misión

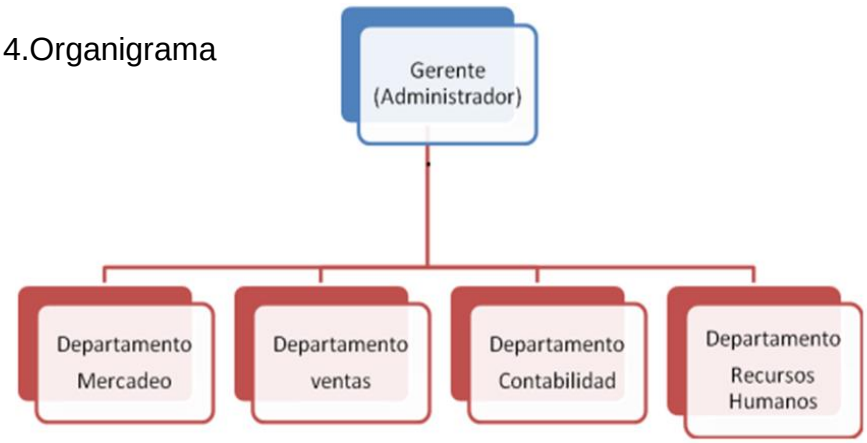
Suplir la demanda de nuestros clientes en la ciudad de Valledupar y el departamento del Cesar a través del suministro oportuno de nuestros productos y servicios con todo el respaldo técnico requerido para garantizar su satisfacción.

### 4.3.7. Visión

Ser la empresa líder en el departamento y Colombia, ofreciendo productos y servicios de alta calidad.

### 4.3.8. Organigrama

Figura 4.Organigrama




Fuente: Archivos de Tecnoval System

# 5. ACTIVIDADES PRELIMINARES

Antes de iniciar se debe especificar que este monografía arroja resultados tanto cualitativos como cuantitativos, ya que, los resultados se dan en diferente tipo de formato, tanto en solución de problema que genera mayor productividad a la hora de ver el rendimiento de la empresa; con las etapas de Análisis y Gestión de Riesgos (AGR) de los sistemas de información (S.I.) de la empresa TECNOVAL SYSTEM.

Para ello se realizarán las siguientes tareas:

- Estudio de oportunidad
- Determinación del alcance de la monografía
- Planificación de la monografía
- Lanzamiento de la monografía

La monografía de AGR será desarrollado con la metodología MAGERIT versión 3 bajo la aplicación de la herramienta PILAR versión 5.2.9.

Para que sea eficiente la presente etapa, se deberá contar con la ayuda y colaboración de todo el personal involucrado con los sistemas de información.

## 5.1. ESTUDIO DE OPORTUNIDAD

En la empresa TECNOVAL SYSTEM se han beneficiado de la colaboración que brindan las nuevas tecnologías informáticas y comunicación a su funcionamiento, pero no se han percatado de los problemas de seguridad que estas tecnologías traen.

Mediante entrevistas y encuestas realizadas a los empleados de los departamentos de: Recursos Humanos, Financiero, Contabilidad y Ventas de esta empresa, se ha percibido que se ha generado incidentes significativos relacionados a la seguridad. (Ver Anexo A. Encuestas realizadas a los empleados).

Como es la falta de mantenimiento a los soportes de información, donde la información queda vulnerable para los empleados que acceden a ella.

El ambiente inadecuado donde está situado el servidor que almacena la información del sistema, al mismo tiempo del crecimiento acelerado de la base de datos.

En cuanto a las contraseñas de cada computadora de escritorio, no son confidenciales, lo que puede provocar robo de información.

Los antivirus que están desactualizados, y por último un pésimo respaldo de la información.

# 6. ALCANCE

## 6.1. DETERMINACIÓN DEL ALCANCE

Después de haber comprobado la oportunidad de ejecutar la monografía de Análisis y Gestión de Riesgos, en esta fase se procede a identificar los objetivos que debe cumplir el monografía y definir su dominio y límites.

Los objetivos se ordenan en tres ciclos

- Definir una programación orientada a la seguridad del sistema de información.
- Analizar el estado actual de la empresa y especificar cuáles son las necesidades de mayor importancia respecto a la seguridad.
- Escoger mecanismos de salvaguarda.

El dominio de monografía se centra en los Departamentos de Contabilidad, Financiero, Recursos Humanos y Ventas.

Los empleados de los diferentes departamentos que van a estar involucrados en la realización de la monografía:

- Ing. Luis Enrique Morales Nieves - jefe del Departamento de Financiero
- Ing. José Alfonso Triana - Ventas
- José Álvaro Plata - jefe del Departamento de Contabilidad
- José Alberto Mora - Auxiliar Contable
- Nelva Luquez - jefa del Departamento de Recursos Humanos
- Cesar Augusto Arzuaga - Persona encargada del mantenimiento de los equipos informáticos
- Viviana Carolina Plata – Digitadora

## 6.2. PLANIFICACIÓN

En la empresa TECNOVAL SYSTEM, para la realización de las entrevistas y encuestas se programará una cita a cada entrevistado en un plazo no mayor a 7 días laborables.

Las entrevistas nos permitirán determinar por ámbito a los usuarios afectados y a planificar la intervención de ellos en la monografía.

Y las encuestas arrojarán porcentajes exactos sobre las fallas de seguridad en los sistemas de información y su demás entorno. (Ver Anexo A. Encuestas realizadas a los empleados)

La monografía AGR de los Sistemas de Información de la empresa TECNOVAL SYSTEM está constituido por los siguientes órganos:

- Equipo: Sandra Borrego estudiante de Especialista en Seguridad Informática de la Universidad Abierta y a Distancia.

- Grupo de usuarios: está formado por los utilizadores, actuales del Sistema de Información.

## 6.3. LANZAMIENTO

Para la recolección de la información se han escogido las fichas de captura de datos de la Metodología MAGERIT, ya que se ajusta a las necesidades de este tipo de monografías.

Las fichas de captura de datos recogen información específica de cada activo perteneciente a la empresa tomando en cuenta como dimensiones de seguridad y dependencias de activos, que ayudará a identificar correctamente lo que son: vulnerabilidades, impactos, salvaguardas efectivas. La situación de la seguridad de

los sistemas de información de la empresa TECNOVAL SYSTEM. Es el resultado de la incorporación de salvaguardas tomadas para prevenir o reducir riesgos que no han sido debidamente estudiadas de forma sistemática. Hasta ahora no se ha encontrado ningún fallo operacional informático de envergadura en el que se hayan forzado a tomar precauciones drásticas. (Ver Anexo B. Fichas para la recolección de datos)
Gracias al análisis de riesgos permitirá sistematizar las medidas actuales y mejorarlas con algunas otras que serán suficientes para lograr un nivel de seguridad estable.
En esta empresa se disponen de los recursos a utilizarse para el desarrollo de la monografía en disponibilidad de equipos, tiempos planificados, medios materiales-herramientas, envío de documentos y manuales.

Primeramente, se estableció la comunicación con las unidades involucradas sobre el lanzamiento de la monografía. Se tuvo comunicación con el Ing. Luis Enrique Morales Nieves, sobre la monografía y su contenido, quien supo informar a los departamentos implicados sobre la monografía y que estén prestos ayudarnos para el desarrollo del mismo. Además, se envió un oficio a la Gerencia (Ver Anexo C. Oficio dirigido al Gerente) en el cual se indicaba la monografía, la metodología y demás parámetros formales para un buen desempeño de la monografía de Análisis y Gestión de Riesgos. Indicando lo anterior, se informó que la monografía está autorizado y listo para su ejecución.

# 7. METODOLOGIA

Para el desarrollo de la metodología de esta monografía se escogió la Metodología MAGERIT, ya que es la más se ajusta a las necesidades de este tipo de monografía.

Las fichas de captura de datos recogen información específica de cada activo perteneciente a la empresa tomando en cuenta como dimensiones de seguridad y dependencias de activos, lo cual ayuda a identificar correctamente lo que son: vulnerabilidades, impactos salvaguardas efectivas. La situación de la seguridad de los sistemas de información de la empresa TECNOVAL SYSTEM, es el resultado de la incorporación de salvaguardas tomadas para prevenir o reducir riesgos que no han sido debidamente estudiadas de forma sistemática.

Gracias al análisis de riesgos permite sistematizar las medidas actuales y mejorarlas con algunas otras que serán suficientes para lograr un nivel de seguridad estable.

Esta empresa dispone de los recursos a utilizarse para el desarrollo de la monografía en disponibilidad de equipos, tiempos planificados, medios materiales-herramientas, envió de documentos y manuales.

## 7.1. ANÁLISIS DE RIESGOS.

Esta etapa se constituye en el núcleo central de MAGERIT, y su correcta aplicación condiciona la validez y utilidad de toda la monografía.

Mediante el Análisis de Riesgos se debe alcanzar los siguientes objetivos:

- Determinar los activos más significativos que posee la empresa
- Establecer las amenazas a las que están expuestos cada activo.
- Escoger salvaguardas apropiadas para los activos
- Estimar el impacto si se materializara alguna amenaza.

Para la ejecución de esta fase, la recolección de la información es desarrollada mediante encuestas y entrevistas a los usuarios responsables de los sistemas de información de la empresa TECNOVAL SYSTEM**.**

- Mediante el análisis de riesgos se puede saber cuánto vale y como están protegidos los activos evaluándolos de manera metódica para obtener conclusiones con fundamento.

## 7.2. CARACTERIZACIÓN DE LOS ACTIVOS

Acá se divide en tres sub-tareas:

- Identificar los activos
- Dependencias entre los activos
- Valoración de los activos

Con esto se reconocen los activos que componente el sistema, definir las dependencias entre ellos, y determinar de parte del valor del sistema se soporta en cada activo. Es como establecer el conocimiento general de la empresa.[5]

### 7.2.1. Identificación de los Activos

Con una buena identificación se permite establecer las siguientes tareas:

- Establecer las dependencias entre los activos
- Permite valorar a los activos con precisión.
- Ayuda a identificar y valorar amenazas
- Escoge que salvaguardas serán necesarios para proteger el sistema.

- **Servicios Internos**

  Para los empleados, de esta empresa se presta los siguientes servicios

  Internet

- **Aplicaciones**

  Algunas de las aplicaciones que se manejan

  - ✓ Ofimática

[5] Magerit-versión 3 .0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro 1-Método, https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/ç, p 37

- ✓ Antivirus
- ✓ Sistemas operativos
- ✓ Entre otros software

- **Equipos**

  Dentro de los equipos informáticos que posee la empresa tenemos los siguientes:

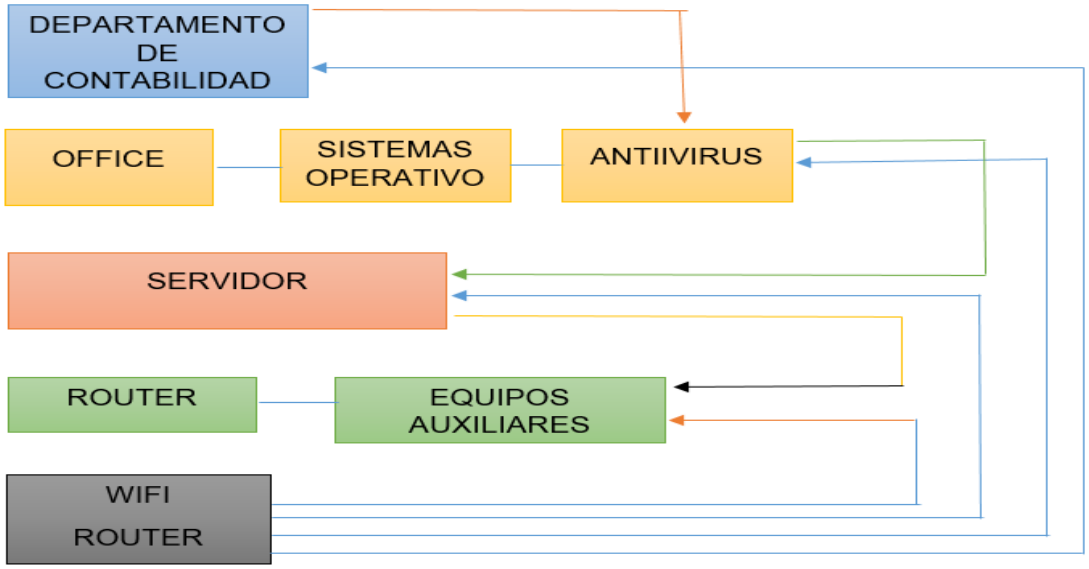
  - ✓ Servidor de Base de Datos
  - ✓ Medios de Impresión
  - ✓ Computadoras de escritorio
  - ✓ Router

- **Equipamiento Auxiliar**
  - ✓ Generador eléctrico
  - ✓ Cableado
  - ✓ Mobiliario
  - ✓ Sistema de Vigilancia
- **Personal**
  - ✓ Jefe de departamento recursos humanos
  - ✓ Jefe de departamento de contabilidad
  - ✓ Jefe de departamento mercadeo
  - ✓ Jefe de departamento de ventas

### 7.2.2. Dependencia de Activos

Reconocer la dependencia entre activos, es decir, la medida en que un activo de orden superior se puede ver perjudicado por una amenaza materializada sobre un activo de orden inferior.

Figura 5.Diagrama de Dependencia entre los Activos




Fuente: Autor

La dependencia va desde el “Departamento de Contabilidad”, que es fundamental en sus actividades por eso se encuentra en la parte superior

Los programas que están instalados en los equipos son importantes como es el caso del paquete de office ya que pueden hacer reportes e informes, en el mismo nivel están los sistemas operativos y los antivirus

El servidor está por encima de todos los equipos porque es el que almacena la información

En los activos inferiores están el router, los equipos auxiliares.

Los activos de menor jerarquía como son la red Wifi.

Todos estos activos están dentro de un mismo edificio.

### 7.2.3. Valoración de los Activos

Para cada valoración conviene tomar en consideración la siguiente información

Tabla 1. Criterios de Valoración

| CRITERIOS DE LA VALORACION | |
|---|---|
| **NIVEL** | **CRITERIO** |
| 10 | Nivel 10 |
| 9 | Nivel 9 |

Tabla 1. (Continuación)

| | |
|---|---|
| 8 | Nivel 8(+) |
| 7 | Alto |
| 6 | Alto(-) |
| 5 | Medio(+) |
| 4 | Medio |
| 3 | Medio(-) |
| 2 | Bajo(+) |
| 1 | Bajo |
| 0 | Depreciable |

Fuente: Autor a partir de la metodología

**Dimensiones**

- [D] disponibilidad
- [I] integridad de los datos
- [C] confidencialidad de los datos
- [A] autenticidad de los usuarios y de la información
- [T] trazabilidad del servicio y de los datos

Tabla 2. Valor propio de los activos

| | **Dimensiones** | | | | |
|---|---|---|---|---|---|
| **Activos** | **[D]** | **[I]** | **[C]** | **[A]** | **[T]** |
| **Servicios internos** | | | | | |
| Internet | [8](1) | | | [8] | [8] |
| **Aplicaciones** | | | | | |
| Ofimática | | | | | [7] |
| Antivirus | | | | | [7] |
| Sistema Operativo | | | | | [7] |
| Otros Software | | | | | [5] |
| **Equipos** | | | | | |
| Servidor de Base de Datos | | [9] | [9] | [9] | [9] |
| Medios de Impresión | | | | | [6] |
| Computadoras de Escritorio | | | | | [8] |
| Router | | | | | [8] |

Tabla 2. (Continuación)

| | | | | | |
|---|---|---|---|---|---|
| **Comunicaciones** | | | | | |
| Telefonía IP | | [7] | | | |
| Red WIFI | | | | | [7] |
| Red LAN | | | | | [7] |
| Internet | | [7] | [7] | | |
| **Equipos Auxiliares** | | | | | |
| CABLEADO | [7](2) | | | | |
| Mobiliario | [7] | | | | |
| Sistema de Vigilancia | [7] | | | | |
| Otros Equipos Auxiliares | [5] | | | | |
| **Soportes de Información** | | | | | |
| CD | | [7] | [7] | | |
| **Instalaciones** | | | | | |
| Edificio | | | [8] | | |
| **Personal** | | | | | |
| Jefa del Dto. de Contabilidad | | | [8] | | |
| Jefa del Dto. de Recursos humanos | | | [8] | | |
| Jefa del Dto. de ventas | | | [8] | | |
| Jefa del Dto. de mercadeo | | | [8] | | |
| Auxiliar de Contabilidad | | | [7] | | |
| Digitadora | | | [6] | | |

Fuente: Autor a partir de la metodología

- Pudiera causar la interrupción de actividades propias de la Organización
- Pérdida de Confianza (Reputación):

El resultado de esta primera tarea es el informe de Modelo de Valor (Ver Anexo E.) donde se describe detalladamente cada uno los activos antes mencionados.

## 7.3. CARACTERIZACIÓN DE LAS AMENAZAS|

Según MAGERIT, las amenazas están clasificadas en cuatro grupos:

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

El objetivo de estas tareas es caracterizar el entorno al que se enfrenta el sistema, que puede pasar, que consecuencias se derivan y como de probable es que pase. Podemos resumirlo en la expresión “conoce a tu enemigo”[6]

Esta actividad consta de 2 sub-tareas:

- Identificación de las amenazas
- Valoración de la amenazas

### 7.3.1. Identificación de las amenazas

El objetivo de esta tarea:

✓ Identificar las amenazas relevantes sobre cada activo

Tabla 3. Identificación de Amenazas a cada uno de los activos

| Activos | Amenazas |
|---|---|
| INTERNET | [A.7] Uso no previsto |
| OFIMÁTICA | [E.1] Errores de los usuarios<br>[E.20] Vulnerabilidades de los programas (software)<br>[E.21] Errores de mantenimiento /actualización de programas (software)<br>[A.8] Difusión de software dañino |

[6] Magerit-versión 3 .0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro 1-Método, https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/ç, p 40

| | |
|---|---|
| ANTIVIRUS | [E.8] Difusión de software dañino<br>[E.20] Vulnerabilidades de los programas (software)<br>[E.21] Errores de mantenimiento / actualización de programas (software) |
| SISTEMA OPERATIVO | [I.5] Avería de origen físico o lógico<br>[E.1] Errores de los usuarios<br>[E.8] Difusión de software dañino<br>[E.20] Vulnerabilidades de los programas (software)<br>[E.21] Errores de mantenimiento / actualización de programas (software)<br>[A.7] Uso no previsto |
| OTROS SOFTWARE | [E.8] Difusión de software dañino<br>[E.20] Vulnerabilidades de los programas (software)<br>[E.21] Errores de mantenimiento / actualización de programas (software) |
| SERVIDOR DE BASE DE DATOS | [N.1] Fuego<br>[N.2] Daños por agua<br>[N.*] Desastres naturales<br>[I.3]Contaminación medioambiental<br>[I.5] Avería de origen físico o lógico<br>[I.7] Condiciones inadecuadas de temperatura o humedad<br>[E.2] Errores del administrador del sistema / de la seguridad<br>[E.23] Errores de mantenimiento / actualización de equipos (hardware)<br>[A.11] Acceso no autorizado [A.23]<br>Manipulación del hardware |
| MEDIOS DE IMPRESIÓN | [I.5] Avería de origen físico o lógico<br>[I.7] Condiciones inadecuadas de temperatura o humedad |

| | |
|---|---|
| | [E.23] Errores de mantenimiento / actualización de equipos (hardware)<br>[A.11] Acceso no autorizado |
| COMPUTADORA DE ESCRITORIO | [N.2] Daños por agua [N.*]<br>Desastres naturales<br>[I.*] Desastres industriales<br>[I.5] Avería de origen físico o lógico<br>[I.7] Condiciones inadecuadas de temperatura o humedad<br>[E.23] Errores de mantenimiento / actualización de equipos (hardware)<br>[E.24] Caída del sistema por agotamiento de recursos<br>[A.6] Abuso de privilegios de acceso<br>[A.7] Uso no previsto |
| ROUTER | [N.1] Fuego<br>[N.2] Daños por agua [N.*]<br>Desastres naturales<br>[I.3] Contaminación medioambiental<br>[I.5] Avería de origen físico o lógico<br>[I.7] Condiciones inadecuadas de temperatura o humedad [A.11] Acceso no autorizado |
| RED WIFI | [I.8] Fallo de servicios de comunicaciones<br>[E.9] Errores de [re-]encaminamiento |
| RED LAN | [I.8] Fallo de servicios de comunicaciones<br>[E.9] Errores de [re-]encaminamiento<br>[E.10] Errores de secuencia<br>[A.5] Suplantación de la identidad del usuario [A.9] [Re-]encaminamiento de mensajes [A.10] Alteración de secuencia<br>[A.11] Acceso no autorizado |

| | |
|---|---|
| INTERNET | [I.8] Fallo de servicios de comunicaciones<br>[E.15] Alteración de la información |
| CABLEADO | [I.3] Contaminación medioambiental<br>[I.7] Condiciones inadecuadas de temperatura o humedad |
| MOBILIARIO | [I.3] Contaminación medioambiental |
| SISTEMA DE VIGILANCIA | [I.3] Contaminación medioambiental<br>[I.7] Condiciones inadecuadas de temperatura o humedad |
| SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA | [I.3] Contaminación medioambiental |
| OTROS EQUIPOS AUXILIARES | [I.3] Contaminación medioambiental |
| CD | [E.15] Alteración de la información<br>[E.19] Fugas de información<br>[A.15] Modificación de la información<br>[A.19] Revelación de información |
| EDIFICIO | [N.1] Fuego<br>[N.2] Daños por agua<br>[N.*.1] Tormentas [N.*.4] Terremotos [N.*.9] Tsunamis [N.*.11] Calor extremo<br>[I.*] Desastres industriales<br>[A.27] Ocupación enemiga |
| JEFA DEL DTO. FINANCIERO | [E.28.1]Enfermedad<br>[E.28.2]Huelga<br>[A.29] Extorsión<br>[A.30] Ingeniería social (picaresca) |

| | |
|---|---|
| MANTENIMIENTO | [E.4] Errores de configuración |
| BD | [E.19.3] A personas externas que no necesitan conocerlo |
| MANTENIMIENTO EQ | [E.4] Errores de configuración<br>[E.19.3] A personas externas que no necesitan conocerlo<br>[A.29.2] Ataque desde el interior |
| JEFA DEL DTO. DE CONTABILIDAD | [E.28.1] Enfermedad<br>[E.28.2] Huelga<br>[A.29] Extorsión<br>[A.30] Ingeniería social (picaresca) |
| JEFA DEL DTO. DE LOGÍSTICA Y COMPRAS | [E.28.2] Huelga<br>[A.29] Extorsión<br>[A.30] Ingeniería social (picaresca) |
| JEFA DEL DTO. DE PERSONAL | [E.28.1] Enfermedad<br>[E.28.2] Huelga<br>[A.29] Extorsión |
| AUXILIAR DE CONTABILIDAD | [E.28.1] Enfermedad<br>[E.28.2] Huelga<br>[A.29] Extorsión<br>[A.30] Ingeniería social (picaresca) |
| DIGITADORA | [A.29] Extorsión<br>[A.30] Ingeniería social (picaresca)<br>[E.28.1] Enfermedad |

Fuente. Autor a partir de la metodología

### 7.3.2. Valoración de las amenazas

Los objetivos planteados en esta tarea son:

- Evaluar la probabilidad de ocurrencia de cada amenaza concerniente a cada activo

- Estimar la degradación que causaría la amenaza en cada dimensión del activo si llegara a materializarse.

Para valorar las amenazas de cada activo se han tomado en cuenta la degradación de valor y la probabilidad de ocurrencia.(VER ANEXO D, Valoración de amenazas a cada uno de los activos)

Tabla 4. Degradación del valor y Probabilidad de ocurrencia

| | |
|---|---|
| MA | MUY ALTA |
| A | ALTA |
| M | MEDIA |
| B | BAJA |
| MB | MUY BAJA |
| CS | CASI SEGURO |
| MA | MUY ALTO |
| P | POSIBLE |
| PP | POCO PROBABLE |
| MB | SIGLOS |
| MR | MUY RARA |
| 0 | |

Fuente. Autor a partir de la metodología

### 7.4. CARACTERIZACIÓN DE LAS SALVAGUARDAS

Se definen las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se conjuran organizándose adecuadamente, otras requieren elementos técnicos (programas o equipos), otra seguridad física y por último, está la política de personal.[7]

En esta actividad se identifican las salvaguardas efectivas para la organización junto con la eficacia que tiene cada una de ellas para mitigar el riesgo. Dentro de esta metodología se pueden definir varias etapas de estudio que pueden

[7] Magerit-versión 3 .0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro 1-Método, https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/ç, p 31

abarcar lapsos de tiempo corto o largos incluso de un año, pero nuestro caso de estudio tomaremos tres fases:

- Primera etapa llamada POTENCIAL
- Segunda etapa llamada SITUACIÓN ACTUAL
- Tercera etapa llamada OBJETIVO

Esta actividad consta de dos sub-tareas:

- Identificación de las salvaguardas pertinentes
- Valoración de las salvaguardas

### 7.4.1. Identificación de las salvaguardas

Su objetivo principal es:

- Identificar Las Salvaguardas Convenientes Para Proteger El Sistema.

  En esta tarea contaremos con la ayuda de la herramienta PILAR 5.2.9 que nos ayuda a la elección de salvaguardas de cada activo para contrarrestar las amenazas identificadas.

Figura 6.Identificación de las Salvaguardas

[base_seguridad] baseseguridad

| aspecto | tdp | salvaguarda | dudas | fuente | comen.. | recom.. | on / off | aplica.. |
|---|---|---|---|---|---|---|---|---|
| | | SALVAGUARDAS | | | | | | |
| G | PR | [H] Protecciones Generales | | | | 8 | ... | ... |
| G | PR | [D] Protección de la Información | | | | 7 | off | ... |
| G | EL | [K] Gestión de claves criptográficas | | | | | off | n.a. |
| G | PR | [S] Protección de los Servicios | 1 | | | 6 | ... | ... |
| G | PR | [SW] Protección de las Aplicaciones Informáticas (SW) | | | | 7 | ... | ... |
| G | PR | [HW] Protección de los Equipos Informáticos (HW) | | | | 7 | ... | ... |
| G | PR | [COM] Protección de las Comunicaciones | | | | 9 | ... | ... |
| G | PR | [IP] Puntos de interconexión: conexiones entre zonas de confianza | | | | | off | n.a. |
| G | PR | [MP] Protección de los Soportes de Información | | | | 6 | | |
| G | PR | [AUX] Elementos Auxiliares | | | | 6 | ... | ... |
| F | PR | [L] Protección de las Instalaciones | | | | 7 | | |
| P | PR | [PS] Gestión del Personal | | | | 5 | ... | ... |
| G | AD | [G] Organización | | | | 6 | off | n.a. |
| G | RC | [BC] (or) Continuidad del negocio | | | | 5 | off | n.a. |
| G | AD | [E] Relaciones Externas | | | | 5 | off | n.a. |
| G | AD | [NEW] Adquisición / desarrollo | 1 | | | 4 | off | n.a. |

Fuente: Tomado de la Herramienta PILAR

### 7.4.2. Protecciones Generales:

Las protecciones generales que se pueden destacar y por supuesto aplicar serian:

Se requiere autorización previa: Con esto se da restricción de acceso a la información, que a su vez también pertenece al Control de Acceso Lógico. La razón por la que se escogió esta salvaguarda es porque, cualquier persona puede acceder a los activos inclusive los más importantes en cualquier puesto de trabajo, por ende, se enfrentará a una serie de amenazas a las que están expuestos los activos; y por esto se aplicara a activos como: Datos/ Información, Servicios, Aplicaciones (software), Equipamiento informático (hardware), Redes de comunicaciones y Soportes de información Protege a las siguientes dimensiones de seguridad: Integridad, Confidencialidad y Autenticidad.

- **Protecciones de las Aplicaciones Informáticas:**

Se seleccionan las siguientes salvaguardas ya que la empresa no posee estas normas de seguridad como son:

- Se dispone de normativa sobre el uso autorizado de las aplicaciones
- Se dispone de normativa relativa al cumplimiento de los derechos
- Se controla la instalación de software autorizado y productos con licencia
- Se dispone de procedimientos para realizar copias de seguridad

- **Se aplican perfiles de seguridad:**

Esta salvaguarda se encuentra a medias porque solo existe cuentas de usuario lo que es suficiente para acceder a cualquier parte del sistema, pero gracias a esta salvaguarda podemos hacer frente a amenazas como:

- Errores de los usuarios
- Difusión de software dañino
- Vulnerabilidad de los programas (software)
- Errores de mantenimiento/actualización de programas (software)

- **Protección de los Equipos Informáticos (HW):**

A continuación, las salvaguardas adecuadas para la protección de los equipos.

- Se dispone de normativa sobre el uso correcto de los equipos
- Se dispone de procedimientos de uso de equipamiento

- Se aplican perfiles de seguridad: si se implementa esta salvaguarda en la empresa minimiza amenazas como son: Errores del administrador del sistema / de la seguridad, Uso no previsto y Acceso no autorizado, además de asegurar las dimensiones: integridad y confidencialidad.

Además, se debe de tener en cuenta con estas salvaguardas al momento de utilizar los equipos como son:

- Protección física de los equipos: son mecanismos que la empresa no ha tomado en cuenta para proteger la información principalmente sobre un activo que es el Servidor de Datos
- Para evitar accesos innecesarios
- Para evitar acceso no autorizados
- Seguridad del equipamiento de oficina

Después de evaluar las salvaguardas anteriormente dichas, se deben implantar las siguientes como:

- Autorización previa al uso de activos
- Protección a las aplicaciones informáticas
- Perfiles de seguridad
- Protección de los equipos informáticos

Se debe implantar sobre estas mismas, salvaguardas de nivel superior como:

Se evalúa el impacto en la confidencialidad de los datos

Se evalúa el impacto en la integridad de los datos Ninguna de estas salvaguardas posee la empresa como son:

- Se priorizan las actuaciones encaminadas corregir riesgos elevados
- Se mantiene en todo momento la regla de “seguridad por defecto”
- Se debe de controlar: Reproducción de documentos

### 7.4.3. Protección de las comunicaciones

Se han escogido las siguientes salvaguardas para minimizar riesgos:

- Se deben de aplicar perfiles de seguridad: Para garantizar la comunicación en la empresa y para hacer frente amenazas, como: Errores de [re] – encaminamiento, Errores de secuencia, Alteración de la información, Uso no previsto, [Re-]encaminamiento de mensajes, Alteración de secuencia y Acceso no autorizado, además proteger las dimensiones de seguridad: integridad , confidencialidad y autenticidad.
- La empresa no posee dispone de normativa de uso de los servicios de red.
- Así mismo no dispone de un Control de filtrado

Todas las salvaguardas anteriormente desplegadas hacen frente a la amenaza de

- Acceso no autorizado

Para garantizar las comunicaciones cuando están utilizando el internet es necesario emplear siguientes salvaguardas:

- Herramienta de control de contenidos con filtros actualizados
- Se controla la configuración de los navegadores
- Se registra la descarga
- Se han instalado herramientas antispyware
- Se deshabilitan las “cookies” en los navegadores
- Se registra la navegación web
- Se dispone de normativa sobre el uso de los servicios Internet
- Herramienta de monitorización del trafico
- Se toman medidas frente a la inyección de información espuria
- Se aplica la regla de “seguridad por defecto”
- Se requiere autorización para que medios y dispositivos que tengan acceso a redes y servicios

- **Protección de los Soportes de Información:**

Para proteger el único activo se han escogido las salvaguardas más apropiadas:

- Proteger en uso de contenedores cerrados
- Se dispone de normativa de relativa a la protección criptográfica de los contenidos

- **Protección de las Instalaciones**

  - Se dispone de normativa de seguridad para la seguridad de las instalaciones.
  - Se dispone de áreas específicas para equipos informáticos , para protegerlos de la Ocupación enemiga
  - Además de la Protección del perímetro y reforzar la Vigilancia en las instalaciones de la empresa.
  - Protección frente a explosivos

- **Gestión del Personal:**

Se deben de crear las siguientes normas de seguridad

  - Se dispone de normativa relativa a la gestión de personal (materia de seguridad)
  - Se dispone de procedimientos para la gestión de personal (materia de seguridad)
  - Creación de normas del personal: Propio y Subcontratado
  - Se dispone de normativa de obligado cumplimiento en el desempeño del puesto de trabajo
  - Se establecen normas para la contratación de personal, para garantizar la confidencialidad de los datos, frente ataques de cómo Extorsión y Ataque desde el interior
  - Procedimientos relevantes de seguridad: Emergencias, incidencias.

Después de haber realizado esta tarea tendremos la Declaratoria de Aplicabilidad que es documento formal donde constan las salvaguardas necesarias para proteger al sistema.

### 7.4.4. Valoración De Las Salvaguardas

Objetivo:

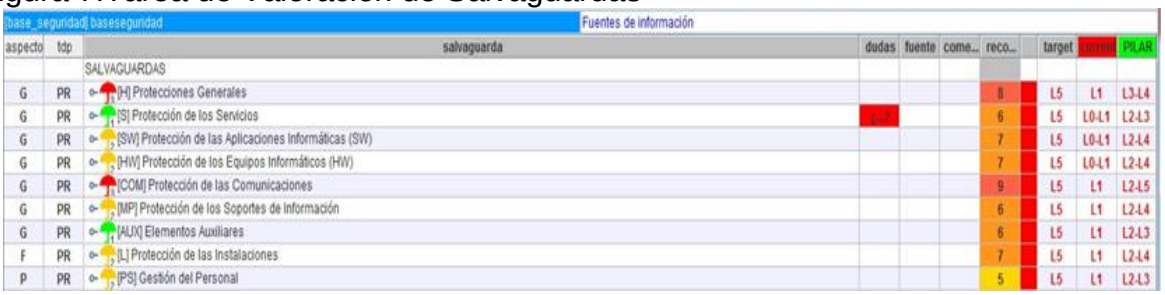
- Determinar la eficacia de las salvaguardas pertinentes

Tabla 5. Niveles de Madurez

| Eficacia | Nivel | Madurez | Estado |
|---|---|---|---|
| 0% | L0 | Inexistente | inexistente |
| 10% | L1 | inicial/ad hoc | iniciado |
| 50% | L2 | reproducible, pero intuitivo | parcialmente realizado |
| 90% | L3 | proceso definido | en funcionamiento |
| 95% | L4 | gestionado y medible | monitorizado |
| 100% | L5 | Optimizado | mejora continua |

Fuente. Autor a partir de la metodología

Figura 7.Tarea de Valoración de Salvaguardas




Fuente: Tomado de la Herramienta PILAR

## 7.5. ESTIMACIÓN DEL ESTADO DE RIESGO

En esta tarea se procesa e interpretan los resultados obtenidos de las actividades anteriores para detallar en un informe del estado de riesgo de la empresa.

Y consta de dos tareas:

- Estimación del impacto
- Estimación del riesgo

El objetivo de esta tarea es:

- Disponer de una estimación fundada de lo que puede ocurrir (impacto) y de lo que probablemente ocurra (riesgo)

### 7.5.1. Estimación de Impacto

Su objetivo es:

- Establecer el impacto potencial al que está sometido el sistema
- Establecer el impacto residual al que está sometido el sistema

En esta tarea se estima al que están expuestos los activos del sistema:

- El impacto potencial, al que está expuesta el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas; pero no las salvaguardas actualmente desplegadas.
- El impacto residual, al que está expuesto el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas, así como la eficacia de las salvaguardas actualmente desplegadas.[8]

La fórmula emplea un sistema de salvaguardas, absolutamente ineficaz (ei=0) deja el impacto donde está, mientras que un sistema de salvaguardas plenamente eficaz (ei=1) reduce el impacto residual a 0

$$\text{Impacto residual} = \text{impacto potencial} \times (1 - e^{i})$$

#### 7.5.1.1. Impacto Potencial

"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 el impacto que estas tendrían sobre el sistema."[9]

Tabla 6. Impacto Potencial sobre cada uno de los activos

| **Activos** | [D] | [I] | [C] | [A] | **[T]** |
|---|---|---|---|---|---|
| **Servicios Internos** | | | | | |
| Internet | [4] | [6] | [6] | | |
| **Equipamiento** | | | | | |
| **Aplicaciones** | | | | | |

[8] Magerit-versión 3 .0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro 1-Método, https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/ç, p. 44
[9] Idem, p 28

| Tabla 6. (Continuación) | | | | | |
|---|---|---|---|---|---|
| Ofimática | | [6] | [6] | | |
| Antivirus | | [6] | [6] | | |
| Sistema Operativo | | [7] | [7] | | |
| Tabla 6. (Continuación) | | | | | |
| Otros Software | | [6 | [6] | | |
| **Equipos** | | | | | |
| Servidor de Base de Datos | | [8] | [8] | | |
| Medios de Impresión | | [6] | [6] | | |
| Computadoras de Escritorio | | [6] | [6] | | |
| Router | | [3] | [3] | | |
| **Comunicaciones** | | | | | |
| Red WIFI | | | [6] | | |
| Red LAN | | [6] | [8] | [6] | |
| Internet | | [6] | | | |
| **Elementos Auxiliares** | | | | | |
| CABLEADO | [6] | | | | |
| Mobiliario | [4] | | | | |
| Sistema de Vigilancia | [4] | | | | |
| Sistema de Alimentación In Interrumpida | [1] | | | | |
| Otros Equipos Auxiliares | [2] | | | | |
| **Soportes de Información** | | | | | |
| CD | | [3] | [3] | | |
| **Instalaciones** | | | | | |
| Edificio | | | [8] | | |
| **Personal** | | | | | |
| Jefa del Departamento Financiero | | | [5] | | |
| Mantenimiento BD | | | [4] | | |
| Mantenimiento EQ | | | [4] | | |

| Tabla 6. (Continuación) | | | | | |
|---|---|---|---|---|---|
| Jefa del Dto. de Contabilidad | | | [7] | | |
| Jefa del Dto. de Ventas | | | [5] | | |
| Jefa del Dto. De Recursos Humanos | | | [5] | | |

Fuente. Autor a partir de la metodología

Los impactos que se muestran con la siguiente escala de colores según su valor:

[10]: Crítico

[9]: Muy alto

[8]: Muy Alto

[7]: Alto

[6]: Alto

[5]: Medio

[4]: Medio

[3]: Bajo

[2]: Bajo

[1]: Despreciable

[0]: Despreciable

#### 7.5.1.2. Impacto Residual Acumulado

El impacto acumulado se calcula con los datos de impacto acumulado sobre un activo y salvaguardas apropiadas para las amenazas sobre dicho activo.

Tabla 7. Impacto Residual sobre cada uno de los activos

| **Activos** | **[D]** | **[I]** | **[C]** | **[A]** | **[T]** |
|---|---|---|---|---|---|
| **Servicios Internos** | | | | | |
| Internet | [4] | [5] | [5] | | |
| **Equipamiento** | | | | | |
| **Aplicaciones** | | | | | |
| Ofimática | | [0] | [0] | | |
| Antivirus | | [3] | [3] | | |

| Tabla 7. (Continuación) | | | | | |
|---|---|---|---|---|---|
| Sistema Operativo | | [4] | [4] | | |
| Otros Software | | [3] | [3] | | |
| **Equipos** | | | | | |
| Servidor de Base de Datos | | [3] | [4] | | |
| Medios de Impresión | | [3] | [3] | | |
| Computadoras de Escritorio | | [3] | [5] | | |
| Router | | [0] | [0] | | |
| **Comunicaciones** | | | | | |
| Red WIFI | | | [2] | | |
| Red LAN | | [3] | [4] | [3] | |
| Internet | | [2] | | | |
| Tabla 7. (Continuación) | | | | | |
| **Elementos Auxiliares** | | | | | |
| CABLEADO | [4] | | | | |
| Mobiliario | [0] | | | | |
| Sistema de Vigilancia | [1] | | | | |
| Sistema de Alimentación Ininterrumpida | [0] | | | | |
| Otros Equipos Auxiliares | [1] | | | | |
| **Soportes de Información** | | | | | |
| CD | | [3] | [3] | | |
| **Instalaciones** | | | | | |
| Edificio | | | [5] | | |
| **Personal** | | | | | |
| Jefa del Departamento Financiero | | | [2] | | |
| Mantenimiento BD | | | [0] | | |
| Mantenimiento EQ | | | [1] | | |
| Jefa del Dto. de Contabilidad | | | [2] | | |
| Jefa del Dto. de Ventas | | | [0] | | |
| Jefa del Dto. De Recursos Humanos | | | [0] | | |

Fuente. Autor a partir de metodología

### 7.5.2. Estimación del Riesgo

Sus objetivos son:

- Determinar el riesgo potencial al que está sometido el sistema
- Determinar el riesgo residual al que está sometido el sistema

En esta tarea se estima el riesgo al o que están sometidos los activos del sistema:

- El riesgo potencial, al que está sometido el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas; pero no las salvaguardas actualmente desplegadas.
- El riego residual , al que está sometido el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas, así como eficacia de las salvaguardas actualmente desplegadas. [10]

Emplea la siguiente formula

Riesgo residual= impacto residual x frecuencia residual

#### 7.5.2.1. Riesgo Potencial

Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener la probabilidad de ocurrencia.

Tabla 8. Riesgo Potencial sobre cada uno de los activos

| **Activos** | **Dimensiones** | | | | |
|---|---|---|---|---|---|
| | [D] | [I] | [C] | [A] | [T] |
| **Servicios Internos** | | | | | |
| Internet | {4,2} | {5,4} | {5,4} | - | - |
| **Equipamiento** | | | | | |
| **Aplicaciones** | | | | | |
| Ofimática | - | {5,4} | {5,4} | - | - |
| Antivirus | - | {5,4} | {5,4} | - | - |
| Sistema Operativo | - | {5,4} | {5,4} | - | - |
| Otros Software | - | {4,5} | {4,5} | - | - |
| **Equipos** | | | | | |
| Servidor de Base de Datos | - | {6,6} | {6,6} | - | - |
| Medios de Impresión | - | {3,6} | {3,6} | - | - |
| Computadoras de Escritorio | - | {4,5} | {4,5} | - | - |
| Router | - | {1,8} | {1,8} | - | - |

[10] Magerit-versión 3 .0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro 1-Método, https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/ç, p. 45

| Tabla 8. (Continuación) | | | | | |
|---|---|---|---|---|---|
| **Comunicaciones** | | | | | |
| Red WIFI | - | - | {4,5} | - | - |
| Red LAN | - | {4,5} | {6,6} | {4,5} | - |
| **Elementos Auxiliares** | | | | | |
| CABLEADO | {4,5} | - | - | - | - |
| Mobiliario | {2,4} | - | - | - | - |
| Sistema de Vigilancia | {3,3} | - | - | - | - |
| Sistema de Alimentación Ininterrumpida | {1,5} | - | - | - | - |
| Otros Equipos Auxiliares | {2,1} | - | - | - | - |
| **Soportes de Información** | | | | | |
| CD | - | {1,8} | {1,8} | - | - |
| **Instalaciones** | | | | | |
| Edificio | - | - | {6,6} | - | - |
| **Personal** | | | | | |
| Jefa del Departamento Financiero | - | - | {4,8} | - | - |
| Mantenimiento BD | - | - | {3,3} | - | - |
| Mantenimiento EQ | - | - | {3,3} | - | - |
| Jefa del Dto. De Contabilidad | - | - | {6,0} | - | - |
| Jefa del Dto. De Ventas | - | - | {3,0} | - | - |
| Jefa del Dto. De Recursos Humanos | - | - | {3,0} | - | - |

Fuente. Autor a partir de metodología

Los riesgos se muestran con la siguiente escala de colores según su valor:

{9} NIVEL 9

{8} NIVEL 8

{7} Extremadamente Crítico

{6} Muy Critico

{5} Crítico

{4} Muy Alto

{3} Alto

{2} Medio

{1} Bajo

{0} Despreciable

#### 7.5.2.2. Riesgo Residual

**Riesgo Residual Acumulado**

La estimación de riesgo residual acumulado nos indica la medida que las amenazas que afectan a los activos de orden superior que dependen de dicho activo. Los valores de la tabla 9 que tienen resultados mayores a 3 son riesgos Altos.

Tabla 9. Riesgo Residual sobre cada uno de los activos

| **Activos** | **Dimensiones** | | | | |
|---|---|---|---|---|---|
| | [D] | [I] | [C] | [A] | [T] |
| **Servicios Internos** | | | | | |
| Internet | {4,} | {4,} | {4,8} | - | - |
| **Equipamiento** | | | | | |
| **Aplicaciones** | | | | | |
| Ofimática | - | {0,83} | {0,83} | - | - |
| Antivirus | - | {3,2} | {3,2} | - | - |
| Sistema Operativo | - | {3,1} | {3,1} | - | - |
| Otros Software | - | {1,7} | {1,7} | - | - |
| **Equipos** | | | | | |
| Servidor de Base de Datos | - | {2,1} | {3,8} | - | - |
| Medios de Impresión | - | {0,95} | {0,96} | - | - |
| Computadoras de Escritorio | - | {1,7} | {3,3} | - | - |
| Router | - | {0,59} | {0,59} | - | - |
| **Comunicaciones** | | | | | |
| Red WIFI | - | - | {1,1} | - | - |

| | | | | | |
|---|---|---|---|---|---|
| Red LAN | - | {2,2} | {2,8} | {2,5} | - |
| Internet | - | {1,2} | - | - | - |
| **Elementos Auxiliares** | | | | | |
| CABLEADO | {3,0} | - | - | - | - |
| Mobiliario | {0,63} | - | - | - | - |
| Tabla 9. (Continuación) | | | | | |
| Sistema de Vigilancia | {0,93} | - | - | - | - |
| Sistema de Alimentación Ininterrumpida | {1,1} | - | - | - | - |
| Otros Equipos Auxiliares | {1,8} | - | - | - | - |
| **Soportes de Información** | | | | | |
| CD | - | {0,86} | {0,90} | - | - |
| **Instalaciones** | | | | | |
| Edificio | - | - | {3,5} | - | - |
| **Personal** | | | | | |
| Jefa del Departamento Financiero | - | - | {1,9} | - | - |
| Mantenimiento BD | - | - | {0,97} | - | - |
| Mantenimiento EQ | - | - | {1,8} | - | - |
| Jefa del Dto. de Contabilidad | - | - | {1,3} | - | - |
| Jefa del Dto. de Ventas | - | - | {0,42} | - | - |
| Jefa del Dto. De Recursos Humanos | - | - | {0,42} | - | - |

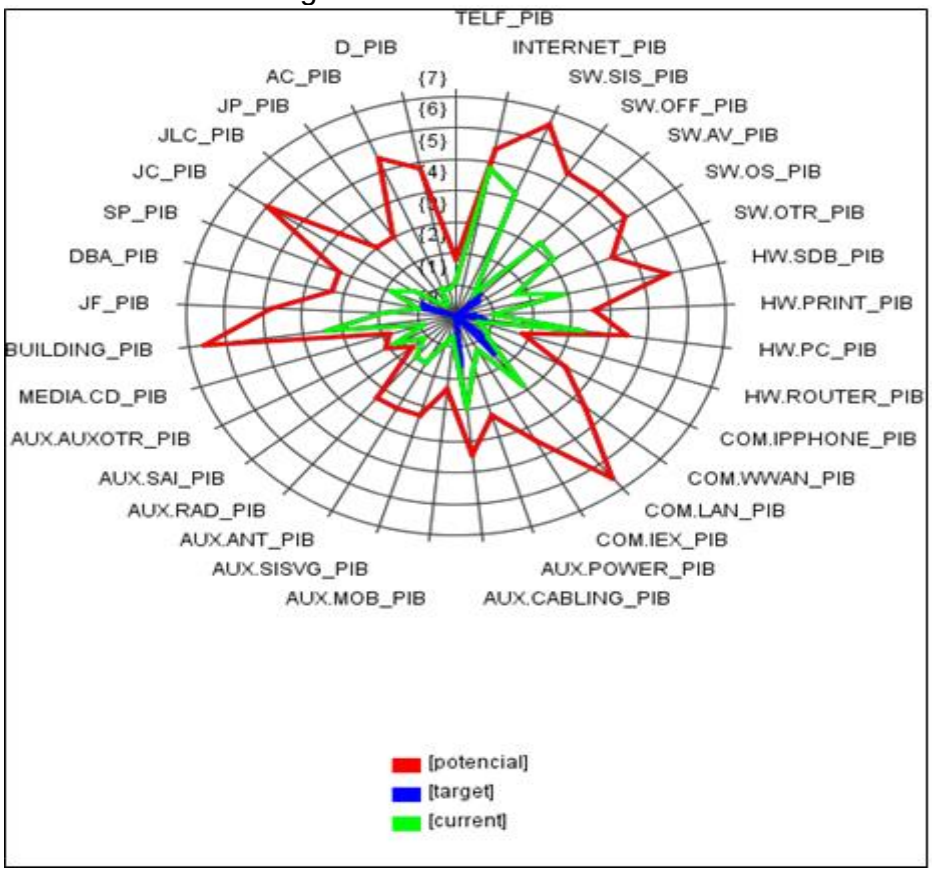
Fuente. Autor a partir de metodología

### 7.6. Interpretación de los Resultados

Como se puede observar en la Figura 8, este es el resultado de todos los pasos del Análisis de Riesgos ya que se hace fácil saber cuáles son los activos que tiene un nivel alto de riesgos, según la figura necesitarían mayor atención serian en Ofimática,

Antivirus, Sistema Operativo, Otros Software, Servidor de Base de Datos, Medios de Impresión, Computadoras de Escritorio, Router, Red WIFI, Red LAN, CABLEADO, Mobiliario, Sistema de Vigilancia, Sistema de Alimentación Ininterrumpida, Otros Equipos Auxiliares, CD, Edificio, Jefa el Departamento Financiero, Mantenimiento BD, Mantenimiento EQ, Jefa del Dto. de Contabilidad, Jefa del Dto. de Ventas, Jefa del Dto. De Recursos Humanos, los cuales para mitigarlos en la siguiente fase que es la Gestión de Riesgos.

Figura 8.Identificación de Riesgos




Fuente: Autor

# 8. PLAN DE SEGURIDAD

En esta fase de la monografía se trata de cómo llevar a cabo planes de seguridad, para materializar las decisiones adoptadas para el tratamiento de los riesgos.

Aquí se identifican 3 tareas

- PS.1 Identificación de seguridad
- PS.2 Plan Ejecución
- PS.3 Ejecución

Típicamente un plan de seguridad se planifica en tres niveles de detalle:

- Plan director (uno) A menudo denominado “plan de actuación”, trabaja sobre un periodo largo (típicamente entre 3 y 5 años), estableciendo las directrices de actuación.
- Plan anual (una serie de planes anuales) Trabaja sobre un periodo corto (típicamente entre 1 y 2 años), estableciendo la planificación de los programas de seguridad.
- Plan de ejecución (un conjunto de proyectos con su planificación) Trabaja en el corto plazo (típicamente menos de 1 año), estableciendo el plan detallado de ejecución de cada programa de seguridad

## 8.1. Identificación de Seguridad

El objetivo de esta tarea es:

Elaborar un conjunto integral de programas de seguridad

“Un programa seguridad es una agrupación de tareas. La agrupación se realiza por conveniencia, porque se trata de tareas que en singular carecerían de eficacia, bien porque se trata de tareas con objetivo en común, bien porque se trata de tareas que competen a una única unidad acción.”[11]

Esta tarea se va a realizar 3 actividades:

- Normativas de Seguridad
- Eliminar fallos de seguridad evidentes
- Clasificación del inventario (Soportes de Información, Elementos auxiliares)[12]

---

[11] *Magerit-versión 3 .0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro 1-Método*, https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/ç, p. 74

[12] PADILLA, Cristina, *Análisis y Gestión de Riesgos Informáticos para la protección de los Sistemas de Información en el Área de Tecnologías Informáticas del Gobierno Provincial de Tungurahua*, Tesis Universidad Técnica de Ambato Facultad de Ingeniería en Sistemas, Electrónica e Industrial, Ambato , julio del 2012 ,p .138

### 8.1.1. Normativas de Seguridad

Documentación del uso autorizado de las aplicaciones

- Se considerará una falta grave el que los empleados instalen cualquier tipo de programa (Software) en sus computadoras, que sea para fines personales o de recreación.
- Para prevenir infecciones por virus informáticos, los empleados deberán evitar hacer uso de cualquier clase de software que no sea evaluado y autorizado por el jefe de sistemas a cargo.
- Los empleados están obligados a verificar que la información y que los medios de almacenamiento, considerando memorias USB, CDs, estén libres de cualquier tipo de software dañino, para ello deben ejecutar el software antivirus.
- Documentación del uso correcto de equipos de equipos informáticos
    - A cada empleado se le asigna un equipo del cual será responsable.
    - Los empleados no deberán mover o reubicar los equipos de cómputo, instalar o desinstalar dispositivos. Solo el personal autorizado podrá realizarlo.
    - Mientras se utilizan los equipos de cómputo, no se podrá consumir alimentos o ingerir líquidos.
    - Evitar colocar objeto encima del equipo o cubrir los orificios de ventilación.
    - Mantener el equipo informático en un entorno limpio y sin humedad.
    - Solo el personal autorizado podrá llevar a cabo los servicios y reparaciones al equipo informático.
    - En caso de que exista un daño por maltrato, por descuido o negligencia por parte del empleado, estará obligado a cubrir el valor de la reparación o reposición del equipo o accesorio afectado.

- Documentación del resguardo y protección de la información
    - El uso de CDs es exclusivo para respaldos de información. El empleado es el responsable de su resguardo.
    - Los empleados deberán respaldar de manera periódica la información sensible y critica que se encuentren en sus computadoras.

- Documentación del uso de servicios de internet
    - Para el uso del correo electrónico los empleados no deben de usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros.
    - Los empleados deben tratar los mensajes de correo electrónico y archivos adjuntos como información que es de propiedad de la empresa.
    - Queda prohibido falsear, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.
    - El acceso a internet es exclusivamente para actividades relacionadas con las necesidades del puesto y función que desempeña.

- Documentación de protección de las instalaciones
    - Establecer normas de conducta cuando estén cerca del servidor, lugares de trabajo, etc. además de cumplir todas las normas de sanidad y seguridad existentes para las instalaciones de la empresa.

- Documentación de la gestión del personal
    - En cada contrato de trabajo se deberá incluir cláusulas de confidencialidad para asegurar información de la empresa.
    - Todo empleado que utilice los bienes y servicios informáticos se comprometen a conducirse bajo los principios de confidencialidad de la información.
    - Que cada empleado deberá cumplir con un horario de trabajo.
    - Establecer normas de conducta de los empleados para crear un ambiente laboral adecuado y respetuoso entre todos.

Con el estudio de salvaguardas en el nivel de riesgo actual (current), a la aplicación de salvaguardas al nivel de riesgo objetivo (target), los riesgos disminuyen considerablemente como se puede observar en la siguiente tabla.

Tabla 10. Resultados de Riesgos Residuales

| **Activos** | **[D]** | **[I]** | **[C]** | **[A]** | **[T]** |
|---|---|---|---|---|---|
| **Servicios Internos** | | | | | |
| Internet | {0} | {0} | {0} | - | - |
| **Equipamiento** | | | | | |
| **Aplicaciones** | | | | | |
| Antivirus | - | {0,90} | {0,90} | - | - |
| Sistema Operativo | - | {0,71} | {0,71} | - | - |
| **Equipos** | | | | | |
| Servidor de Base de Datos | - | {0} | {0} | - | - |
| Computadoras de Escritorio | - | {0,41} | {0,76} | - | - |
| **Comunicaciones** | | | | | |
| Red LAN | - | {0,68} | {1,6} | {0} | - |
| **Elementos auxiliaries** | | | | | |
| CABLEADO | {1,6} | - | - | - | - |
| **Instalaciones** | | | | | |
| Edificio | - | - | {0} | - | - |

Fuente. Autor

### 8.2. Eliminar fallos de seguridad evidentes

El lugar donde se encuentra el servidor de base de datos no cuenta con una instalación adecuada ya que no han seguido ninguna estándar de seguridad, además de que se encuentra ubicado en una oficina donde está el Dto. De Personal lo preocupante es que está a la vista de todos pudiendo cualquier persona manipular el equipo. Además, si ocurriera un incendio no tienen los elementos como extinguidores y no maneja redundancia del equipo.

Las contraseñas que son empleadas para el uso de los computadores no son secretas cada empleado sabe la contraseña de su compañero, existe una amenaza evidente que es la ingeniería social pudiendo afectar el trabajo de su compañero. Lo ideal sería que las contraseñas fueran secretas o que tuvieran que ser cambiadas dentro de un periodo determinado.

En cuanto a la actualización antivirus tienen serios problemas porque algunos equipos no tienen acceso a internet, los mismos se ven afectados y desprotegidos. Asimismo, pasa con los equipos que si tienen acceso a internet ya que el antivirus ya expiro. Lo correcto sería que cada cierto tiempo existe un mantenimiento del Antivirus y no esperar que el equipo deje de funcionar o que peor aún la información se pierda para tomar estas acciones de seguridad.

#### 8.2.1. Clasificación del inventario (Soportes de Información, Elementos auxiliares)

La empresa no contaba con un inventario donde se clasifica para cada uno de sus activos de una manera más detallada como se lo ha realizado en esta monografía, ya que para ellos todos eran equipos informáticos, pero en cuanto aplicación no tiene ningún inventario registrado y lo que son soportes de información solo poseen CDs donde resguardan su información diaria pero no llevan una lista de los CDs donde tengan la fecha, el responsable y el departamento al que pertenece.

### 8.3. Plan de Ejecución

El objetivo principal del plan de ejecución es “Ordenar temporalmente los programas de seguridad.”

Para obtener un plan de seguridad optimo se ha llegado al siguiente orden de los programas de seguridad.

- Eliminar fallos de seguridad evidentes
- Clasificación del inventario (Soportes de Información, Elementos auxiliares)
- Normativas de Seguridad[13]

[13] PADILLA, Cristina, *Análisis y Gestión de Riesgos Informáticos para la protección de los Sistemas de Información en el Área de Tecnologías Informáticas del Gobierno Provincial de Tungurahua*, Tesis

### 8.3.1. Ejecución del plan

Esta actividad recoge la serie de monografía que materializan el plan de seguridad y que se van realizando según dicho plan de acuerdo a lo analizado.[14]

## 8.4. Ejecución

Su principal objetivo es:

Alcanzar los objetivos previstos en el plan de seguridad para cada monografía planificado.

Lo que se pretende alcanzar cuando se ejecuta esta tarea es:

- Implantar salvaguardas
- Modelo de valor actualizado
- Mapa de riesgo actualizado
- Estado de riesgo actualizado

Universidad Técnica de Ambato Facultad de Ingeniería en Sistemas, Electrónica e Industrial, Ambato, julio del 2012 ,p .140

[14] PADILLA, Cristina, *Análisis y Gestión de Riesgos Informáticos para la protección de los Sistemas de Información en el Área de Tecnologías Informáticas del Gobierno Provincial de Tungurahua*, Tesis Universidad Técnica de Ambato Facultad de Ingeniería en Sistemas, Electrónica e Industrial, Ambato , julio del 2012 ,p .140

## 9. POLITICAS DE SEGURIDAD INFORMATICA

Después del desarrollo de la metodología Magerit el cual nos ayudó a identificar los riesgos, y las debilidades con las que cuenta la empresa Tecnoval System se hace necesario estableces ciertas políticas de seguridad, para que sean implementadas e informadas al personal a cargo del funcionamiento de esta misma, las políticas a resaltar y especificar para la empresa Tecnoval System, serian:

- Política de la organización de seguridad
- Política de uso aceptable de los activos y Recursos de Información
- Política de Seguridad Física y del Entorno
- Política de control de acceso a la información

Tabla 11. Políticas de la organización de seguridad

| **Política** | **Políticas de la organización de seguridad** |
|---|---|
| **Objetivo** | Garantizar el cumplimiento normativo de la seguridad de la información y minimizar los riesgos en el desarrollo de las actividades propias de la empresa |
| **Aplicabilidad** | Dirigida a todos los colaboradores de TECNOVAL SYSTEM |
| **Directrices específicas** | |
| • La gerencia de la empresa debe mantener contacto con las autoridades y grupos de interés para estar al corriente en cambios de normativa del gobierno electrónico en Colombia e identificar las tendencias en Seguridad de la Información.<br>• Los jefes de cada área conscientes de los riesgos a la que está expuesta la información a su cargo, deben ejercer frente a sus colaboradores el liderazgo apropiado para disminuirlos.<br>• Anualmente se realizará una Auditoría Interna examinando la seguridad de la información. El Plan de dicha auditoría debe estar enfocado hacia la revisión de todos los requerimientos (políticas y procedimientos) de seguridad. Los resultados deben generar un programa de seguridad, que incluya como mínimo: acciones a realizar, tablas de tiempo y responsables. El programa debe ser aprobado por el Gerencia.<br>• El jefe del área de sistemas debe realizar una evaluación de riesgos para identificar el riesgo de acceso por terceros a la información de Tecnoval System, cada jefe de área debe verificar la implementación de acuerdos, monitorear el cumplimiento de ellos y gestionar los cambios para asegurar que los servicios que se prestan cumplen los requisitos acordados con los terceros | |
| **Responsables** | Gerente, Jefes de Áreas, Jefe de Sistemas |
| **Sanciones** | Iniciar proceso disciplinarios, dar por terminado contrato laboral |

Fuente. Autor

Tabla 12. Políticas de uso aceptable de los activos y Recursos de Información

| **Política** | **Políticas de uso aceptable de los activos y Recursos de Información** |
|---|---|
| **Objetivo** | Definir las pautas generales para asegurar una adecuada protección de los activos y los recursos de información de TECNOVAL SYSTEM |
| **Aplicabilidad** | Dirigida a todos los colaboradores, consultores, contratistas, terceras partes, que usen activos de información que sean propiedad de TECNOVAL SYSTEM |
| **Directrices específicas** | |

- **Uso de los sistemas y equipos de cómputo:** La empresa tiene regla de renuncia, que debe utilizarse al inicio de sesión en los equipos de cómputo: "Advertencia! Este sistema (hardware, software y periféricos), así como la información en él contenida es propiedad de la empresa y su uso está restringido únicamente para propósitos de su negocio, reservándose el derecho de monitorearlo en cualquier momento. El ingreso y utilización de este sistema implica su consentimiento con esta política."

- **Correo electrónico:** Las comunicaciones por correo electrónico entre la empresa y sus públicos de interés deben hacerse a través del correo homologado y proporcionado por la empresa. No es permitido utilizar cuentas personales para comunicarse con los públicos de interés de la empresa, ni para transmitir cualquier otro tipo de información del negocio. A los colaboradores que de acuerdo con sus funciones requieran una cuenta de correo, esta se les asigna en el servidor una vez son vinculados. El jefe de Recursos Humanos y Administrativa es responsable de informar al área de sistemas, las vinculaciones que requieran creación de cuenta de correo; de igual manera debe informar oportunamente los retiros de colaboradores para la suspensión de este servicio. Una vez se produzca la desvinculación de la persona, la cuenta será dada de baja en el servidor mediante una solicitud enviada a la mesa de servicios. La capacidad máxima para almacenamiento de correo electrónico está definida por el área de sistemas y depende del tipo de usuario. No obstante, en caso de necesidades especiales, el interesado podrá solicitar la ampliación de la capacidad. El sistema de monitoreo filtrará los archivos anexos a los mensajes de correo electrónico, para verificar la ausencia de virus. La entrega de todo mensaje a su destinatario final está sujeta a que esta comprobación sea exitosa.
  La empresa tiene regla de comprobación de seguridad, que debe utilizarse siempre en los mensajes. Para evitar reclamaciones legales todos los usuarios de correo de la empresa tienen que hacer pública la renuncia de responsabilidad legal por el envío de la información. El mensaje de aprobación es `El buzón de correo es personal e intransferible y corresponde al colaborador velar por la seguridad protegiendo su clave de acceso`. El usuario es el único responsable por el buen uso de su cuenta de correo electrónico.
  En consecuencia, al aceptar el buzón otorgado por la organización, el usuario se compromete a:

- ✓ Respetar la privacidad de las cuentas de otros usuarios del servicio, tanto dentro como fuera de la red corporativa. El usuario no podrá utilizar identidades ficticias o pertenecientes a otros usuarios para el envío de mensajes.
- ✓ El titular de correo o cuenta asignada por la empresa, usará el correo electrónico para enviar y recibir mensajes necesarios para el desarrollo de las labores propias de su cargo; las únicas áreas autorizadas para el envío de correos masivos son la Gerencia.
- ✓ El uso del correo electrónico propiedad de la empresa deberá ser usado solamente para fines propios a la organización.
- ✓ En su uso el empleado actuará siempre con respeto y cortesía; no podrá crear, distribuir o reenviar mensajes que ofendan la dignidad, intimidad y buen nombre de las personas, de las instituciones, o para realizar algún tipo de acoso, difamación, calumnia, con intención de intimidar, insultar o cualquier otra forma de actividad hostil; de igual forma se prohíbe difundir ideas políticas, religiosas, propagandas entre otros.

- **Navegación en internet:** El uso de Internet debe estar destinado exclusivamente a la ejecución de las actividades de la organización y deben ser utilizados por el colaborador para realizar las funciones establecidas para su cargo, por lo cual la empresa definió los siguientes parámetros para su uso:

- ✓ El colaborador debe abstenerse de descargar programas que realicen conexiones automáticas o visores de sitios clasificados como pornográficos y la utilización de los recursos para distribución o reproducción de este tipo de material, ya sea vía web o medios magnéticos.
- ✓ La descarga de música y videos no es una práctica permitida.
- ✓ Abstenerse de usar sitios que salten la seguridad del servidor de acceso a Internet (proxy).
- ✓ El uso con fines comerciales, políticos, particulares o cualquier otro que no sea el laboral y que dio origen a la habilitación del servicio, no está permitido.
- ✓ Evitar coleccionar, almacenar, difundir, transmitir, solicitar, inducir o incitar en cualquier forma actos ilegales, inmorales, engañosos y/o fraudulentos es una responsabilidad de los colaboradores de la organización; así como también amenazas, abusos, difamaciones, injurias, calumnias, escándalos, actos obscenos, pornográficos, profanos, racistas, discriminatorios, actos que invadan la privacidad de los demás u otro tipo de materias, informaciones, mensajes o comunicaciones de carácter ofensivo.
- ✓ Coleccionar, almacenar, divulgar, transmitir o solicitar información personal (incluyendo sin limitación alguna, información biográfica, habitacional, social, marital, ocupacional, Política Seguridad de la información financiera, y de salud) sobre otros usuarios, sin su consentimiento o conocimiento, son prácticas no permitidas por la empresa
- ✓ Hacer ofertas fraudulentas de compra o venta, así como también, conducir cualquier tipo de fraude financiero, tales como "cartas en cadena" o "las pirámides", son faltas se constituyen como violaciones a esta Política.

- **Uso de herramientas que comprometen la seguridad:** Hacer o intentar hacer, sin permiso del dueño del sistema o del área de sistemas cualquiera de los siguientes actos:

✓ Acceder el sistema o red
✓ Monitorear datos o tráfico.
✓ Sondear, copiar, probar firewalls o herramientas de hacking
✓ Atentar contra la vulnerabilidad del sistema o redes.
✓ Violar las medidas de seguridad o las rutinas de autenticación del sistema o de la red.

- **Recursos compartidos**: El uso de carpetas compartidas en los equipos de cómputo de los usuarios es una práctica que, aunque puede ser una herramienta útil de trabajo, tiene implícitos algunos riesgos que pueden afectar los principios de confidencialidad, integridad y disponibilidad de la información, por lo tanto su uso y aplicación debe ser controlado. Con este propósito la organización define los siguientes lineamientos para su uso seguro:

✓ Se debe evitar el uso de carpetas compartidas en equipos de escritorio.
✓ Los administradores de la red establecen e implementan, en los casos aprobados, la configuración de acceso a la carpeta, previo requerimiento formal de la misma a través de la Mesa de Servicios.
✓ El usuario que autoriza y dispone el recurso compartido es el responsable por las acciones y los accesos sobre la información contenida en dicha carpeta.
✓ Se debe definir el tipo de acceso y los roles estrictamente necesarios sobre la carpeta (lectura, escritura, modificación y borrado).
✓ Debe tenerse claramente especificado el límite de tiempo durante el cual estará publicada la información y compartido el recurso en el equipo.
✓ Si se trata de información confidencial o crítica para la empresa, deben utilizarse las carpetas destinadas para tal fin en el servidor de archivos de usuarios, para que sean incluidos en las copias diarias de respaldo de información o implementar herramientas para el respaldo continuo de información sobre dichos equipos.
✓ El acceso a carpetas compartidas debe delimitarse a los usuarios que las necesitan y deben ser protegidas con contraseñas.
✓ No se debe permitir el acceso a dichas carpetas a usuarios que no cuenten con antivirus corporativo actualizado.

- **Sitios Web para compartir documentos:** El dueño del sitio será el responsable de la seguridad de este y del acceso a la información que se encuentra alojada.

✓ El dueño del sitio será el responsable de otorgar los permisos requeridos.

| | |
|---|---|
| ✓ El dueño del sitio definirá un delegado que tengan control total sobre el sitio, a manera de contingencia, para la asignación de los permisos requeridos en su ausencia.<br><br>• **Computación en nube:** Ninguna información de TECNOVAL SYSTEM podrá utilizar tecnologías de computación en nube si no está previamente autorizado por el área de sistemas.<br><br>• **Uso equipos portátiles y dispositivos móviles:** Los implicados, contratistas y terceros se comprometen a hacer uso adecuado de los dispositivos móviles para el acceso a los servicios corporativos de movilidad proporcionados por la empresa, tales como escritorios y aplicaciones virtuales, correo, comunicaciones unificadas, redes virtuales privadas (VPN), entre otros, atendiendo las siguientes directrices:<br>✓ El dispositivo móvil debe estar en el bolsillo, maletín o lugar no visible en partes públicas.<br>✓ El dispositivo móvil debe estar configurado para bloqueo automático por un tiempo de inactividad a través de medios disponibles de configuración tales como contraseña, patrón huella dactilar, reconocimiento de voz, entre otras.<br>✓ Uso de aplicación de antivirus.<br>✓ Uso de canales seguros y cifrados cuando se conecte a redes compartidas de acceso libre, no seguras.<br>✓ Acceso de equipos distintos a los asignados<br>✓ Desactivar la opción de autoguardado de contraseñas en los diferentes navegadores web.<br>✓ No dejar claves en ningún sistema de almacenamiento de información web.<br>✓ Creación de contraseñas seguras, no incluir información personal como nombres, fechas de nacimiento, otros.<br>✓ Cerrado de sesión de escritorio virtual cuando no esté en uso.<br><br>El área de sistemas debe implementar las medidas necesarias para protección frente al riesgo de la utilización de equipos y comunicación móvil. Se prestará especial cuidado para asegurar que no se compromete la información del negocio, teniendo en cuenta los riesgos que conlleva el trabajar con el equipo móvil en entornos desprotegidos.<br>La utilización de los servicios móviles conectados a las redes debe tener una protección idónea. El acceso remoto a la información del negocio a través de redes públicas usando servicios de computación móvil, sólo debería tener lugar después de la identificación y autenticación exitosa y con el establecimiento de los mecanismos adecuados del control del acceso | |
| **Responsables** | Jefe de Sistemas |
| **Sanciones** | Iniciar proceso disciplinarios, dar por terminado contrato laboral |

Fuente Autor

Tabla 13. Políticas de Seguridad Física y del Entorno

| **Política** | **Políticas de Seguridad Física y del Entorno** |
|---|---|
| **Objetivo** | Determinar las acciones necesarias para el acceso a las instalaciones de forma que se garantice la confidencialidad, disponibilidad e integridad de la información de la empresa |
| **Aplicabilidad** | Dirigida a todos los colaboradores, consultores, contratistas, terceras partes, que ingresen a la sede de TECNOVAL SYSTEM |
| **Directrices específicas** | |
| • Las diferentes áreas de trabajo, deben de estar en áreas protegidas físicamente contra el acceso no autorizado, daño o interferencia y deben cumplir con las políticas de seguridad física.<br><br>• **Controles de acceso físico.** El acceso a las áreas restringidas sólo se debe permitir para:<br>✓ Desarrollo de operaciones tecnológicas<br>✓ Tareas de aseo<br>✓ Pruebas de equipos<br>✓ Almacenamiento de equipos.<br>✓ Implementación o mantenimiento de los controles ambientales.<br><br>• **Escritorio limpio:** La implementación de una directriz de escritorio limpio permitirá reducir el riesgo de acceso no autorizado o daño a medios y documentos. Los computadores deben bloquearse después de diez (10) minutos de inactividad, el usuario tendrá que autenticarse antes de reanudar su actividad. Todos los empleados, consultores, contratistas, terceras partes, deben bloquear la sesión al alejarse de su computador.<br><br>• **Seguridad de los equipos:** Para prevenir la pérdida de información daño o el compromiso de los activos de información y la interrupción de las actividades de TECNOVAL SYSTEM, los equipos deben estar conectados a la toma regulada destinada para tal fin.<br><br>• **Retiro de equipos:** Se deben tener en cuenta los procesos de instalación y retirada del equipo, de tal manera que estos se hagan de forma controlada y segura. La protección de los equipos, incluso cuando se utilizan fuera de la oficina, es necesaria para reducir el riesgo no autorizado de acceso a la información y para protegerlo contra pérdida o robo. | |
| **Responsables** | Jefes de Áreas, Jefe de Sistemas |
| **Sanciones** | Iniciar proceso disciplinarios, dar por terminado contrato laboral |

Fuente. Autor

.

Tabla 14. Políticas de Control de Acceso a la Información

| **Política** | **Políticas de Control de Acceso a la Información** |
|---|---|
| **Objetivo** | Documentar las reglas para asegurar un acceso controlado a la información que es procesada en TECNOVAL SYSTEM |
| **Aplicabilidad** | Dirigida a todos los colaboradores, consultores, contratistas, terceras partes, que ingresen a la sede de TECNOVAL SYSTEM |
| **Directrices específicas** | |

- Las diferentes áreas, conforme la clasificación de activos de información, deben implementar las medidas de seguridad aplicables según el caso, con el fin de evitar la adulteración, pérdida, fuga, consulta, uso o acceso no autorizado o fraudulento. El control de acceso de datos e información sensible se debe basar en el principio del menor privilegio, lo que implica que no se otorgará acceso a menos que sea explícitamente permitido.

- **Gestión de acceso a usuarios:** Las diferentes áreas establecerán procedimientos formales para controlar la definición de perfiles y la asignación de derechos de acceso a los usuarios, previamente definidos por el responsable del proceso. Dichos procedimientos deben cubrir todas las etapas del ciclo de vida del usuario, desde su registro inicial hasta la eliminación o desactivación del registro a quienes no necesiten el acceso. Se debe brindar atención y seguimiento especial, donde sea apropiado, a la necesidad del control de asignaciones de accesos privilegiados.

- **Registro de usuarios:** Todos los usuarios deben tener una identificación única personal o jurídica, que se utilizará para el seguimiento de las actividades de responsabilidad individual o jurídica. Las actividades habituales de usuario no deben ser desempeñadas a través de cuentas privilegiadas. En circunstancias excepcionales, por beneficio de la compañía, se podrá usar **u**n identificador compartido, para un grupo de usuarios con trabajo específico; este debe ser autorizado y debidamente aprobado por la respectiva área
  El usuario debe tener autorización del jefe de sistemas para el uso del sistema o servicio de información. Se debe verificar que el nivel de acceso otorgado sea adecuado para los propósitos de la empresa y conserven una adecuada segregación de funciones. Adicionalmente, deben tomar y certificar la formación y así garantizar el uso adecuado del sistema o servicio de información.

- **Responsabilidades del usuario:** Una seguridad efectiva requiere la cooperación de los usuarios autorizados, quienes deben saber sus responsabilidades para el mantenimiento de controles efectivos al acceso, en particular, aquellos con referencia al uso de contraseñas, el área de sistemas implementará los procedimientos necesarios que permitan controlar la creación, modificación, desactivación y eliminación de usuarios, administración de contraseñas y permisos de acceso a los recursos tecnológicos y a la información. Adicionalmente, es necesario

implementar un procedimiento de revisión periódica de los permisos de acceso de los usuarios.

Los empleados, contratistas y terceros entienden las condiciones de acceso y deben mantener confidenciales las contraseñas personales y conservar las contraseñas de grupo únicamente entre los miembros de este**.** Esta declaración puede ser incluida en los términos y condiciones laborales. Igualmente deben cumplir las buenas prácticas en la selección y uso de la contraseña.

- **Control de acceso a la red:** Únicamente se debe proporcionar a los colaboradores el acceso a los servicios para los que específicamente se les haya autorizado su uso. Se deben utilizar métodos apropiados de autenticación para el control de acceso a los usuarios remotos. Se deben implantar controles adicionales para el acceso por redes inalámbricas. Se debe establecer una adecuada segregación de redes, separando los entornos de red de usuarios y los servicios**.**

- **Control de acceso a las aplicaciones:** El uso de programas que puedan ser capaces de invalidar los controles del sistema y de la aplicación, deben estar restringidos y estrictamente controlados.
  Las sesiones inactivas deben cerrarse después de un período de inactividad definido y se deben usar restricciones en los tiempos de conexión para proporcionar una seguridad adicional a las aplicaciones de alto riesgo.
  Las cuentas de usuario de herramientas o productos que vengan por omisión se deben deshabilitar inmediatamente después de la instalación de **l**os sistemas o software.
  Las contraseñas predeterminadas por el proveedor se deben cambiar inmediatamente después de la instalación de los sistemas o software.
  El área de sistemas debe integrar las aplicaciones con el Directorio Activo.

| | |
|---|---|
| **Responsables** | Jefe de Sistemas |
| **Sanciones** | Iniciar proceso disciplinarios, dar por terminado contrato laboral |

Fuente. Autor

# 10. CONCLUSIONES

La empresa “TECNOVAL SYSTEM.” no contaba con las medidas de seguridad guiados y documentados, por lo cual este estudio fue de gran beneficio para minimizar riesgos en el futuro.

Gracias a la metodología implementada llamada MAGERIT, la cual cuenta con una serie de pasos estructurados para el análisis y gestión de riesgos, parte fundamental a la hora de tener un diagnóstico claro de los riegos y falencias en que la empresa podría estar expuesta, con base a esto se supo escoger cuales son las medidas necesarias para mitigar los riesgos.

La empresa “TECNOVAL SYSTEM.”, como todas las empresas que manejan información de prioridades, requiere el desarrollo de unas políticas de seguridad que le dé mayor protección a dicha información, las políticas de seguridad planteadas en esta monografía llevaran a esta empresa a tener una organización clara en la información manejada, un personal mejor capacitado para el uso de la información, un equipamiento más óptimo según cada área de la empresa, y el control estricto de cada área y su respectiva información.

# 11. RECOMENDACIONES

Se recomienda que haya una revisión periódica de las amenazas y riesgos ya que la tecnología está cambiando constantemente y deben ser controlados para evitar futuros problemas.

Se sugiere al gerente de la empresa que contrate al personal adecuado para implementar las salvaguardas que fueron escogidas en el análisis de riesgos para la empresa “TECNOVAL SYSTEM.”

El jefe del área de sistemas debe realizar una evaluación de riesgos para identificar el riesgo de acceso por terceros a la información de Tecnoval System, cada jefe de área debe verificar la implementación de acuerdos, monitorear el cumplimiento de ellos y gestionar los cambios para asegurar que los servicios que se prestan cumplen los requisitos acordados con los terceros.

El área de sistemas debe implementar las medidas necesarias para protección frente al riesgo de la utilización de equipos y comunicación móvil. Se prestará especial cuidado para asegurar que no se compromete la información del negocio, teniendo en cuenta los riesgos que conlleva el trabajar con el equipo móvil en entornos desprotegidos.

La utilización de los servicios móviles conectados a las redes debe tener una protección idónea. El acceso remoto a la información del negocio a través de redes públicas usando servicios de computación móvil, sólo debería tener lugar después de la identificación y autenticación exitosa y con el establecimiento de los mecanismos adecuados del control del acceso.

## GLOSARIO

**ATAQUES INFORMÁTICOS**
método por el cual un individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático (ordenador, red privada, etcétera) ..... 6

**DOCUMENTACIÓN**
ciencia que consiste en documentar, ésta se encuentra identificada por el procesamiento de información que otorgará datos específicos sobre un tema determinado..... 48, 49

**EJECUCIÓN**
proceso mediante el cual una computadora lleva a cabo las instrucciones de un programa informático..... 9, 47, 50, 51

**EQUIPOS**
son los dispositivos de hardware que se encuentran en la computadora con la finalidad de aumentar las posibilidades de acceso, almacenamiento y salida . 23, 25, 26, 35, 40, 41, 42, 43, 44, 45, 46, 49, 84

**FALLAS**
es un estado o situación en la que se encuentra un sistema formado por dispositivos, equipos, aparatos y/o personas en el momento que deja de cumplir la función para el cual había sido diseñado..... 4, 19, 63

**GESTIÓN DE RIESGOS**
es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza, a través de una secuencia de actividades humanas que incluyen la identificación, el análisis y la evaluación de riesgo... 3, 12, 16, 18, 20, 22, 27, 33, 40, 43, 46, 47, 50, 51, 56

**IDENTIFICACIÓN**
es la acción y efecto de identificar o identificarse (reconocer si una persona o una cosa es la misma que se busca..... 7, 8, 1, 2, 12, 22, 27, 34, 46, 47

**IMPACTO**
Resultado sobre un activo ante la materialización de una amenaza.. 8, 1, 2, 39, 40, 42

**INCIDENTE**
Cualquier evento no esperado o no deseado que pueda comprometer la seguridad del sistema ..... 11

**INFORMACIÓN**

es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje. ..... 1, 2, 89, 90, 94, 97

**INVENTARIO**

registro documental de los bienes y demás objetos pertenecientes a una persona física o una empresa ..... 9, 47, 50

**MONOGRAFÍA**

trabajo escrito, metódico y completo que trata sobre la descripción especial de una determinada ciencia o asunto en particular 8, 3, 6, 12, 16, 18, 19, 20, 21, 47, 50, 51, 52, 84

**NORMATIVA DE SEGURIDAD**

Conjunto de documentos que desarrollan la política de seguridad. ..... 37

**NORMATIVAS**

designa a la agrupación de normas o reglas que son plausibles de ser aplicadas a instancias de una determinada actividad o asunto ..... 8, 47, 48, 50

**PROTECCIÓN**

es un cuidado preventivo ante un eventual riesgo o problema. . 4, 9, 35, 37, 47, 48, 49, 50, 51, 56

**ROUTER**

dispositivo de hardware que permite la interconexión de ordenadores en red .... 23, 26, 41, 42, 43, 45, 46

**SALVAGUARDAS**

procedimiento que reduce un riesgo .....8, 12, 19, 20, 21, 22, 33, 34, 35, 36, 37, 38, 40, 42, 43, 49, 51, 53

**SEGURIDAD**

Capacidad de resistir, con un determinado nivel de confianza, los incidentes que puedan causar daño..9, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 16, 18, 19, 20, 21, 29, 33, 35, 36, 37, 38, 47, 49, 50, 51, 52, 53, 56, 57, 64, 65, 66, 79, 84, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99

**USUARIOS**

quien usa ordinariamente algo ....3, 6, 19, 22, 25, 27, 28, 35, 78, 84, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99

**VALOR**

Estimación de la unidad de una determinada activo de información para la organización teniendo en cuenta los diferentes requerimientos. 2, 22, 32, 33, 40, 41, 43, 44, 48, 51, 67, 68, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99

## BIBLIOGRAFIA


CASTRO, R. (15 de ABRIL de 2015). *Avanzando en la seguridad de las redes wifi. En Boletin RedIRIS N° 73. 2005.* Obtenido de http://www.rediris.es/difusion/publicaciones/boletin/73/ENFOQUE1.pdf

Directrices. (20 de MAYO de 2015). *Seguridad de la información.* Obtenido de http://mgd.redrta.org/directrices-seguridad-de-la-informacion/mgd/2015-01-22/145337.html

*El portal de ISO 27002 en Español*. (13 de ENERO de 2015). Obtenido de http://www.iso27000.es/iso27002.html

Gerencie.com. (5 de noviembre de 2017). *Auditoria de sistemas de información*. Obtenido de https://www.gerencie.com/auditoria-de-sistemas-de-informacion.html

KATZ, M. (2013). *Redes y seguridad.* España: Alfaomega.

LAMILLA, E. P. (12 de JUNIO de 2015). *Desarrollo de políticas de seguridad informática e implantación de cuatro dominios en base a la norma 27002 para el área de hardware en la empresa Uniplex Systems S.A. en Guayaquil. Obtenido de Escuela Superior Politécnica del Litoral.* Obtenido de http://www.dspace.espol.edu.ec/handle/123456789/77094

MENDEZ, J. (15 de ABRIL de 2015). *Estudio de metodologías para la implantación de la seguridad en redes inalámbricas de área local.* Obtenido de http://hdl.handle.net/10596/2764

MENDEZ, J. (4 de ENERO de 2015). *Estudio de Metodologías para la implantación de la seguridad en Redes Inalámbricas de Área Local.* Obtenido de http://repositorios.unimet.edu.ve/docs/88/P.GTT2006M45A5.pdf

MENDEZ, J. (14 de ABRIL de 2015). *Estudio de metodologías para la implantación de la seguridad en redes inalámbricas de área local. .* Obtenido de < http://hdl.handle.net/10596/2764>

Molina Rincón, E. L. (1 de febrero de 2015). *GUÍA PARA LA SEGURIDAD BASADA EN LA NORMA ISO/IEC 27002, PARA LA DEPENDENCIA DIVISIÓN DE SISTEMAS DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA.* Obtenido de http://repositorio.ufpso.edu.co:8080/dspaceufpso/bitstream/123456789/439/1/25830.pd

PADILLA, C. (JULIO de 2012). Análisis y Gestión de Riesgos Informáticos para la protección de los Sistemas de Información en el Área de Tecnologías Informáticas del Gobierno Provincial de Tungurahua. Ambato : Tesis

Universidad Técnica de Ambato Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

PERAFAN, J. C. (16 de MAYO de 2015). *Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca.* Obtenido de http://hdl.handle.net/10596/2655

RAMIREZ, J. (13 de febrero de 2015). *Análisis, evaluación de riesgos y asesoramiento de la seguridad informática en el área de redes y sistemas de la alcaldía de pamplona.* Obtenido de http://repository.unad.edu.co/bitstream/10596/3415/1/88030934.pdf

Recuperado. (20 de MARZO de 2013). Obtenido de Aceptación del Riesgo: http://www.sunai.gob.ve/index.php/glosario-de-terminos#

RECUPERADO. (20 de MARZO de 2013). Obtenido de Conceptos Informáticos: http://www.seguridadpc.net/conceptos.htm

SIMAL, T. (10 de diciembre de 2014). *Monografico Redes WIFI. [Articulo Online]* . Obtenido de http://recursostic.educacion.es/observatorio/web/en/cajon-de-sastre/38-cajon-de-sastre/961-monografico-redes-wifi

USCATEGUI, J. (17 de abril de 2015). *Diagnóstico del estado y nivel de seguridad de la información vigente en la empresa Disemeq LTDA del departamento de Casanare – DISEINFORDI.* Obtenido de http://repositorios.unimet.edu.ve/docs/88/P.GTT2006M45A5.pdf

## ANEXOS

### A. Encuestas realizadas a los empleados

La encuesta fue realizada para el siguiente personal: Jefa del Departamento Financiero, Jefa del Departamento de Contabilidad, Jefa del Departamento de Ventas, Jefa del Departamento de Recursos Humanos, Auxiliar de Contabilidad y Digitadora

1. ¿Su computadora recibe mantenimiento periódicamente?

   Sí _ No_

**Interpretación**

| Nº | Ítem | Frecuencia | % |
|---|---|---|---|
| 1 | Si | 0 | 0,00 |
| 2 | No | 6 | 100 |
| | **Total** | 6 | 100% |

De 6 empleados encuestados todos mencionaron que sus equipos no reciben mantenimiento en determinado tiempo sino que el equipo debe presentar problemas serios para ser llevado donde el (Ingeniero de sistemas).

2. ¿Si en caso de daño de su computadora que tiempo se demoran en arreglos?

   Una hora__ Dos Horas__

   Un Dia__ Otros_____

**Interpretación**

| Nº | Ítem | Frecuencia | % |
|---|---|---|---|
| 1 | Una hora | 0 | 0,00 |
| 2 | Dos horas | 0 | 0,00 |
| 3 | Un dia | 6 | 100,00 |
| 4 | Otros | 0 | 0,00 |
| | **Total** | 6 | 100% |

Los empleados dijeron que cuando su computador no funciona tienen que llamar al Ing. Carolo García para que les arregle su equipo y demora un día para traerlo reparado provocando que las actividades laborales se detengan

3. ¿Usted apaga su computador cuando va almorzar?

Si___ No____

**Interpretación**

| **Nº** | **Ítem** | **Frecuencia** | **%** |
|---|---|---|---|
| 1 | Si | 2 | 33,2 |
| 2 | No | 4 | 66,8 |
| | **Total** | 6 | 100% |

Como el tiempo es muy corto que tienen para ir almorzar la mayoría de los empleados no apagan su computador.

4. Usted guarda la información o la actividad que está realizando cuando se va almorzar

SI____ NO____

**Interpretación**

| **Nº** | **Ítem** | **Frecuencia** | **%** |
|---|---|---|---|
| 1 | Si | 6 | 100,00 |
| 2 | No | 0 | 0,00 |
| | **Total** | 6 | 100% |

Todos los empleados guardan la información antes de ir almorzar para después seguir con sus actividades en su jornada de labor normal.

5. ¿Posee algún periodo de tiempo para el cambio de equipos de computación?

SI____ NO_____

**Interpretación**

| Nº | Ítem | Frecuencia | % |
|---|---|---|---|
| 1 | Si | 0 | 0,00 |
| 2 | No | 6 | 100,00 |
| | **Total** | 6 | 100% |

No tiene ningún periodo de tiempo para el cambio de equipos para eso debe de estar en pésimas condiciones donde ya deje de funcionar para hacer la compra de un equipo nuevo.

6. Posee contraseña su equipo de computación

Si_____ NO_____

**Interpretación**

| Nº | Ítem | Frecuencia | % |
|---|---|---|---|
| 1 | Si | 6 | 100,00 |
| 2 | No | 0 | 0,00 |
| | **Total** | 6 | 100% |

Todos los equipos de computación tienen contraseñas, pero no son secretas por que se comparten de un empleado a otro.

7. Con que frecuencia cambia su contraseña

Nunca___ Cada mes_____

Tres meses____ Seis Meses_____

Una vez al año____

**Interpretación**

| Nº | Ítem | Frecuencia | % |
|---|---|---|---|
| 1 | Nunca | 6 | 100,00 |
| 2 | Cada mes | 0 | 0,00 |
| 3 | Tres meses | 0 | 0,00 |
| 4 | Seis meses | 0 | 0,00 |
| 5 | Una vez al año | 0 | 0,00 |
| | **Total** | 6 | 100% |

Los empleados no tienen por costumbre cambiar las contraseñas de sus equipos por órdenes del Gerente de la empresa.

8. Usted tiene acceso a Internet

Si____ NO___

**Interpretación**

| Nº | Ítem | Frecuencia | % |
|---|---|---|---|
| 1 | Si | 4 | 66,8 |
| 2 | No | 2 | 33,2 |
| | **Total** | 6 | 100% |

El internet es utilizado por las empleadas de Financiero, Personal, Contabilidad, Logística y Compras, para realizar labores de acuerdo a su cargo. Las empleadas que no tienen acceso a internet son Auxiliar de Contabilidad y Digitadora.

9. ¿Tiene alguna restricción para ingresar páginas de internet?

SI_____ NO____

**Interpretación**

| Nº | Ítem | Frecuencia | % |
|---|---|---|---|
| 1 | Si | 0 | 0,00 |
| 2 | No | 6 | 100,00 |
| | **Total** | 6 | 100% |

Los empleados tienen acceso a cualquier página de internet. Además, mencionaron que todo comunicado llega por su cuenta de correo electrónico personal.

10. ¿Posee antivirus su computador?

SI_____ NO_____

**Interpretación**

| Nº | Ítem | Frecuencia | % |
|---|---|---|---|
| 1 | Si | 6 | 100,00 |
| 2 | No | 0 | 0,00 |
| | **Total** | 6 | 100% |
| | | | |

Todos los equipos poseen antivirus, pero en la mayoría mencionaron que ya están caducados.

11. ¿Ha presentado fallas en el sistema?

SI____ NO____

**Interpretación**

| Nº | Ítem | Frecuencia | % |
|---|---|---|---|
| 1 | Si | 2 | 40,00 |
| 2 | No | 3 | 60,00 |
| | **Total** | 5 | 100% |

Esta pregunta se realizó a las cinco personas que utilizan el sistema que mencionaron que cuando presenta fallas como es cuando no ingresa un empleado nuevo, deben de llamar a Cesar Augusto Arzuaga para que revise porque da ese problema.

12. ¿La empresa se ha visto afectada por amenazas como son?

Fuego__
Daños por agua__
Tormentas__
Terremotos__
Tsunamis___
Calor extremo___

**Interpretación**

| Nº | Ítem | Frecuencia | % |
|---|---|---|---|
| 1 | Fuego | 0 | 0,00 |
| 2 | Daños por agua | 2 | 33,2 |
| 3 | Tormentas | 4 | 66,8 |
| 4 | Terremotos | 0 | 0,00 |
| | **Total** | 6 | 100% |

Los empleados se han percato de estas amenazas se materialicen en una época del año como son los meses de invierno donde se producen tormentas en donde las instalaciones se han visto afectadas por el agua que a veces ha ingresado a las oficina

13. Se realizan copias de los datos?

SI__ NO__

**Interpretación**

| Nº | Ítem | Frecuencia | % |
|---|---|---|---|
| 1 | Si | 6 | 100,00 |
| 2 | No | 0 | 0,00 |
| | **Total** | 6 | 100% |

Si se realizan copias en CDs después de cada jornada de laboral.

14. ¿Existen procedimientos de copias de seguridad?

SI___ NO___

**Interpretación**

| Nº | Ítem | Frecuencia | % |
|---|---|---|---|
| 1 | Si | 0 | 0,00 |
| 2 | No | 6 | 100,00 |
| | **Total** | 6 | 100% |

No existe ningún procedimiento de copias de seguridad solo las que se realizan en CDs en donde este medio no posee ninguna etiqueta donde especifique la fecha o el departamento a quien le pertenece.

15. ¿Existen controles que detecten posibles fallos de seguridad en los sistemas de información?

SI__ NO__

**Interpretación**

| Nº | Ítem | Frecuencia | % |
|---|---|---|---|
| 1 | Si | 0 | 0,00 |
| 2 | No | 6 | 100,00 |
| | **Total** | 6 | 100% |

Todos mencionaron que no existe ningún medio que detecte posibles fallos en los sistemas de información.

16. ¿Existe o se tiene pensado realizar un plan de seguridad?

SI___ NO____

**Interpretación**

| Nº | Ítem | Frecuencia | % |
|---|---|---|---|
| 1 | Si | 0 | 0,00 |
| 2 | No | 6 | 100,00 |
| | **Total** | 6 | 100% |

En la actualidad la empresa no posee ningún Plan de Seguridad.

17. ¿Existe un documento llamado Declaratoria de Aplicabilidad?

SI___ NO___

**Interpretación**

| **Nº** | **Ítem** | **Frecuencia** | **%** |
|---|---|---|---|
| 1 | Si | 0 | 0,00 |
| 2 | No | 6 | 100,00 |
| | **Total** | 6 | 100% |

En la actualidad la empresa no posee ningún documento en donde este la Declaratoria de Aplicabilidad.

18. ¿Existe un presupuesto asignado para la seguridad en la empresa?

SI__ NO__

Esta pregunta fue realizada para el empleado Ing. Luis Enrique Morales encargada del Dto. Financiero y su respuesta fue que NO

## B. Fichas de Recolección de Información

### 1. [info] Activos esenciales: información

| *[info]información* | |
|---|---|
| **Código** | **Nombre** |
| **Descripción** | |
| **Propietario** | |
| **Responsable** | |
| **Tipo** | |

| **Valoración** | | |
|---|---|---|
| **Dimensión** | **valor** | **justificación** |
| **[I]** | | |
| **[C]** | | |
| **[A]** | | |
| **[T]** | | |

| **Dependencias de activos inferiores (hijos)** | |
|---|---|
| **activo:** | **grado:** |
| **¿por qué?** | |

| **activo:** | **grado:** |
|---|---|

| |
|---|
| **¿por qué?** |

| | |
|---|---|
| **activo:** | **grado:** |
| **¿por qué?** | |

## 2. [service] Activos esenciales: Servicio

| | |
|---|---|
| ***[servicio]Servicio*** | |
| **Código** | **Nombre** |
| **Descripción** | |
| **Responsable** | |
| **Tipo** | |

| **Valoración** | | |
|---|---|---|
| **Dimension** | **valor** | **justificación** |
| **[I]** | | |
| **[A]** | | |
| **[T]** | | |

| Dependencias de activos inferiores (hijos) | |
|---|---|
| **activo:** | **grado :** |
| **¿por qué ?** | |

| **activo:** | **grado :** |
|---|---|
| **¿por qué ?** | |

| **activo:** | **grado :** |
|---|---|
| **¿por qué ?** | |

### 3. [S] Servicios

| *[S]servicios* | |
|---|---|
| **Código** | **Nombre** |
| **Descripción** | |
| **Responsible** | |
| **Tipo** | |

| Dependencias de activos inferiores (hijos) | |
|---|---|
| **activo:** | **grado :** |

| |
|---|
| **¿por qué ?** |

| | |
|---|---|
| **Activo** | **grado:** |
| **¿por qué ?** | |

## 4. [SW] Aplicaciones (software)

| | |
|---|---|
| ***[SW]Aplicaciones (software)*** | |
| **Código** | **Nombre** |
| **Descripción** | |
| **Responsable** | |
| **Tipo** | |

| | |
|---|---|
| **Dependencias de activos inferiores (hijos)** | |
| **activo:** | **grado:** |
| **¿por qué?** | |

| | |
|---|---|
| **activo:** | **grado:** |
| **¿por qué?** | |

| | |
|---|---|
| **activo:** | **grado:** |
| **¿por qué?** | |

## 5. [HW] Equipamiento informático (hardware)

| | |
|---|---|
| ***[HW]Equipamiento informático*** | |
| **Código** | **Nombre** |
| **Descripción** | |
| **Responsable** | |
| **Ubicación** | |
| **Número** | |
| **Tipo** | |

| | |
|---|---|
| **Dependencias de activos inferiores (hijos)** | |
| **activo:** | **grado:** |
| **¿por qué?** | |

| | |
|---|---|
| **activo:** | **grado:** |
| **¿por qué?** | |

## 6. [COM] Redes de comunicaciones

| *[COM]Redes de comunicaciones* | |
|---|---|
| **Código** | **Nombre** |
| **Descripción** | |
| **Responsible** | |
| **Ubicación** | |
| **Número** | |
| **Tipo** | |
| **Dependencias de activos inferiores (hijos)** | |
| **activo:** | **grado :** |
| **¿por qué ?** | |

| | |
|---|---|
| **activo:** | **grado :** |
| **¿por qué ?** | |

## 7. [Media] Soportes de información

| *[SI]Soportes de información* | |
|---|---|
| **Código** | **Nombre** |
| **Descripción** | |
| **Responsable** | |
| **Ubicación** | |
| **Número** | |
| **Tipo** | |

| **Dependencias de activos inferiores (hijos)** |
|---|
| **activo:** **grado:** |
| **¿por qué?** |

| **activo:** **grado:** |
|---|
| **¿por qué?** |

## 8. [AUX] Equipamiento auxiliar

| *[AUX]Equipamiento auxiliar* | |
|---|---|
| **Código** | **Nombre** |
| **Descripción** | |
| **Responsable** | |
| **Ubicación** | |
| **Número** | |
| **Tipo** | |

| **Dependencias de activos inferiores (hijos)** |
|---|
| **activo:** **grado:** |
| **¿por qué?** |

| |
|---|
| **activo:** **grado:** |
| **¿por qué?** |

## 9. [L] Instalaciones

| *[L]Instalaciones* | |
|---|---|
| **Código** | **Nombre** |
| **Descripción** | |
| **Responsable** | |
| **Ubicación** | |
| **Número** | |
| **Tipo** | |

| **Dependencias de activos inferiores (hijos)** |
|---|
| **activo:** **grado:** |
| **¿por qué?** |

| **activo:** **grado:** |
|---|
| **¿por qué?** |

## 10. [P] Personal

| *[P]Personal* | |
|---|---|
| **Código** | **nombre** |
| **Descripción** | |
| **Número** | |
| **Tipo** | |

## C. OFICIO DEL GERENTE


Valledupar 26, de Septiembre de 2018

**Señores**
**Universidad Abierta y a Distancia UNAD**
**Ciudad**

Por este medio hago de su conocimiento que esta institución apoya el desarrollo de la investigación en "**ESTUDIO DEL ESTADO DE SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA TECNOVAL SYSTEM PARA DESARROLLAR POLÍTICAS DE SEGURIDAD**, que será realizado por la estudiante de la Universidad Abierta y a Distancia UNAD, Sandra Borrego con documento número 49719026 y constituye el trabajo de tesis de Especialista en Seguridad Informática.

Atentamente,

**LUIS ENRRIQUE MORALES NIEVES**
**77.158.240 de Agustín Codazzi**
**Gerente**
**DIRECCION:** Mz A casa 9 Mirador de la Sierra 1
**TELEFONO:** 3008100028
**Correo:** luismora1207@hotmail.com
**Ciudad:** Valledupar

## D. VALORACIÓN DE AMENAZAS A CADA UNO DE LOS ACTIVOS

| Activos | Amenazas | P | [D] | [I] | [C] | [A] | [T] |
|---|---|---|---|---|---|---|---|
| INTERNET | [A.7] Uso no previsto | MA | M | M | M | - | - |
| OFIMÁTICA | [E.1] Errores de los usuarios | P | M | M | M | - | - |
| | [E.20] Vulnerabilidades de los programas (software) | P | M | M | M | - | - |
| | [E.21] Errores de mantenimiento / actualización de programas (software) | P | M | B | - | - | - |
| | [A.8] Difusión de software dañino | PP | B | B | B | - | - |
| ANTIVIRUS OPERATIVO | [E.8] Difusión de software dañino | PP | B | B | B | - | - |
| | [E.20] Vulnerabilidades de los programas (software) | P | M | M | M | - | - |
| | [E.21] Errores de mantenimiento / actualización de programas (software) | P | M | M | - | - | - |
| | [I.5] Avería de origen físico o lógico | P | M | - | - | - | - |
| ANTIVIRUS | [E.1] Errores de los usuarios | PP | M | M | M | - | - |
| | [E.8] Difusión de software dañino | PP | B | B | B | - | - |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | [E.20] Vulnerabilidades de los programas (software) | P | B | M | M | - | - |
| OPERATIVO OTROS SOFTWARE SERVIDOR DE | [E.21] Errores de mantenimiento / actualización de programas (software) | P | M | B | - | - | - |
| | [A.7] Uso no previsto | P | B | B | B | - | - |
| | [E.8] Difusión de software dañino | PP | B | B | B | - | - |
| | [E.20] Vulnerabilidades de los programas (software) | PP | B | B | B | - | - |
| | [E.21] Errores de mantenimiento / actualización de programas (software) | PP | M | M | - | - | - |
| | [N.1] Fuego | P | A | - | - | - | - |
| BASE DE DATOS | [N.2] Daños por agua | P | A | - | - | - | - |
| | [N.*] Desastres naturales | P | A | - | - | - | - |
| | [I.3] Contaminación medioambiental | P | A | - | - | - | - |
| | [I.5] Avería de origen físico o lógico | P | A | - | - | - | - |
| | [I.7]Condiciones inadecuadas de temperatura o humedad | MA | MA | | | | |
| | [E.2] Errores del administrador del sistema / de la seguridad | P | M | M | M | - | - |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | [E.23] Errores de mantenimiento / actualización de equipos (hardware) | P | M | - | - | - | - |
| | [A.11] Acceso no autorizado | MA | - | A | A | - | - |
| | [A.23] Manipulación del hardware | MA | A | - | A | - | - |
| MEDIOS DE IMPRESIÓN | [I.5] Avería de origen físico o lógico | P | M | - | - | - | - |
| | [I.7] Condiciones inadecuadas de temperatura o humedad | P | M | - | - | - | - |
| | [E.23] Errores de mantenimiento / actualización de equipos (hardware) | P | M | - | - | - | - |
| | [A.11] Acceso no autorizado | PP | - | M | M | - | - |
| COMPUTADOR AS DE ESCRITORIO | [N.2] Daños por agua | PP | M | - | - | - | - |
| | [N.*] Desastres naturales | PP | M | - | - | - | - |
| | [I.*] Desastres industriales | P | B | - | - | - | - |
| | [I.5] Avería de origen físico o lógico | P | M | - | - | - | - |
| | [I.7] Condiciones inadecuadas de temperatura o humedad | PP | M | - | - | - | - |
| | [E.23] Errores de mantenimiento / actualización de equipos (hardware) | P | M | - | - | - | - |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | [E.24] Caída del sistema por agotamiento de recursos | P | M | - | - | - | - |
| | [A.6] Abuso de privilegios de acceso | PP | M | M | M | - | - |
| | [A.7] Uso no previsto | P | M | B | M | - | - |
| ROUTER | [N.1] Fuego | PP | M | - | - | - | - |
| | [N.2] Daños por agua | PP | M | - | - | - | - |
| | [N.*] Desastres naturales | PP | M | - | - | - | - |
| | [I.3] Contaminación medioambiental | PP | M | - | - | - | - |
| | [I.5] Avería de origen físico o lógico | P | M | - | - | - | - |
| | [I.7] Condiciones inadecuadas de temperatura o humedad | P | M | - | - | - | - |
| | [A.11] Acceso no autorizado | PP | - | B | B | - | - |
| RED WIFI | [I.8] Fallo de servicios de comunicaciones | P | M | - | - | - | - |
| | [E.9] Errores de [re-]encaminamiento | P | - | - | B | - | - |
| RED LAN | [I.8] Fallo de servicios de comunicaciones | PP | B | - | - | - | - |
| | [E.9] Errores de [re-]encaminamiento | P | - | - | M | - | - |
| | [E.10] Errores de secuencia | P | - | M | - | - | - |
| | [A.5] Suplantación de la identidad del usuario | P | - | M | M | M | - |
| | [A.9] [Re-]encaminamiento de mensajes | P | - | - | M | - | - |
| | [A.10] Alteración de secuencia | P | - | M | - | - | - |
| | [A.11] Acceso no autorizado | PP | - | M | - | - | - |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| INTERNET | [I.8] Fallo de servicios de comunicaciones | P | A | - | - | - | - |
| | [E.15] Alteración de la información | P | - | B | - | - | - |
| CABLEADO | [I.3] Contaminación medioambiental | PP | A | - | - | - | - |
| | [I.4] Contaminación electromagnética | MR | B | - | - | - | - |
| MOBILIARIO | [I.3] Contaminación medioambiental | PP | M | - | - | - | - |
| SISTEMA DE VIGILANCIA | [I.3] Contaminación medioambiental | PP | M | - | - | - | - |
| | [I.7] Condiciones inadecuadas de temperatura o humedad | MA | A | - | - | - | - |
| SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA | [I.3] Contaminación medioambiental | PP | M | - | - | - | |
| OTROS EQUIPOS | [I.3] Contaminación medioambiental | P | M | - | - | - | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| AUXILIARES | | | | | | | |
| CD | [E.15] Alteración de la información | PP | - | B | - | - | - |
| | [E.19] Fugas de información | PP | - | - | B | - | - |
| | [A.15] Modificación de la información | PP | - | B | - | - | - |
| | [A.19] Revelación de información | PP | - | - | B | - | - |
| EDIFICIO | [N.1] Fuego | P | A | - | - | - | - |
| | [N.2] Daños por agua | P | A | - | - | - | - |
| | [N.*] Desastres naturales | P | A | - | - | - | - |
| | [N.*.4] Terremotos | P | M | - | - | - | - |
| | [N.*.9] Tsunamis | P | M | - | - | - | - |
| | [N.*.11] Calor extremo | MA | B | - | - | - | - |
| | [I.*] Desastres industriales | P | B | - | - | - | - |
| | [A.27] Ocupación enemiga | P | MA | - | A | - | - |
| | [A.11] Acceso no autorizado | P | - | A | M | - | - |
| | [A.27] Ocupación enemiga | P | M | - | M | - | - |
| JEFA DEL DTO. CONTABILIDA | [E.28.1] Enfermedad | P | M | M | M | - | - |
| | [E.28.2] Huelga | PP | B | - | - | - | - |
| | [A.29] Extorsión | PP | M | M | M | - | - |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| D | [A.30] Ingeniería social (picaresca) | MA | A | A | B | - | - |
| JEFA DEL DTO. DE RECURSOS HUMANOS | [E.28.1] Enfermedad | P | M | M | M | - | - |
| JEFA DEL DTO. DE VENTAS | [A.29] Extorsión | PP | M | M | M | - | - |
| | [A.30] Ingeniería social (picaresca) | MA | A | A | B | - | - |
| | [E.28.2] Huelga | PP | B | - | - | - | - |
| JEFA DEL DTO. DE MERCADEO | [A.29] Extorsión | PP | M | B | M | - | - |
| | [A.30] Ingeniería social (picaresca) | P | MA | - | - | - | - |
| | [E.28.1] Enfermedad | P | M | - | - | - | - |
| | [E.28.2] Huelga | PP | M | M | M | - | - |

## E. Modelo de Valor

| | |
|---|---|
| ***AR_PIB*** | TESIS |
| ***desc*** | ANÁLISIS DE RIESGOS |
| ***Resp*** | ING. SANDRA BORRERO |
| ***Org*** | TECNOVAL SYSTEM |
| ***date*** | 26-OCTUBRE-2018 |

Descripción

Realizado para un monografía de trabajo de grado en la Universidad Nacional Abierta y a Distancia

Licencia

[edu] Universidad Nacional Abierta y a Distancia

Dimensiones

- [D] disponibilidad
- [I] integridad de los datos
- [C] confidencialidad de los datos
- [A] autenticidad de los usuarios y de la información
- [T] trazabilidad del servicio y de los datos

Dominios de seguridad

- [base_seguridad] baseseguridad

Activos

Capa - [IS] Servicios internos [INTERNET_PIB] INTERNET

Capa - [E] Equipamiento

[SW] Aplicaciones [OFF_PIB] OFIMÁTICA [AV_PIB] ANTIVIRUS [OS_PIB] SISTEMA OPERATIVO [OTR_PIB] OTROS SOFTWARE

[HW] Equipos [SDB_PIB] SERVIDOR DE BASE DE DATOS [PRINT_PIB] MEDIOS DE IMPRESIÓN [PC_PIB] COMPUTADORAS DE ESCRITORIO [ROUTER_PIB] ROUTER

[COM] Comunicaciones [IPPHONE_PIB] TELEFONÍA IP [WIFI_PIB] RED WIFI [LAN_PIB] RED LAN [IEX_PIB] INTERNET

[AUX] Elementos auxiliares
[POWER_PIB] GENERADOR ELÉCTRICO [CABLING_PIB] CABLEADO
[MOB_PIB] MOBILIARIO
[SISVG_PIB] SISTEMA DE VIGILANCIA [ANT_PIB] ANTENAS
[SAI_PIB] SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA [AUXOTR_PIB] OTROS EQUIPOS AUXILIARES
[MEDIA] Soportes de Información [CD_PIB] CD
Capa - [L] Instalaciones

[BUILDING_PIB] EDIFICIO
Capa - [P] Personal

[JF_PIB] JEFA DEL DEPARTAMENTO RECURSOS HUMANOS [DBA_PIB] MANTENIMIENTO BD
[JC_PIB] JEFA DEL DEPARTAMENTO DE CONTABILIDAD [JLC_PIB] JEFA DEL DEPARTAMENTO DE VENTAS [JP_PIB] JEFA DEL DEPARTAMENTO DE MERCADEO
Resumen de valoración [IS] Servicios internos

| ***activo*** | [D] | [I] | [C] | [A] | [T] |
|---|---|---|---|---|---|
| [INTERNET_PIB] INTERNET | [7](1) | | | [7] | [7] |

(1) [1.da] Pudiera causar la interrupción de actividades propias de la Organización

[E] Equipamiento

| ***Activo*** | [D] | [I] | [C] | [A] | [T] |
|---|---|---|---|---|---|
| [SW.OFF_PIB] OFIMÁTICA | | | | | [7] |
| [SW.AV_PIB] ANTIVIRUS | | | | | [7] |
| [SW.OS_PIB] SISTEMA OPERATIVO | | | | | [7] |
| [SW.OTR_PIB] OTROS SOFTWARE | | | | | [5] |
| [HW.SDB_PIB] SERVIDOR DE BASE DE DATOS | | [9] | [9] | [9] | [9] |
| [HW.PRINT_PIB] MEDIOS DE IMPRESIÓN | | | | | [6] |
| [HW.PC_PIB] COMPUTADORAS DE ESCRITORIO | | | | | [8] |
| [HW.ROUTER_PIB] ROUTER | | | | | [8] |
| [COM.WIFI_PIB] RED WIFI | | | | | [7] |
| [COM.IEX_PIB] INTERNET | | [7] | [7] | | |
| [AUX.CABLING_PIB] CABLEADO DE DATOS | [7](1) | | | | |

| | | | | | |
|---|---|---|---|---|---|
| [AUX.MOB_PIB] MOBILIARIO | [7] | | | | |
| [AUX.SISVG_PIB] SISTEMA DE VIGILANCIA | [7] | | | | |
| [AUX.ANT_PIB] ANTENAS | [7] | | | | |
| [AUX.RAD_PIB] RADIOS | [7] | | | | |
| [AUX.SAI_PIB] SISTEMA DE ALIMENTACIÓN INITERRUMPIDA | [7] | | | | |
| [AUX.AUXOTR_PIB] OTROS EQUIPOS AUXILIARES | [7] | | | | |
| [MEDIA.CD_PIB] CD | | [8] | [8] | | |

(1) [lg] Pérdida de Confianza (Reputación):

[L] Instalaciones

| ***Activo*** | [D] | [I] | [C] | [A] | [T] |
|---|---|---|---|---|---|
| [BUILDING_PIB] EDIFICIO | | | [8] | | |

[P] Personal

| ***Activo*** | [D] | [I] | [C] | [A] | [T] |
|---|---|---|---|---|---|
| [JF_PIB] JEFA DEL DEPARTAMENTO RECURSOS HUMANOS | | | [8] | | |
| [DBA_PIB] MANTENIMIENTO BD | | | [7] | | |
| [JC_PIB] JEFA DEL DEPARTAMENTO DE CONTABILIDAD | | | [8] | | |
| [JLC_PIB] JEFA DEL DEPARTAMENTO DE VENTAS | | | [8] | | |
| [JP_PIB] JEFA DEL DEPARTAMENTO DE MERCADEO | | | [8] | | |

Activos

[TELF_PIB] TELEFONÍA IP

- [S] Servicios
- [S.int] interno (usuarios y medios de la propia organización)
- [S.voip] voz sobre ip

Dominio de seguridad

- [base_seguridad] baseseguridad

Datos

| | |
|---|---|
| **CANTIDAD** | 7 |
| **TIPO** | ALAMBRICO |

Descripción

Control de servicios a través de equipo IP , Call Manager y transferencia.

Superiores (activos que dependen de este)

- [SW.OS_PIB] SISTEMA OPERATIVO

Valor

| ***Dimensión*** | ***valor*** | ***valores acumulados*** |
|---|---|---|
| [D] disponibilidad | [6] | [6] |
| [I] integridad de los datos | | [9] |
| [C] confidencialidad de los datos | | [9] |
| [A] autenticidad de los usuarios y de la información | [7] | [9] |
| [T] trazabilidad del servicio y de los datos | [7] | [9] |

[INTERNET_PIB] INTERNET

- [S] Servicios
- [S.www] world wide web

Dominio de seguridad

- [base_seguridad] baseseguridad

Datos

| | |
|---|---|
| **DISEÑO** | HTML, XML |
| **PROTOCOLO** | HTTP, FTP |
| **SISTEMA OPERATIVO** | WINDOWS |
| **VERSION** | XP |

Descripción

Es utilizado para la navegación de internet y la configuración de router

Superiores (activos que dependen de este)

- [SW.OS_PIB] SISTEMA OPERATIVO

Valor

| ***Dimensión*** | ***valor*** | ***valores acumulados*** |
|---|---|---|
| [D] disponibilidad | [7](1) | [7] |
| [I] integridad de los datos | | [9] |
| [C] confidencialidad de los datos | | [9] |
| [A] autenticidad de los usuarios y de la información | [7] | [9] |
| [T] trazabilidad del servicio y de los datos | [7] | [9] |

(1) [1.da] Pudiera causar la interrupción de actividades propias de la Organización

[SW.OFF_PIB] OFIMATICA

- [SW] Aplicaciones (software)
- [SW.std] estándar (off the shelf)
- [SW.std.office] ofimática
- [SW.std.os] sistema operativo
- [SW.std.os.windows] windows

Dominio de seguridad

- [base_seguridad] baseseguridad

Datos

| | |
|---|---|
| **SISTEMA OPERATIVO WINDOWS** | MICROSOFT 2013 |

Descripción

ES UTILIZADO PARA FUNCIONES DE TEXTO, HOJAS DE CÁLCULO, ETC.

Inferiores (activos de los que depende este)

- [HW.SDB_PIB] SERVIDOR DE BASE DE DATOS

Valor

| ***Dimensión*** | ***valor*** | ***valores acumulados*** |
|---|---|---|
| [I] integridad de los datos | | [9] |
| [C] confidencialidad de los datos | | [9] |
| [A] autenticidad de los usuarios y de la | | [9] |

| | | |
|---|---|---|
| información | | |
| [T] trazabilidad del servicio y de los datos | [7] | [9] |

[SW.AV_PIB] ANTIVIRUS

- [D] Datos / Información
- [D.other] otros ...
- [SW] Aplicaciones (software)
- [SW.std] estándar (off the shelf)
- [SW.std.av] anti virus
- [SW.std.os] sistema operativo
- [SW.std.os.windows] windows

Dominio de seguridad

- [base_seguridad] baseseguridad

Datos

| ***NOMBRE*** | AVAST |
|---|---|

Descripción

ES UTILIZADO PARA DESINFECTAR MEMORIAS USB Y PARA ANALIZAR SU PROPIO COMPUTADOR PARA PROTEGERLO DE VIRUS INFORMÁTICO O DE PROGRAMAS MALICIOSOS.

Superiores (activos que dependen de este)

- [HW.SDB_PIB] SERVIDOR DE BASE DE DATOS

Valor

| ***Dimensión*** | ***valor*** | ***valores acumulados*** |
|---|---|---|
| [I] integridad de los datos | | [9] |
| [C] confidencialidad de los datos | | [9] |
| [A] autenticidad de los usuarios y de la información | | [9] |
| [T] trazabilidad del servicio y de los datos | [7] | [9] |

[SW.OS_PIB] SISTEMA OPERATIVO

- [SW] Aplicaciones (software)
- [SW.std] estándar (off the shelf)
- [SW.std.os] sistema operativo
- [SW.std.os.windows] windows

Dominio de seguridad

- [base_seguridad] baseseguridad

Datos

| | |
|---|---|
| ***NOMBRE*** | WINDOWS 10 |

Descripción

ES UTILIZADO PARA REALIZAR TAREAS COMO:

- ADMINISTRACIÓN DEL PROCESADOR
- GESTIÓN DE ENTRADAS/SALIDAS
- GESTIÓN DE EJECUCIÓN DE APLICACIONES
- GESTIÓN DE ARCHIVOS
- GESTIÓN DE LA INFORMACIÓN

Inferiores (activos de los que depende este)

- [TELF_PIB] TELEFONÍA IP
- [INTERNET_PIB] INTERNET
- [SW.OTR_PIB] OTROS SOFTWARE
- [HW.SDB_PIB] SERVIDOR DE BASE DE DATOS
- [MEDIA.CD_PIB] CD

Valor

| ***Dimensión*** | ***valor*** | ***valores acumulados*** |
|---|---|---|
| [I] integridad de los datos | | [9] |
| [C] confidencialidad de los datos | | [9] |
| [A] autenticidad de los usuarios y de la información | | [9] |
| [T] trazabilidad del servicio y de los datos | [7] | [9] |

[SW.OTR_PIB] OTROS SOFTWARE

- [SW] Aplicaciones (software)
- [SW.std] estándar (off the shelf)

Dominio de seguridad

- [base_seguridad] baseseguridad

Datos

| | |
|---|---|
| ***SOFTWARE 1*** | WINRAR |

Descripción

LOS PROGRAMAS MÁS UTILIZADOS POR PARTE DE LOS EMPLEADOS

Superiores (activos que dependen de este)

- [SW.OS_PIB] SISTEMA OPERATIVO

Inferiores (activos de los que depende este)

- [HW.SDB_PIB] SERVIDOR DE BASE DE DATOS

Valor

| ***Dimensión*** | ***valor*** | ***valores acumulados*** |
|---|---|---|
| [I] integridad de los datos | | [9] |
| [C] confidencialidad de los datos | | [9] |
| [A] autenticidad de los usuarios y de la información | | [9] |
| [T] trazabilidad del servicio y de los datos | [5] | [9] |

[HW.SDB_PIB] SERVIDOR DE BASE DE DATOS

- [HW] Equipamiento informático (hardware)
- [HW.pc] informática personal
- [HW.backup] equipamiento de respaldo
- [HW.data] que almacena datos

Dominio de seguridad

- [base_seguridad] baseseguridad

Datos

| | |
|---|---|
| ***SISTEMA OPERATIVO*** | WINDOWS SERVER 20016 |

Descripción

LA BASE DE DATOS ALMACENA INFORMACIÓN DEL SISTEMA

Superiores (activos que dependen de este)

- [SW.OFF_PIB] OFIMÁTICA
- [SW.AV_PIB] ANTIVIRUS
- [SW.OS_PIB] SISTEMA OPERATIVO
- [SW.OTR_PIB] OTROS SOFTWARE

Inferiores (activos de los que depende este)

- [HW.PC_PIB] COMPUTADORAS DE ESCRITORIO

Valor

| ***Dimensión*** | ***valor*** | ***valores acumulados*** |
|---|---|---|
| [I] integridad de los datos | [9] | [9] |
| [C] confidencialidad de los datos | [9] | [9] |
| [A] autenticidad de los usuarios y de la información | [9] | [9] |
| [T] trazabilidad del servicio y de los datos | [9] | [9] |

[HW.PRINT_PIB] MEDIOS DE IMPRESIÓN

- [HW] Equipamiento informático (hardware)
- [HW.peripheral] periféricos
- [HW.peripheral.print] medios de impresión

- [HW.peripheral.scan] escáner
- [HW.peripheral.other] otros ...

Dominio de seguridad

- [base_seguridad] baseseguridad

Datos

| | |
|---|---|
| ***IMPRESORA1*** | LEXMARK |
| ***IMPRESORA2*** | EPSON |
| ***IMPRESORA3*** | HP PHOTOSMART C4780 |
| ***IMPRESORA4*** | MULTIFUNCIÓN TOSHIBA STUDIO 202S |

Descripción

SIRVEN PARA IMPRIMIR LOS DIFERENTES INFORMES QUE REQUIEREN PARA SUS ACTIVIDADES DIARIAS

Superiores (activos que dependen de este)

- [HW.PC_PIB] COMPUTADORAS DE ESCRITORIO **Inferiores (activos de los que depende este)** [BUILDING_PIB] EDIFICIO

Valor

| ***Dimensión*** | ***valor*** | ***valores acumulados*** |
|---|---|---|
| [I] integridad de los datos | | [9] |
| [C] confidencialidad de los datos | | [9] |
| [A] autenticidad de los usuarios y de la información | | [9] |
| [T] trazabilidad del servicio y de los datos | [6] | [9] |

[HW.PC_PIB] COMPUTADORAS DE ESCRITORIO

- [HW] Equipamiento informático (hardware)
- [HW.pc] informática personal

Dominio de seguridad

- [base_seguridad] baseseguridad

Datos

| | |
|---|---|
| ***MARCA*** | INTEL |
| ***PROCESADOR*** | CORE DOS DUO |
| ***MEMORIA RAM*** | 2 GB |

| | |
|---|---|
| ***UBICACIÓN*** | ESTA DENTRO DE LAS INSTALACIONES DE LA EMPRESA |
| ***CANTIDAD*** | 7 |

Descripción

Estas computadoras son pc clon que tiene instalado solo Windows XP, que son utilizadas para ejecutar las operaciones cotidianas en la empresa.

Superiores (activos que dependen de este)

- [HW.SDB_PIB] SERVIDOR DE BASE DE DATOS

Inferiores (activos de los que depende este)

- [HW.PRINT_PIB] MEDIOS DE IMPRESIÓN
- [HW.ROUTER_PIB] ROUTER
- [AUX] Elementos auxiliares
- [MEDIA.CD_PIB] CD

Valor

| ***Dimensión*** | ***valor*** | ***valores acumulados*** |
|---|---|---|
| [I] integridad de los datos | | [9] |
| [C] confidencialidad de los datos | | [9] |
| [A] autenticidad de los usuarios y de la información | | [9] |
| [T] trazabilidad del servicio y de los datos | [8] | [9] |

[HW.ROUTER_PIB] ROUTER

- [HW] Equipamiento informático (hardware)
- [HW.network] soporte de la red
- [HW.network.router] encaminador
- [HW.network.gtwy] pasarela
- [HW.network.wap] punto de acceso wireless

Dominio de seguridad

- [base_seguridad] baseseguridad

Datos

| | |
|---|---|
| ***MARCA*** | D LINK D |
| ***MODELO*** | DES-1024 |
| ***AÑO*** | 3 AÑOS |
| ***CANTIDAD*** | 2 |

Descripción

Es utilizado para interconectar redes cableadas y permite proveer de servicios a los equipos que hagan la petición.

Superiores (activos que dependen de este)

- [HW.PC_PIB] COMPUTADORAS DE ESCRITORIO

Inferiores (activos de los que depende este)

- [COM.WIFI_PIB] RED WIFI
- [COM.LAN_PIB] RED LAN
- [BUILDING_PIB] EDIFICIO

Valor

| ***Dimensión*** | ***valor*** | ***valores acumulados*** |
|---|---|---|
| [I] integridad de los datos | | [9] |
| [C] confidencialidad de los datos | | [9] |
| [A] autenticidad de los usuarios y de la información | | [9] |
| [T] trazabilidad del servicio y de los datos | [8] | [9] |

[COM.IPPHONE_PIB] TELEFONÍA IP

- [COM] Redes de comunicaciones
- [COM.radio] red inalámbrica

Dominio de seguridad

- [base_seguridad] baseseguridad

Datos

Inferiores (activos de los que depende este)

- [BUILDING_PIB] EDIFICIO

Valor

| ***Dimensión*** | ***valor*** | ***valores acumulados*** |
|---|---|---|
| [I] integridad de los datos | [7] | [7] |

[COM.WIFI_PIB] RED WIFI

- [COM] Redes de comunicaciones
- [COM.wifi] WiFi
- [COM.Internet] Internet

Dominio de seguridad

- [base_seguridad] baseseguridad

Datos

| | |
|---|---|
| ***SISTEMA*** | WIFI |
| ***DISTANCIA*** | 100 METROS |
| ***TOPOLOGÍA*** | ESTRELLA |

Descripción

Es utilizado por equipos que puedan conectarse a la red wifi que posee la empresa para cumplir con sus respectivas actividades de trabajo

Superiores (activos que dependen de este)

[HW.ROUTER_PIB] ROUTER

Inferiores (activos de los que depende este)

[COM.IEX_PIB] INTERNET

Valor

| ***Dimensión*** | ***valor*** | ***valores acumulados*** |
|---|---|---|
| [I] integridad de los datos | | [9] |
| [C] confidencialidad de los datos | | [9] |
| [A] autenticidad de los usuarios y de la información | | [9] |
| [T] trazabilidad del servicio y de los datos | [7] | [9] |

[COM.LAN_PIB] RED LAN

- [COM] Redes de comunicaciones
- [COM.LAN] red local
- [COM.Internet] Internet

Dominio de seguridad

- [base_seguridad] baseseguridad

Datos

| | |
|---|---|
| ***INTERCONEXIÓN*** | COMPUTADORAS Y PERIFÉRICOS |
| ***DISTANCIA*** | 50 METROS |
| ***CATEGORÍA*** | 6 |

**Descripción**

ES RED LAN ES UNA RED PARA DATOS SE ENCUENTRA DENTRO DE LA EMPRESA

Superiores (activos que dependen de este)

[HW.ROUTER_PIB] ROUTER

Inferiores (activos de los que depende este)

[COM.IEX_PIB] INTERNET

Valor

| ***Dimensión*** | ***valor*** | ***valores acumulados*** |
|---|---|---|
| [I] integridad de los datos | | [9] |
| [C] confidencialidad de los datos | | [9] |
| [A] autenticidad de los usuarios y de la información | | [9] |
| [T] trazabilidad del servicio y de los datos | [7] | [9] |

[COM.IEX_PIB] INTERNET

- [COM] Redes de comunicaciones
- [COM.Internet] Internet

Dominio de seguridad

- [base seguridad] base seguridad

Datos

| | |
|---|---|
| ***TIPO*** | ETHERNET Y WIRELESS |
| ***ISP*** | ROMEO VINTIMILLA |

Descripción

Se utilizó para envío de información, además de gestionar trámites de empleados en la página del Ministerio de Trabajo y tramitar en la página correspondiente

Superiores (activos que dependen de este)

- [COM.WIFI_PIB] RED WIFI
- [COM.LAN_PIB] RED LAN

Valor

| ***Dimensión*** | ***valor*** | ***valores acumulados*** |
|---|---|---|
| [I] integridad de los datos | [7] | [9] |
| [C] confidencialidad de los datos | [7] | [9] |
| [A] autenticidad de los usuarios y de la información | | [9] |
| [T] trazabilidad del servicio y de los datos | | [9] |

[AUX.CABLING_PIB] CABLEADO DE DATOS

- [AUX] Equipamiento auxiliar
- [AUX.cabling] CABLEADO de datos
- [AUX.cabling.wire] cable eléctrico

Dominio de seguridad

- [base_seguridad] baseseguridad

Superiores (activos que dependen de este)

- [AUX] Elementos auxiliares

Valor

| ***Dimensión*** | ***valor*** | ***valores acumulados*** |
|---|---|---|
| [D] disponibilidad | [7](1) | [7] |
| [I] integridad de los datos | | [9] |
| [C] confidencialidad de los datos | | [9] |
| [A] autenticidad de los usuarios y de la información | | [9] |
| [T] trazabilidad del servicio y de los datos | | [9] |

(1) [lg] Pérdida de Confianza (Reputación):

[AUX.MOB_PIB] MOBILIARIO

- [AUX] Equipamiento auxiliar
- [AUX.furniture] mobiliario
- [AUX.other] otros ...

Dominio de seguridad

- [base_seguridad] baseseguridad

Superiores (activos que dependen de este)

- [AUX] Elementos auxiliares

Valor

| ***Dimensión*** | ***valor*** | ***valores acumulados*** |
|---|---|---|
| [D] disponibilidad | [7] | [7] |
| [I] integridad de los datos | | [9] |
| [C] confidencialidad de los datos | | [9] |
| [A] autenticidad de los usuarios y de la información | | [9] |
| [T] trazabilidad del servicio y de los datos | | [9] |

[AUX.SISVG_PIB] SISTEMA DE VIGILANCIA

- [AUX] Equipamiento auxiliar
- [AUX.other] otros ...

Dominio de seguridad

- [base_seguridad] baseseguridad

Superiores (activos que dependen de este)

- [AUX] Elementos auxiliares

Valor

| ***Dimensión*** | ***valor*** | ***valores acumulados*** |
|---|---|---|
| [D] disponibilidad | [7] | [7] |
| [I] integridad de los datos | | [9] |
| [C] confidencialidad de los datos | | [9] |
| [A] autenticidad de los usuarios y de la información | | [9] |
| [T] trazabilidad del servicio y de los datos | | [9] |

[AUX.ANT_PIB] ANTENAS

- [AUX] Equipamiento auxiliar
- [AUX.other] otros ...

Dominio de seguridad

- [base_seguridad] baseseguridad

Superiores (activos que dependen de este)

- [AUX] Elementos auxiliares

Valor

| ***Dimensión*** | ***valor*** | ***valores acumulados*** |
|---|---|---|
| [D] disponibilidad | [7] | [7] |
| [I] integridad de los datos | | [9] |
| [C] confidencialidad de los datos | | [9] |
| [A] autenticidad de los usuarios y de la información | | [9] |
| [T] trazabilidad del servicio y de los datos | | [9] |

[MEDIA.CD_PIB] CD

- [D] Datos / Información
- [D.backup] copias de respaldo
- [Media] Soportes de información
- [Media.electronic] electrónicos
- [Media.electronic.disk] discos
- [Media.electronic.cd] cederrón (CD-ROM)

Dominio de seguridad

- [base_seguridad] baseseguridad

Descripción

DESPUÉS DE CADA JORNADA LABORAL TIENEN QUE GRABAR LA

INFORMACIÓN EN CDs

Superiores (activos que dependen de este)

- [SW.OS_PIB] SISTEMA OPERATIVO
- [HW.PC_PIB] COMPUTADORAS DE ESCRITORIO

Inferiores (activos de los que depende este)

- [BUILDING_PIB] EDIFICIO

Valor

| ***Dimensión*** | ***valor*** | ***valores acumulados*** |
|---|---|---|
| [I] integridad de los datos | [8] | [9] |
| [C] confidencialidad de los datos | [8] | [9] |
| [A] autenticidad de los usuarios y de la información | | [9] |
| [T] trazabilidad del servicio y de los datos | | [9] |

[BUILDING_PIB] EDIFICIO

- [L] Instalaciones
- [L.building] edificio

Dominio de seguridad

- [base_seguridad] baseseguridad

Superiores (activos que dependen de este)

- [HW.PRINT_PIB] MEDIOS DE IMPRESIÓN
- [HW.ROUTER_PIB] ROUTER
- [COM.IPPHONE_PIB] TELEFONÍA IP
- [MEDIA.CD_PIB] CD

Valor

| ***Dimensión*** | ***valor*** | ***valores acumulados*** |
|---|---|---|
| [I] integridad de los datos | | [9] |
| [C] confidencialidad de los datos | [8] | [9] |
| [A] autenticidad de los usuarios y de la información | | [9] |
| [T] trazabilidad del servicio y de los datos | | [9] |

[JF_PIB] JEFA DEL DEPARTAMENTO FINANCIERO

- [P] Personal
- [P.ui] usuarios internos
- [P.other] otros ...

Dominio de seguridad

- [base_seguridad] baseseguridad

Valor

| ***Dimensión*** | ***valor*** | ***valores acumulados*** |
|---|---|---|
| [C] confidencialidad de los datos | [8] | [8] |

[DBA_PIB] MANTENIMIENTO BD

- [P] Personal
- [P.dba] administradores de BBDD
- [P.dev] desarrolladores / programadores

Dominio de seguridad

- [base_seguridad] baseseguridad

Valor

| ***Dimensión*** | ***valor*** | ***valores acumulados*** |
|---|---|---|
| [C] confidencialidad de los datos | [7] | [7] |

SP_PIB] MANTENIMIENTO EQ

- [P] Personal
- [P.adm] administradores de sistemas

Dominio de seguridad

- [base_seguridad] baseseguridad

Descripción

PERSONA ENCARGADA DEL SOPORTE TÉCNICO EN LA EMPRESA

Valor

| ***Dimensión*** | ***valor*** | ***valores acumulados*** |
|---|---|---|
| [C] confidencialidad de los datos | [7] | [7] |

[JC_PIB] JEFA DEL DEPARTAMENTO DE CONTABILIDAD

- [P] Personal
- [P.ui] usuarios internos
- [P.other] otros ...

Dominio de seguridad

- [base_seguridad] baseseguridad Valor

| ***Dimensión*** | ***valor*** | ***valores acumulados*** |
|---|---|---|
| [C] confidencialidad de los datos | [8] | [8] |

[JLC_PIB] JEFA DEL DEPARTAMENTO DE VENTAS

- [P] Personal
- [P.ui] usuarios internos
- [P.other] otros ...

Dominio de seguridad

- [base_seguridad] baseseguridad

Valor

| ***Dimensión*** | ***valor*** | ***valores acumulados*** |
|---|---|---|
| [C] confidencialidad de los datos | [8] | [8] |

[JP_PIB] JEFA DEL DEPARTAMENTO DE MERCADEO

- [P] Personal
- [P.ui] usuarios internos
- [P.other] otros ...

Dominio de seguridad

- [base_seguridad] baseseguridad

Valor

| ***Dimensión*** | ***valor*** | ***valores acumulados*** |
|---|---|---|
| [C] confidencialidad de los datos | [8] | [8] |

**RESUMEN ANALITICO EDUCATIVO**
**RAE**

| | |
|---|---|
| **Título del texto** | ESTUDIO DEL ESTADO DE SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA TECNOVAL SYSTEM PARA DESARROLLAR POLÍTICAS DE SEGURIDAD |
| **Autor** | Sandra Johana Borrego Plata |
| **Edición** | Universidad nacional abierta y a distancia |
| **Fecha elaboración** | 09 de diciembre de 2018 |
| **Palabras Claves** | Magerit, Riesgo, Análisis, Seguridad, Información, Políticas de Seguridad, Vulnerabilidad, Salvaguarda. |
| **Descripción:** Monografía para optar por el título de especialista en seguridad informática de la universidad abierta y a distancia. | |
| **Fuentes:** | 18 fuentes bibliográficas |

**Contenidos:** La presente monografía, tiene como fin la aplicación del modelo MAGERIT versión 2 -Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información-, para poder llegar al objetivo principal que sería, contribuir a que la empresa TECNOVAL SYSTEM posea un conocimiento claro sobre los riesgos que pueden presentarse en sus sistemas de información.

Siguiendo una serie de pasos, empezando por un análisis de riesgos para la empresa TECNOVAL SYSTEM con el fin de garantizar mayor efectividad y eficiencia dentro de cada uno de los procesos; teniendo en cuenta que al conocer las fortalezas y debilidades se mejoran los controles y administración de recursos tecnológicos acorde a los estándares nacionales e internacionales que buscan proporcionar mecanismos y herramientas para adoptar buenas prácticas.

TECNOVAL SYSTEM a pesar de ser una empresa que se dedica a comercializar elementos de seguridad tales como cámaras, alarmas comunitarias, ventas de computadores, impresoras y otros elementos informáticos carece de políticas o estrategias organizacionales que le permitan controlar la integralidad, disponibilidad y confiabilidad de su información, producto de la ejecución de las actividades propias de su razón social. Encontramos que su red de datos tiene una minina seguridad en la configuración de su cifrado, los dispositivos de interconexión de red se encuentran expuestos a terceros, entre otros.

El desarrollo de esta monografía es muy importante para la empresa TECNOVAL SYSTEM, ya que se están realizando todas las adecuaciones tecnológicas y de infraestructura para el ajuste de procesos y restructuración de las distintas áreas brindando a cada uno de los departamentos de la empresa el control de los riesgos de información basándose en reglas y controles claros que definan el

| |
|---|
| mantenimiento de las mismas, minimizando los riesgos lo menor posible; mejorando los objetivos claros establecidos. Beneficiando así a los usuarios de la empresa. |
| **Metodología:** Para el desarrollo de la metodología de esta monografía se escogió la Metodología MAGERIT, ya que es la más se ajusta a las necesidades de este tipo de monografía. Las fichas de captura de datos recogen información específica de cada activo perteneciente a la empresa tomando en cuenta como dimensiones de seguridad y dependencias de activos, que ayudara a identificar correctamente lo que son: vulnerabilidades, impactos salvaguardas efectivas. La situación de la seguridad de los sistemas de información de la empresa Tecnoval System, es el resultado de a la incorporación de salvaguardas tomadas para prevenir o reducir riesgos que no han sido debidamente estudiadas de forma sistemática. Hasta ahora no habido ningún fallo operacional informático de gravedad en el que se hayan forzado a tomar precauciones drásticas.<br>Gracias al análisis de riesgos permitirá sistematizar las medidas actuales y mejorarlas con algunas otras que serán suficientes para lograr un nivel de seguridad estable.<br>Esta empresa dispone de los recursos a utilizarse para el desarrollo de la monografía en disponibilidad de equipos, tiempos planificados, medios materiales-herramientas, envió de documentos y manuales. |
| **Conclusiones:** La empresa “TECNOVAL SYSTEM.” no tiene medidas de seguridad guiada y documentada, por lo cual este estudio será de gran beneficio para minimizar riesgos en el futuro.<br>Gracias a la metodología Magerit donde se siguió una serie de pasos estructurados para el análisis y gestión de riesgos, fase fundamental en este estudio ya que se obtuvo resultados realistas del estado de riesgo actual en la empresa donde se supo escoger que medidas serán necesarias para mitigar el riesgo.<br>La herramienta PILAR fue de gran ayuda en esta monografía de trabajo de grado ya que ayudo en la valoración de los riesgos en diferentes etapas potencial, situación actual y objetivo. Gracias a este software se supo de manera directa que mecanismos de seguridad se tienen que implementar en esta empresa.<br>Después de haber realizado esta monografía, la empresa obtendrá un documento encaminado a la seguridad que será punto de partida para la creación de normativas de seguridad para los recursos informáticos y para los empleados que laboran en la empresa. |
| **Autor del RAE: Sandra Johana Borrego Plata** |