DISEÑAR UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) A LA EMPRESA UNITRANSA S.A. UBICADA EN LA CIUDAD DE BUCARAMANGA

GERMÁN GARCÍA RAMÍREZ
JAIME CASTRO ANGARITA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA-UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BUCARAMANGA
2017

DISEÑAR UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) A LA EMPRESA UNITRANSA S.A. UBICADA EN LA CIUDAD DE BUCARAMANGA

GERMÁN GARCÍA RAMÍREZ
JAIME CASTRO ANGARITA

Trabajo de grado para optar al título de Especialista en Seguridad Informática

Director
Martín Camilo Cancelado Ruiz
Ingeniero de Sistemas

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA-UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BUCARAMANGA
2017

Nota de Aceptación

_____
_____
_____
_____
_____
_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Bucaramanga, abril de 2017

AGRADECIMIENTOS

De una manera especial agradezco a DIOS por su infinita misericordia al darme la vida y llenarme todos los días de sabiduría, salud, fortaleza, esperanza y deseos de aprender.

Agradezco a mis padres Heraclio García y Ubaldina Ramírez por formar en mí los valores que me hacen una persona responsable, justa y útil a la sociedad.

Gracias doy a mi esposa y a mis hijos por su apoyo incondicional, por sus frases de aliento y aceptar sin reproches que robé su tiempo de compartir en familia y privar a los niños de lo que más quieren, sus juguetes.

Gracias a la Universidad Nacional Abierta y a Distancia-UNAD por darme la oportunidad de alcanzar mis sueños, a los profesores por los conocimientos recibidos y su acompañamiento permanente en todo el proceso académico.

A la empresa UNITRANSA S.A., especialmente al Dr. José Santos Pinilla por darme la oportunidad de aplicar mis conocimientos en aras de brindarle a la organización un aporte importante para mejorar la seguridad de la información.

Germán García Ramírez

Primeramente, a Dios por brindarme muchas bendiciones al lado de mi familia y dejarme cumplir todas las metas que me he propuesto.

A mis padres Jaime Castro Zúñiga y Rosa Delia Angarita Santos, por su apoyo incondicional, sus concejos, sus valores y su sacrificio de convertirme en profesional y ahora en especialista, para salir adelante y ser una persona de bien.

A mi esposa Yaddy Forero y a mis hijos Jaime y Samuel, por entender que este sacrificio es para brindarles un mejor futuro para todos.

A mi compañero Germán García por compartir sus conocimientos y ser ese apoyo para lograr cumplir con todas las tareas propuesta de esta especialización.

A la Universidad Nacional Abierta y a Distancia-UNAD por brindarme la oportunidad de seguir avanzando en mis estudios, a los tutores por la paciencia y el conociendo impartido para que alcanzáramos la metas propuesta del pensum del curso.

Jaime Alfonso Castro Angarita

CONTENIDO

pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

ANEXOS

Pág.

INTRODUCCIÓN

La historia revela que el progreso ha sido el resultado de una serie de innovaciones tanto en la creación de nuevos productos como en la aparición y mejoramiento de las tecnologías. Un ejemplo de un producto nuevo que facilitó el desarrollo de nuevas actividades económicas es la informática, en cuanto a innovaciones en materia tecnológica para aumentar la productividad se puede citar la máquina de vapor y el trabajo en cadena.[1]

Las organizaciones para llegar y mantenerse en el mercado requieren el uso de recursos informáticos para la gestión de los procesos de la información. Las nuevas tecnologías permiten almacenar y procesar grandes cantidades de datos en dispositivos muy pequeños y a altas velocidades, las redes de datos permiten un ahorro importante de recursos y una integración entre los diferentes componentes organizacionales de las empresas.

El presente trabajo aborda el análisis de riegos de los activos más relevantes de UNITRANSA S.A., una empresa privada mediana dedicada al transporte de pasajeros. Para mitigar los problemas de seguridad de la información es indispensable la creación de un Sistema de Gestión de la Información (SGSI) que establezca los derroteros a seguir por todos y cada uno de los funcionarios del sistema de información y el personal externo autorizado para el ingreso al mismo.

Descubrir las amenazas, vulnerabilidades y riesgos a los cuales están expuestos los Activos de Información de UNITRANSA S.A., facilitará el desarrollo de estrategias que contrarresten las fallas encontradas y se logre preservar así, su activo más importante como lo es la información.

La norma ISO/IEC 27001:2013 específica los requisitos para establecer e implementar el SGSI, documentado en el contexto de los riesgos globales de negocio de la organización.[2] (ISO/IEC 27001:2013, 2013)Con base en esta norma se realizó el proceso de evaluación y gestión de riesgos de los activos de información de UNITRANSA S.A.

El dominio No. 5 de la norma ISO/IEC-27002:2013 contempla la definición de las políticas de seguridad de la información para un correcto uso de los activos de información.[3] Este documento contiene un compendio de recomendaciones que con

---

[1]Coraje, Pablo. La tecnología como factor clave del crecimiento económico [online] (febrero, 2013), disponible en Internet: http://www.pablocoraje.es/2013/02/la-tecnologia-como-factor-clave-del.html

[2] International Organization for Standardization. ISO/IEC 27001:2013 [online] (octubre, 2013), Available from Internet: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54534

[3]ISO 27002.es [online] (2012), disponible en Internet: http://iso27000.es/iso27002.html

la aplicación rigurosa de ellas se logra un alto grado de seguridad de la información en la organización.

Las amenazas no siempre afectan a todos los sistemas informáticos de la misma forma, este documento muestra una recopilación de amenazas a la seguridad de la información de UNITRANSA S.A., con el deseo de que su número no crezca demasiado. Las salvaguardas, quizás el apartado más complejo por su amplio contenido tecnológico, productos y combinaciones de ingenio con elementos básicos como políticas de seguridad, constituyen para MAGERIT lo que ellos llaman "identificación de necesidades", labor desarrollada por los responsables de los sistemas de información y los controles de eficacia y eficiencia ejecutados por el personal de auditoría de sistemas.

1. PLANTEAMIENTO DEL PROBLEMA

UNITRANSA S.A. es una empresa de servicios de tipo privado, dedicada al transporte de pasajeros en la ciudad de Bucaramanga y su área metropolitana; que ofrece un servicio a muy bajo costo y llega a los barrios más apartados. Está ubicada en la Cra. 10 No. 44-18 en esta ciudad del departamento de Santander, Colombia.

Para llegar a posicionarse en el exigente y competitivo mercado del transporte ha tenido que afrontar cambios importantes en su infraestructura tecnológica y sistematización de sus procesos. La centralización de la información, la optimización de recursos, la disminución de costos y la necesidad de compartir información entre sus diferentes dependencias y estas con otras empresas, requieren la incorporación de una infraestructura tecnológica eficiente, confiable, amigable y escalable que gestione sus métodos.

Dichos cambios han traído muchos beneficios a la empresa UNITRANSA S.A., pero de la misma manera un sinnúmero de problemas relacionados con la seguridad de la información debido en parte a la falta de una verdadera gestión de activos que permita identificar claramente cada uno de ellos, definir la importancia que representa cada activo para los procesos de la empresa, asignar un propietario del activo que vele por su seguridad y el buen uso que se haga del mismo.

Muchas vulnerabilidades en la información de una organización se dan por la carencia de una herramienta de gestión de los activos de información que administre los equipos de una manera ordenada, responsable y debidamente documentada, que permita solventar sin el mayor traumatismo los incidentes de seguridad. Pero estas herramientas no tendrían la suficiente efectividad sin el acompañamiento de una norma lo suficientemente clara que regule su aplicabilidad.

UNITRANSA S.A. debe considerar formalmente la posibilidad de implementar en su organización un Sistema de Gestión de la Seguridad de la Información (SGSI) que implemente los controles necesarios para la gestión de activos de información, complementado con la creación de una audaz Política de Seguridad de la Información (PSI) que debidamente difundida y documentada le permita a la organización adquirir unos niveles de seguridad aceptables.

1.1 FORMULACIÓN DEL PROBLEMA

¿Cómo se pueden proteger los activos de información de la empresa UNITRANSA S.A.?

2. JUSTIFICACIÓN

A través de la historia se ha demostrado que el hombre vive en permanente cambio y gracias a su afán por crear, descubrir, inventar e innovar, ha hecho la vida más cómoda. Sus creaciones han permitido aumentar la expectativa de vida, acercar los pueblos, conocer otras culturas, comercializar productos y servicios, agilizar los procesos, disminuir las emisiones de Co2, entre muchos otros; todos ellos teniendo como objetivo principal el mejoramiento de la calidad de vida. Entre los 10 descubrimientos más importantes de los últimos 50 años se destacan la computadora, el microprocesador, la fibra óptica y los teléfonos celulares; todos estos relacionados con el procesamiento de información y las comunicaciones[4].

Esto sin duda ha traído un sinnúmero de beneficios a las empresas, representados en un aumento vertiginoso en sus utilidades, su expansión y el reconocimiento de sus marcas, pero de igual manera han dejado al descubierto la existencia de vulnerabilidades que aprovechadas por los intrusos, penetran los sistemas de información, hurtan, modifican o borran los datos, ocasionando a las diferentes organizaciones grandes pérdidas económicas y de reputación.

UNITRANSA S.A. como empresa de categoría mediana y a pesar de manejar datos de criticidad media, no es ajena a la ocurrencia de incidentes de seguridad de la información, en tal sentido el Sistema de Gestión de la Seguridad de la Información (SGSI) a diseñarse mejorará ostensiblemente la seguridad de la información de la empresa, primordialmente en lo relacionado con la gestión de activos que soportan, transportan y procesan los datos con los cuales se toman las decisiones.

Para efectos del presente estudio, el proyecto está delimitado al Dominio A.5. Política de Seguridad de la Información y el Dominio A.8. Gestión de Activos, de la norma ISO/IEC 27001:2013.

De la misma forma con la aplicación de la Política de Seguridad de la Información se creará una cultura de seguridad que marcará los derroteros necesarios para salvaguardar uno de los activos más importantes de la organización, como lo son sus datos.

No menos importante es el hecho de que este documento sirva como un modelo teórico que pueda ser implementado en todo o en parte para mitigar el impacto de los ataques contra la información de la empresa.

[4]Pino, Fernando. Los 10 descubrimientos más importantes de los últimos 50 años [online], disponible en Internet: http://www.batanga.com/curiosidades/3988/los-10-descubrimientos-mas-importantes-de-los-ultimos-50-anos

3. OBJETIVOS DEL PROYECTO

3.1 OBJETIVO GENERAL

Diseñar un Sistema de Gestión de Seguridad de la Información (SGSI) bajo la norma ISO 27001 en la empresa UNITRANSA S.A. para alcanzar unos niveles óptimos de la seguridad de la información.

3.2 OBJETIVOS ESPECÍFICOS

- Plantear una técnica para gestionar el inventario de activos de información de UNITRANSA S.A. que admita incorporar, dar de baja y cambiar ubicación de los activos de información.
- Diseñar una metodología para el manejo de etiquetado de los activos de información de la organización.
- Proponer un mecanismo para concienciar a los empleados de UNITRANSA S.A. de la importancia de asumir la seguridad de la información como parte fundamental de sus funciones diarias.
- Diseñar las Políticas de Seguridad de la Información (PSI) para la empresa UNITRANSA S.A. usando la norma ISO 27001.

4. MARCO REFERENCIAL

4.1 ANTECEDENTE DE LA INVESTIGACIÓN

A partir de octubre de 1971, cuando inició operaciones la empresa UNITRANSA S.A., la organización realizaba los procesos Gestión de Desarrollo Estratégico, Gestión de Mercadeo, Gestión de Talento Humano, Gestión Financiera, Gestión Supervisión y Control de Rutas, Gestión de Estaciones de Servicio, etc. mediante la utilización de formatos en papel y libros contables adquiridos en papelerías. La información era guardada en gavetas metálicas ubicadas en cada una de las oficinas y un cuarto de archivo donde reposaba el historial de documentos, pero no se pensaba en la seguridad de la información como parte importante de la administración. Con la aparición de la computadora, el desarrollo de aplicativos de gestión de nómina, bases de datos, hojas de cálculo, la implementación de las redes de datos, la popularización de internet, correo electrónico, dispositivos móviles y redes inalámbricas, entre otros, la empresa adoptó maneras más prácticas y eficientes para el desarrollo de sus actividades cotidianas. Pero estos adelantos tecnológicos, además de los beneficios en rapidez, precisión, exactitud, eficiencia y permitir la toma de decisiones de una manera más acertada, trae consigo un sin número de inconvenientes que bien vale la pena analizar. Uno de estos problemas es la inseguridad de la información, que ha venido creciendo en los últimos años y ha ocasionado grandes pérdidas económicas y de acreditación a muchas empresas. Por tal razón los directivos de muchas organizaciones han incluido la seguridad de la información como parte esencial de la gestión administrativa.

Varias empresas de diferente índole, han adelantado estudios para la implementación de sistemas de gestión de riesgos de sus activos de información más relevantes:

- Implementación de los controles asignados al dominio “Gestión de Activos”, bajo los lineamientos establecidos por la norma ISO/27001 Anexo A, para las empresas municipales de Cali, EMCALI E.I.C.E-ESP[5]. Este proyecto se realizó para coadyuvar en el cumplimiento del domino Gestión de Activos de la Norma ISO/27001 Anexo A, para lo cual se plantean las estrategias que permiten minimizar los riesgos sobre los activos de información de la organización.
- Análisis de riesgos y recomendaciones de seguridad de la información al área de información y tecnología del hospital Susana López de Valencia de la ciudad de Popayán[6]. El propósito de este trabajo es ayudar en el

[5] Repositorio Digital Universidad Autónoma de Occidente [online], disponible Iinternet: http://bdigital.uao.edu.co. Recuperado el 27 de mayo de 2016.
[6] Repositorio Institucional UNAD [online], disponible en iInternet: http://hdl.handle.net/10596/2668. Recuperado el 25 de mayo de 2016.

cumplimiento del deber institucional del Hospital Susana López de reforzar la seguridad de sus recursos y sus activos informáticos implementando correctamente mecanismos de seguridad en las redes de computadores y gestionando todo lo relacionado con el dominio “Gestión de Activos”, de la norma ISO/IEC 27001, en busca de evitar el mal funcionamiento de sus recursos y disminución de la eficiencia de los mismos, además de pérdidas sustanciales de dinero, credibilidad de la institución y tiempo de ejecución de sus procesos.

- Implementación de un Sistema de Gestión de la Seguridad Informática en la Confederación de Cámaras de comercio - CONFECÁMARAS[7]. Este proyecto se realizó como apoyo en la consolidación de documentos básicos para la ejecución de un SGSI en la Confederación Colombiana de Cámaras (Confecámaras).
- Implementación de un Sistema de Gestión de Seguridad de la Información para una empresa de consultoría y auditoría, aplicando la norma ISO/IEC 27001[8]. Este documento reúne la información necesaria para la implementación de un Sistema de Gestión de Seguridad de la Información, basado en la norma IO 27001:2005, para asegurar la protección de los activos de información y otorgar confianza a los clientes de A&CGroup S.A. La norma adopta un enfoque por procesos para establecer, implantar, operar, supervisar, revisar, mantener y mejorar un SGSI.

4.2 MARCO CONTEXTUAL

4.2.1 Reseña histórica de UNITRANSAS.A. Al darle organización estatutaria a la empresa Unión Santandereana de Transportes Urbanos "UNITRANSA S.A.", no puede pasar inadvertido para ella el reconocimiento que se le debe a los señores Gerardo Ribero, Luis Eduardo Sánchez Martínez, José Miguel Jiménez Pinzón, Hernando Arciniegas Lamos, José del Carmen Vega Galvis, Luis Francisco Villamizar y Tiro Antonio Roa Díaz, quienes firmaron la Escritura Pública No. 3370 de la Notaría Tercera (3ª.) del círculo de Bucaramanga como también los socios fundadores: José Antonio Báez Quintero, Horacio Gómez, Ramiro Quintero Chaparro, Rosaura Joya, Florentino Cristo Aceros, Juan García, Jorge Rojas Martínez, Hernando David Ordoñez, Jesús María Ramírez Bernal, Efraín Sandoval, Héctor Morales Pinzón, Hernando Melgarejo Pinto, Filemón Chaparro Gómez, Hipólito Guarín Becerra, Darío Reyes Espitia, Gratiniano Jiménez y Vicente Reyes, entre otros quienes fueron los pioneros de la actividad que transformó aquellas

[7]Repositorio Institucional UNAD [online], disponible en Internet: http://hdl.handle.net/10596/3653. Recuperado el 27 de mayo de 2016

[8]Repositorio de Space [online], disponible en Internet: http://www.dspace.espol.edu.ec/xmlui/bitstream/handle/123456789/31114/Resumen%20de%20tesis%20DTola%2c%20director%20de%20tesis%20Msig.%20Lenin%20Freire%20C.%2019%20mayo%202015.pdf?sequence=1&isAllowed=y, Recuperado el 27 de mayo de 2016.

empresas: Transportes Urbanos "LA PEDREGOSA", Transportes Urbanos "PALONEGRO" y Transportes "PARQUE ROMERO" en un ente pujante como es "UNITRANSA S.A.", que debió estar acorde con la evolución socio cultural de la ciudad de Bucaramanga, para prestar los servicios públicos que demandaba en aquellos momentos para el despegue hacia un desarrollo integral. Podemos decir que ese 1º de octubre de 1971 marcó un hito histórico, no solamente para nuestra empresa, sino para los destinos de la ciudad y sus áreas adyacentes; y con ello el reflejo de poderío espiritual por parte de los luchadores del volante que con su propio esfuerzo e incansable tesón económico la presentaron diáfana para hacerla brillar y con la pujanza que tiene, constituirse en el medio de transporte masivo de la extensa y amplia zona conocida como "Metropolitana de Bucaramanga".

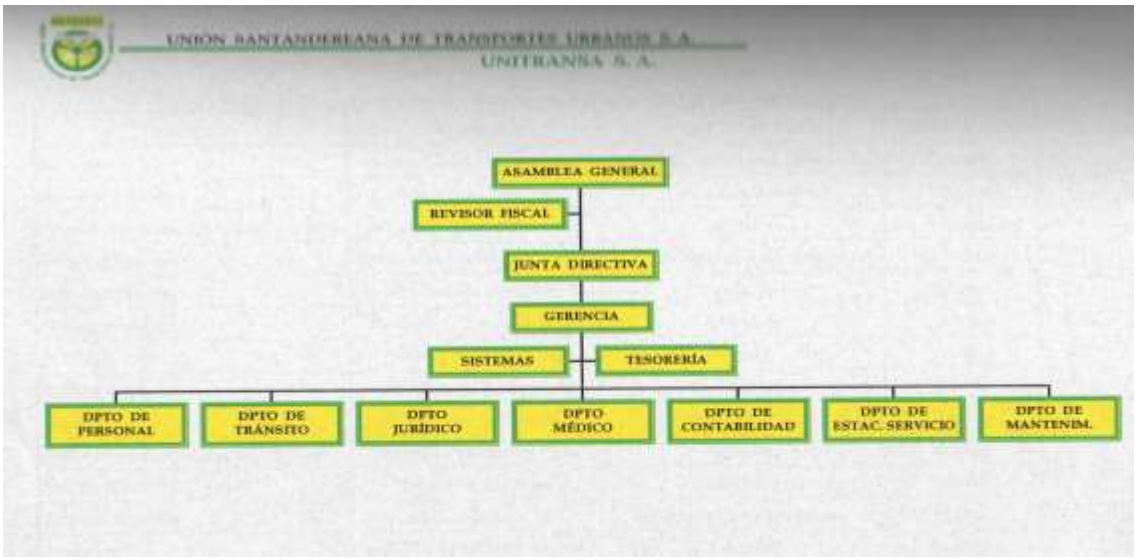
4.2.2 Misión. Organizar y prestar el servicio de transporte terrestre automotor de pasajeros en todos los radios de acción y modalidades, buscando la mejor eficiencia en la prestación de este servicio.[9]

4.2.3 Visión. Llegar a ser la mejor empresa de transporte en el Oriente Colombiana, cumpliendo así el objetivo, de brindar a la comunidad, un servicio moderno, cómodo, seguro, económico y eficaz.[10]

4.2.4 Organigrama de UNITRANSAS.A. La organización cuenta con 283 funcionarios, entre los que se cuentan directivos, accionistas, gerente, secretarios, ingeniero, conductores, mecánicos, operarios de estaciones de servicio, personal de seguridad y oficios varios, entre otros. Doce empleados interactúan con el sistema y poseen cuenta de usuario y contraseña para autenticar y validar su ingreso a los recursos y la información de la empresa. La Figura 3 muestra el organigrama de la compañía.

[9] Obtenido de la Oficina de Jefatura de Personal UNITRANSA S.A.
[10] Ibíd.

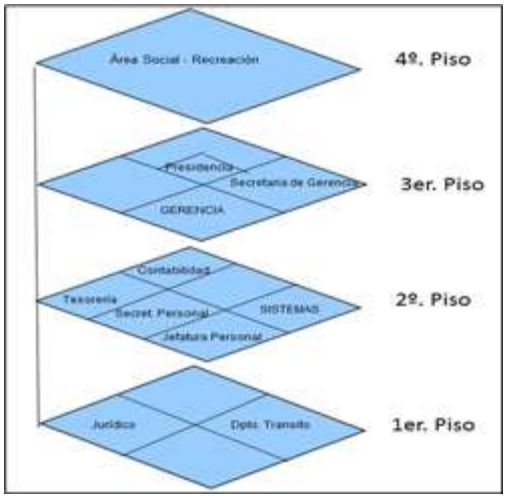
Figura 1. Organigrama de UNITRANSA S.A.



Fuente: oficina Secretaría de Gerencia UNITRANSA S.A.

4.2.5 Distribución de oficinas UNITRANSA S.A. Las instalaciones de UNITRANSA están ubicadas en la Cra. 10 No. 44-18 en la ciudad de Bucaramanga departamento de Santander, en un edificio de cuatro plantas, exclusivo de la empresa. La Figura 2 muestra la distribución de las oficinas por piso.

Figura 2. . Distribución de oficinas



Fuente: oficina Secretaria de Gerencia UNITRANSA S.A.

4.3 MARCO CONCEPTUAL

4.3.1 Seguridad informática. Definiciones de Seguridad Informática hay muchas, pero para obtener un contexto más generalizado podría aseverarse que la Seguridad Informática abarca todos los componentes, características y condiciones que un sistema de procesamiento, almacenamiento y transporte de datos requiere para que esté seguro de daños o riesgos, sean estos provocados por personas, de forma voluntaria o involuntaria o de desastres naturales. En este orden de ideas, proteger la información demanda de componentes software, hardware, documentos estándar y la ejecución de metodologías existentes que admitan la aplicabilidad de normas internacionales certificables (ISO 27001).[11]

4.3.2 Pilares de la seguridad informática. Son los soportes o bases sobre los que se fundamenta la seguridad de la información para su preservación, transporte, edición y/o eliminación. Estos son:

- ✓ **Confidencialidad**. Se entiende como la no divulgación de la información a personas o sistemas no autorizados, dicho de otro modo, es el acceso a la información solo a aquellas personas que posean las credenciales para hacerlo.

- ✓ **Integridad**. Propiedad que garantiza que los datos se preserven libres de modificaciones no autorizadas, es decir, mantienen la información tal cual fue generada y guardada. Esta propiedad es muy importante a la hora de realizar operaciones bancarias por Internet. Los bancos deben garantizar que ningún intruso capture y modifique los datos transmitidos.[12]

- ✓ **Disponibilidad.** Cualidad de la información de estar dispuesta a quienes deben acceder a ella, ya sean personas, aplicaciones o procesos en el momento en que lo requieran. Un clásico ejemplo de ataque a esta cualidad de la información es la desconexión o corte de un cable de comunicación del centro de cómputo de una empresa, denegación del servicio de sitios web o aplicativos por la acción de virus informáticos, código malicioso o desbordamiento de buffer, entre otros.

- ✓ **Autenticidad.** Legitimidad y certeza de que una persona, servicio o elemento es quien dice ser. Esta propiedad de la seguridad informática es la que permite identificar a quien genera la información, es decir, al recibir datos de

---

[11] DATATECA UNAD. SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACIÓN SGSI (2016) [online], disponible en Internet: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/11_leccin_1_pilares_de_la_seguridad_informtica.html

[12] ISACA. La integridad de los datos: el aspecto más relegado de la seguridad de la información (2016) [online], disponible en Internet: http://www.isaca.org/Journal/archives/2011/Volume-6/Pages/Data-Integrity-Information-Securitys-Poor-Relation-spanish.aspx?

un emisor tener la certeza de que ese emisor fue quien envió la información y no de un tercero que se haya hecho pasar por él; esto es lo que se conoce como “no repudio” (ISO-7498-2).[13] Una forma de validar la autenticidad del emisor es el uso de firmas digitales.

- **Firma digital**. Esquema matemático utilizado para demostrar la autenticidad de un mensaje digital o de un documento electrónico. Da al destinatario la certeza de que el mensaje fue creado por el remitente y no sufrió alteración alguna en su transferencia.[14]

4.3.3 Amenazas. Los Activos de Información de una organización y la información misma están expuestos a eventos o acciones capaces de causar alteraciones, hurto o borrado de datos; para ello aprovechan las vulnerabilidades existentes en los sistemas de información. Básicamente las amenazas se pueden agrupar en dos tipos:

- ✓ **Intencionales**: ocurren cuando deliberadamente se quiere ocasionar daño, ejemplo la propagación de código malicioso, la ingeniería social y el hurto de información por medio del trashing.
- ✓ **No intencionales:** suceden cuando por acciones u omisiones que, sin pretender explotar alguna vulnerabilidad ponen en riesgo los activos de información y los datos.

4.3.3.1 Fuentes de amenaza. Existen varias categorías de amenazas clasificadas según su origen, de esta forma se dividen en cinco tipos: amenazas humanas, de hardware, de software, de red y desastres naturales[15].

4.3.3.2 Vulnerabilidades. Constituyen el principal elemento de un sistema de información que puede ser aprovechado por un atacante para afectar la integridad, la disponibilidad y la confiabilidad de la información. De igual manera pueden causar daños por sí mismos sin tratarse necesariamente de un ataque intencionado.

4.3.3.3 Tipos de vulnerabilidades. Las vulnerabilidades son el resultado de errores de programación (bugs), fallos en el diseño del sistema, incluso las limitaciones tecnológicas pueden ser aprovechadas por los atacantes. Para esta investigación, se clasifican las vulnerabilidades en seis tipos: Físicas, naturales, de hardware, de software, de red y de factor humano.

4.3.4 Métodos de ataque más explotados. El primer paso que una persona realiza al planear un ataque informático es hallar las vulnerabilidades que el sistema

---

[13] WIKIPEDIA. Seguridad de la información (septiembre de 2016) [online]; disponible en Internet: https://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n#Autenticaci.C3.B3n_o_autentificaci.C3.B3n

[14] Firma Digital. Cr.¿Qué es la firma digital? (2016) [online], disponible en Internet: http://www.firma-di gital.cr/que_es/

[15] Tutorial de Seguridad Informática, obtenido de: http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap2.html

informático objetivo posee. Detectadas las vulnerabilidades, la información está en inminente riesgo, solo resta efectuar el ataque aprovechando el método que ofrezca la mayor probabilidad de éxito. Entre las muchas metodologías existentes se destacan:

- ✓ **Factor Insiders**. Los últimos estudios han demostrado y evidenciado que la mayoría de las violaciones de seguridad son efectuadas por el personal de la empresa, es decir, por los mismos empleados. Logrando el atacante una mayor efectividad, pues conoce el sistema, sus fortalezas y debilidades.

- ✓ **Ingeniería Social.** Es una habilidad o técnica que usan los atacantes mediante el engaño, explorando las debilidades del personal de la empresa. Con esta metodología, los atacantes la usan como herramienta de penetración a un sistema y es aplicable en cualquier ámbito, en lo que a informática se refiere. Que consiste en adquirir información sensible y/o confidencial del personal cercano al sistema de información de la empresa.
- ✓ **Malware (malicious software)**. Conocido como software malicioso, es un software desarrollado con la única intención de penetrar un sistema de información o una computadora, sin autorización y efectuar daños. Se considera malware debido a los efectos nocivos que provoca en el computador. Pertenecen a esta categoría los virus, gusanos, troyanos, la mayor parte de los rootkits, scareware, spyware, adware intrusivo, crimeware, entre otros.[16]

4.3.5 Dominio A.5 Políticas de Seguridad de la Información. Comprende el documento que enmarca las tareas que debe realizar cada funcionario para minimizar los riesgos a los cuales está expuesta la información, ayudando a la disminución de costos operativos y financieros, además de instaurar la cultura de seguridad y garantizar el cumplimiento de las disposiciones legales vigentes, sirviendo de apoyo a la dirección de la organización en la toma de decisiones disciplinarias y legales en el manejo de incidentes de seguridad de la información. Estas deben cumplir los siguientes requisitos:

- ✓ Estar documentadas.
- ✓ Ser conocidas por todo el personal de la empresa, al igual que los proveedores, practicantes, socios y directivos.
- ✓ Ser revisadas periódicamente o cuando ocurran cambios importantes que puedan afectar la gestión de la seguridad de la información.
- ✓ Documentar cualquier modificación producto las revisiones realizadas.
- ✓ Ser aprobadas por la dirección de la organización.

[16] WIKIPEDIA. Malware (4, octubre, 2016) [online], disponible en: https://es.wikipedia.org/wiki/Malware

- ✓ Expresar claramente el compromiso de la dirección con la creación, ejecución, puesta en marcha y aplicación de las políticas de seguridad de la información.[17]

4.3.6 Normativas de Seguridad. En la actualidad es posible encontrar diferentes normas de seguridad que las empresas implementan para proteger su información. Estas normativas están diseñadas para un mismo objetivo, brindarle a la estructura organizacional una seguridad de los datos, dando como resultado unos lineamientos para la implementación del Sistema de Gestión de la Seguridad de la Información.[18] Gestionar la Seguridad de la Información de una organización conlleva:

- ✓ Establecer los objetivos, estrategias y políticas de Seguridad de la Información.
- ✓ Definir los requerimientos de Seguridad de la Información.
- ✓ Determinar las amenazas y las vulnerabilidades a las que se exponen los Activos de Información de la empresa.
- ✓ Analizar y concretar los riesgos de seguridad de la información.
- ✓ Establecer las salvaguardas más idóneas para cada amenaza.
- ✓ Monitorear la ejecución y funcionamiento de las salvaguardas implementadas.
- ✓ Perseverar en la concienciación del personal en materia de Seguridad de la Información.
- ✓ Detectar incidentes de seguridad y gestionarlos[19].

4.3.7 Factores que afectan la Seguridad de la Información. Actualmente el proceso de Gestión de la Seguridad de la Información en una organización conlleva un alto grado de complejidad, básicamente por el aumento de los ataques informáticos gracias a factores como:

- ✓ ***Motivación económica***. Estimulan la profesionalización de los atacantes, lo que ha permitido la creación de verdaderas empresas dedicadas al aprovechamiento de las debilidades y vulnerabilidades de los sistemas de información y la utilización de la ingeniería social para obtener beneficios financieros.
- ✓ ***Personal propio***. Un número importante de incidentes de seguridad de la información ocurren por la acción u omisión de los usuarios del sistema,

[17]CAMELO, Leonardo. SO 27001 e ISO 27002: Dominio 5 - Política de Seguridad [2, marzo, 2010) [online]. Disponible en Internet: http://seguridadinformacioncolombia.blogspot.com.co/2010/03/iso-27001-e-iso-27002-politica-de_02.html

[18] PREZI. ISO 27005 estándar para la gestión de riesgos de seguridad [online]; Disponible en Internet: https://prezi.com/ackjjdccd2sb/iso-27005/

[19] Rodríguez Mesa, D. Alejandro. Resumen analítico investigativo sobre ISO 27005 [online]; disponible en Internet: http://es.slideshare.net/ffffffffe23/dumar-resumen-analitico-investigativo-sobre-el-iso-27005

movidos por diferentes razones como la sed de venganza, desconocimiento de los riesgos, negligencia, entre otros. Cualquier mecanismo de seguridad resulta ineficiente cuando las personas que lo administran no lo hacen con responsabilidad.

- ✓ ***Objetivos específicos***. Es común encontrar kits de ataques informáticos sofisticados dirigidos a personas con pocos conocimientos tecnológicos, lo que hace que estos aumenten dramáticamente.
- ✓ ***Debilidades no tecnológicas***. Un aumento en la pérdida de información obedece a factores ajenos a la tecnología como lo es el robo o pérdida de soportes de almacenamiento de datos y el abuso de los privilegios de acceso otorgados a los usuarios del sistema.
- ✓ ***Ataques del día cero***. Es una modalidad de ataque informático que aprovecha una vulnerabilidad no conocida por los usuarios y los desarrolladores de aplicativos, por lo que en el momento del ataque no existe parche o actualización que la corrija. Hay algunos mecanismos de protección contra los ataques del Día Cero, como mantener los sistemas operativos y aplicaciones actualizados, disponer de software antivirus y firewall potentes y debidamente actualizados, eliminar el software innecesario y una buena política de seguridad.

4.3.8 Políticas o normativas. La seguridad de la información requiere adoptar un conjunto de reglas, estatutos legales y políticas institucionales que no dejen nada al azar y que integren el esfuerzo y conocimiento humano con las técnicas de mecanismos automatizados para aplicar los mejores controles y procedimientos que sistematicen la forma en que una organización prevenga, proteja y manejo los riesgos de seguridad de sus activos de información en diversas circunstancias. La Organización Internacional de Normalización (ISO) emitió las siguientes normas que regulan la gestión de la seguridad de la información en una empresa:

4.3.9 Norma ISO/IEC 27000. Fue publicada en mayo de 2009 y la tercera edición salió el 14 de enero de 2014. Esta serie de normas contribuye con los fundamentos para la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI), proporcionando los pasos para instaurarlo, monitorearlo, mantenerlo y mejorarlo. La última edición no incluye el ciclo de mejora continua PHVA (del inglés Plan-Do-Check-Act) para no convertirlo en estándar de referencia, además contiene los términos y las definiciones usadas en toda la serie 27000, ya que cualquier estándar necesita un vocabulario propio y definido con claridad para evitar interpretaciones diferentes.

4.3.10 Norma ISO 27001. Esta norma expedida por la Organización Internacional de Normalización (ISO), describe los requisitos para establecer, gestionar, documentar y evaluar un Sistema de Gestión de la Seguridad de la Información (SGSI) en una organización de cualquier orden. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2 (anulada).ISO 27001 contiene en su Anexo A los objetivos de control y controles propios de la ISO

27002, esto con el fin de que las diferentes organizaciones que implementen un SGSI puedan seleccionar los más adecuados a sus necesidades, argumentando explícitamente las razones de la no implementación de los restantes.[20] su nombre completo es ISO/IEC 27001:2013.[21.]

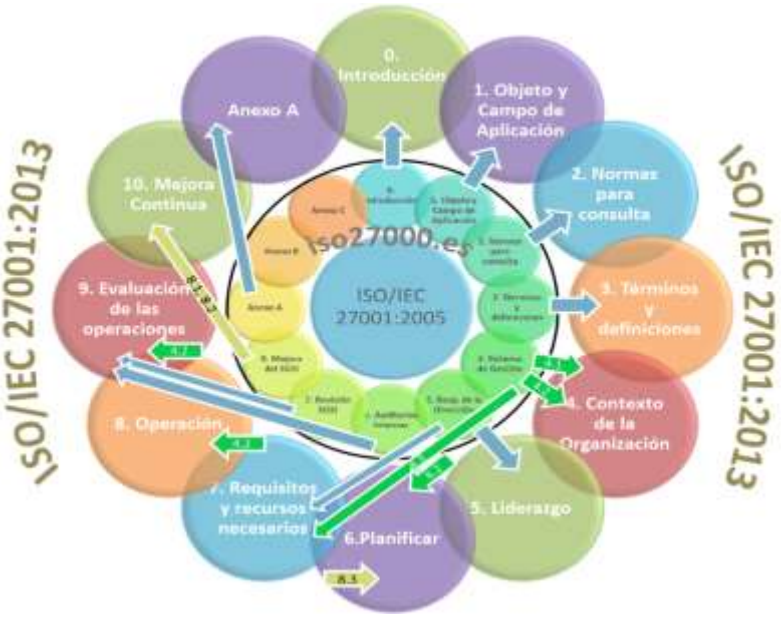
- ✓ **Objetivo de la ISO 27001**. El objetivo general de esta norma es proteger la confidencialidad, la integridad y la disponibilidad de la información de una organización. Para lograrlo, descubre las dificultades que podrían estar afectando la información (riesgos) y posteriormente diseña los mecanismos necesarios para impedir la materialización de las amenazas o la mitigación del impacto. La filosofía de la ISO 27001 se fundamenta en la gestión de riesgos, es decir busca los riesgos y luego los trata sistemáticamente.

- ✓ **Importancia de ISO 27001 para la empresa**. La culminación de esta norma trae las siguientes ventajas para la organización:
  - **Cumplir con el ordenamiento legal**. La legislación colombiana posee ordenanzas relacionadas con el manejo de la información y la norma ISO 27001 permite resolver la mayoría de ellas.
  - **Lograr una ventaja comercial**. Obteniendo una certificación en ISO 27001 la empresa toma la delantera ante aquellas que no la obtienen.
  - **Disminución de costos**. Evitando la ocurrencia de incidentes de seguridad de la información la empresa ahorra dinero y la inversión en ISO 27001 es de menor costo en la mayoría de casos.
  - **Mejorar la organización de sus procesos**. Cuando una empresa crece exponencialmente se olvida precisar los procesos y procedimientos, dejando de lado la asignación de responsabilidades en muchos aspectos. Con ISO 27001 se ayuda a solventar esta situación ya que se exhorta a documentar todos los procesos.

[20] 27001 Academy. ¿Qué es norma ISO 27001? [online], disponible en Internet: http://advisera.com/27001academy/es/que-es-iso-27001/

[21] Enríquez Espinosa, R. P. Implementación de los controles asignados al dominio “gestión de activos”, bajo los lineamientos establecidos por la norma iso/27001 Anexo A, para las empresas municipales de Cali, EMCALI E.I.C.E-ESP (2013) [online], disponible en Internet: http://bdigital.uao.edu.co/handle/10614/53274 (Enriquez Espinosa, 2013)

Figura 3. Correlación ISO/IEC 27001



Fuente: ISO 27000.ES (2016). El portal de ISO 27001en español

4.3.11 Norma ISO 27002. Esta norma suministra recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a los responsables de implementar, administrar o auditar un Sistema de Gestión de la Seguridad de la Información (SGSI)[22]. El objetivo que persigue esta norma es el correcto uso de los activos de información de la organización. La norma ISO 27002 contiene:

- ✓ Políticas de Seguridad.
- ✓ Organización de la Seguridad de la Información.
- ✓ Seguridad de los Recursos Humanos.
- ✓ Gestión de Activos.
- ✓ Control de Accesos.
- ✓ Criptografía.
- ✓ Seguridad Física y Ambiental.
- ✓ Seguridad de las Operaciones.
- ✓ Seguridad de las Comunicaciones.
- ✓ Adquisición de sistemas, desarrollo y mantenimiento.
- ✓ Relaciones con los proveedores.
- ✓ Gestión de Incidentes que afecten la Seguridad de la Información.
- ✓ Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio.
- ✓ Conformidad.

[22] WIKIPEDIA. ISO/IEC 27002 [18, diciembre, 2015) [online], disponible en Internet: https://es.wikipedia.org/wiki/ISO/IEC_27002

4.3.12 Dominio A.8 Gestión de Activos. El Sistema de Gestión de la Seguridad de la Información (SGSI) a implementarse en cualquier organización incluye el dominio Gestión de Activos del anexo A de la norma ISO/IEC 27001, que contiene dos objetivos de control y cinco controles.

- ✓ **Responsabilidad sobre los activos**. El objetivo que se busca es proteger adecuadamente los activos informáticos de la organización, para ello todos los activos deben estar claramente identificados y tener un propietario asignado. Este objetivo de control contiene los siguientes controles:
  - **Inventario de activos**. Es responsabilidad de la empresa documentar pormenorizadamente el inventario de los activos de información, incluyendo su ubicación, tipo de activo, importancia, valor comercial, respaldo de la información y licencia. La Tabla 1 muestra los tipos de Activos de Información y su descripción según la metodología MAGERIT.
  - **Propiedad de los activos**. Corresponde a la parte directiva asignar a cada activo su propietario. El propietario es la persona asignada por la dirección como encargada del control de producción, desarrollo, mantenimiento y uso responsable del activo de información
  - **Uso aceptable de los activos**. La seguridad de la información se inicia con la creación de una política formal, documentada y conocida por todos, que contenga los controles más apropiados que garanticen que el uso de los recursos del sistema se hace de una forma responsable, adecuada y sin poner en riesgo la integridad, la disponibilidad, la confidencialidad y la trazabilidad de la información de la empresa.

Tabla 1. Tipos de Activos.

Tipos de Activos de Información	Descripción
Servicios	Procesos de negocio de la organización, ya sea a nivel externo o interno. Ejemplo la gestión de nómina.
Datos/información	Bases de datos, archivos de data, documentación (manuales de usuario, contratos, normativas, material de capacitaciones, rastros de auditorías, plan de continuidad del negocio, etc.)

Tabla 1. (Continuación)

Tipos de Activos de Información	Descripción
Aplicaciones de Software	Sistemas de información, herramientas de desarrollo, aplicativos desarrollados y en desarrollo, sistemas operativos, aplicaciones de servidores etc.
Equipos informáticos	Equipos de oficina (PC, portátiles, servidores, dispositivos móviles, etc.)
Personal	Principal activo, incluye personal interno, subcontratado, clientes, etc.
Redes de comunicaciones	Dan soporte a la organización para el movimiento de la información. Incluye redes propias o subcontratadas.
Soportes de información	Soportes físicos que permiten el almacenamiento de la información durante largos periodos de tiempo.
Equipamiento auxiliar	Dan soporte a los sistemas de información y no pertenecen a ningún otro grupo. Ejemplo equipos de destrucción de documentos, equipos de climatización, UPS, etc.
Instalaciones	Lugares donde se alojan los sistemas de información como oficinas, edificios o vehículos.
Intangibles	Imagen y reputación de la empresa.

Fuente: MAGERIT libro I Método

- ✓ **Clasificación de la información.** Es importante determinar el grado de criticidad de la información y de esta manera establecer el nivel de protección requerido para cada uno de los tipos de información clasificados. Se necesita definir un esquema de clasificación de la información para de esta manera especificar el grupo de controles necesarios y comunicar esa decisión a la dirección para la toma de medidas pertinentes. Este objetivo de control posee dos controles.[23]

    - **Directrices de clasificación.** Al momento de clasificar la información de la organización debe tenerse en cuenta su sensibilidad, la

[23]Camelo, Leonardo. ISO 27001 e ISO 27002: Dominio 7 - Gestión de Activos (5, marzo, 2010) [online], disponible en Internet: http://seguridadinformacioncolombia.blogspot.com.co/search/label/Dominio%2007

importancia para los procesos de la empresa, disposiciones legales y su valor comercial.[24]

- **Etiquetado y manipulado de la información**. El objetivo que busca este control es desplegar y establecer un conjunto de rutinas para el etiquetado de la información, siguiendo el esquema clasificatorio de la información que la empresa haya adoptado.

4.3.13 Elementos de un análisis de riesgos. El riesgo tecnológico implica:

- La probabilidad de pérdidas de datos ante fallas de los sistemas de información.
- La probabilidad de fraudes internos y externos a través de los sistemas de información.
- El riesgo legal y el riesgo de pérdida de reputación por fallas en la seguridad y por la no disponibilidad de los sistemas de información[25].

Un análisis de riesgos involucra los siguientes elementos:

- Activos
- Valor de activo (impacto potencial)
- Amenazas
- Vulnerabilidades
- Riesgos
- Requisitos de seguridad
- Salvaguardas

4.3.14 Metodologías, normas y estándares para el análisis de riesgos.

¿Qué es el análisis de riesgos informáticos? Es el proceso por medio del cual se descubren las vulnerabilidades y amenazas a las que están expuestos los activos de información de una organización, de igual manera se analiza la probabilidad de ocurrencia de un incidente de seguridad y el impacto causado en caso de materializarse una amenaza. Con esta información es preciso determinar los controles más idóneos para evitar el riesgo, transferirlo, disminuirlo o aceptarlo.[26]

[24] iso27002.es - El Anexo de ISO 27001 en español. Disponible en Internet: https://iso27002.wiki.zoho.com/7-2-Clasificación-de-la-Información.html

[25] ISACA. Metodologías y Normas para el Análisis de Riesgos: ¿Cual debo aplicar? [online]. Disponible en Internet: http://www.isaca.org/chapters7/Monterrey/Events/Documents/20100302%20Metodolog%C3%ADas%20de%20Riesgos%20TI.pdf.

[26] WIKIPEDIA. Análisis de riesgo informático (22, octubre, 2015) [online]. Disponible en Internet: https://es.wikipedia.org/wiki/An%C3%A1lisis_de_riesgo_inform%C3%A1tico

Algunas de las metodologías de gestión de riesgos informáticos más utilizadas son:

- Octave
- MAGERIT
- ISO 27005i
- Risk IT de ISACA
- Mehari
- Citicus One
- CRAMM
- NIST SP 800-39
- NIST SP 800-30
- AS/NZS
- ISO TR 13335

4.3.15 Metodología de análisis y gestión de riesgos de los sistemas de información MAGERIT. Creada por el Consejo Superior de Administración Electrónica de España, teniendo como objetivo la búsqueda de los riesgos a los que están expuestos los Sistemas de Información y de igual manera sugerir las medidas más adecuadas a tomar para mitigar dichos riesgos. Se considera la gestión de los riesgos como la piedra angular en las guías de buen gobierno. MAGERIT básicamente pretende los siguientes objetivos:

- ✓ Crear conciencia de la existencia de riesgos y la necesidad de gestionarlos por parte de los responsables de las diferentes organizaciones de información.
- ✓ Dar a conocer un método ordenado y seguro para la gestión de los riesgos derivados del uso de las TIC.
- ✓ Mantener los riesgos controlados gracias a los métodos de descubrimiento y planificación ofrecidos por MAGERIT.
- ✓ Preparar a las organizaciones para procesos de evaluación, auditoría, certificación o acreditación[27].

4.3.16 Metodología PHVA (Planear, Hacer, Verificar, Actuar).

- ✓ **Planear**. En la etapa de planeación se definirá el alcance del sistema dentro de la organización, así como las políticas y lineamientos sobre los que se desarrollará. Se presentan herramientas para la identificación, análisis y evaluación de riesgos, según el impacto de cada uno y el tipo de información

[27] Consejo Superior de Administración Electrónica. MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de información [online]. Disponible en Internet: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Vf9ehBHlvX4

que se afectaría, de igual forma es objetivo de esta etapa definir la forma de tratamiento de los riesgos identificados.

- ✓ **Hacer**. Con esta implementación de la metodología del PHVA, el desarrollo del paso HACER, inicialmente se debe definir el plan de tratamiento de los riesgos, la manera de gestionar estos riesgos y la selección y aplicación de los controles para mitigarlos. Cuando este implementado el plan de tratamiento y los controles, se debe alcanzar los objetivos de control que se identificaron en el "planear". Para el desarrollo de este punto es necesario tener como referencia la norma ISO 27001:2013 la cual establece las directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en la organización. Como segundo paso se debe empezar con una toma de conciencia y formación de todo el personal de la organización en lo relativo a la seguridad de la información. Si este paso no se lleva a cabo el SGSI no va tener ningún sentido y no va generar los beneficios de la ejecución, para lograr esto se sugiere desarrollar el marco normativo necesario, las normas, los manuales, los procedimientos e instrucciones que permitan gestionar las operaciones del SGSI y los recursos asignados, además se recomienda implementar procedimientos y controles de detección y respuesta a incidentes de seguridad que van a evaluar la efectividad de los controles en funcionamiento.

  Teniendo en cuenta lo anterior el HACER contempla:

  - Precisar el plan de tratamiento de riesgos
  - Implantar el plan de tratamientos de riesgos
  - Establecer los controles
  - Formar y concientizar los usuarios del sistema
  - Poner en marcha el SGSI.

- ✓ **Verificar.** Una vez que está en marcha el SGSI es fundamental hacer un seguimiento de cómo funciona y cómo va evolucionando el sistema. En primer lugar, para corregir las posibles desviaciones sobre lo planificado y previsto y, en segundo lugar, aunque igual de importante, detectar oportunidades de mejora del sistema, ya que en últimas el propósito de implantar el SGSI es siempre la mejora continua, hacer cada vez más con los limitados recursos disponibles.
- ✓ **Actuar**. La implantación del SGSI es un proceso dinámico. Si el proceso llegó a esta etapa, debe estar claro que la misión es situar la seguridad de la información al mismo nivel que cualquier otro objetivo de negocio, y como tal, debe ser optimizado continuamente. Esta etapa corresponde al Capítulo 8 de la ISO 27002. Es en esta fase cuando deberemos establecer las medidas

correctivas fruto de las revisiones efectuadas, y mejorar así el rendimiento del sistema de gestión de la seguridad.

Figura 4. Ciclo de Mejora Continua PHVA

Fuente: https://thriveiberoamerica.org/tag/estandares/

4.4 MARCO TEORICO

4.4.1 Sistema de Gestión de la Seguridad de la información. Las empresas de trasporte de pasajeros, al igual que cualquier organización, requieren de un SGSI como una fuente importante de ayuda en las políticas y procesos propios de una organización porque sistematiza todos sus métodos, asigna responsabilidades y monitorea permanentemente su desempeño, efectuando los ajustes necesarios que la tecnología y las personas lo requieran. En este orden de ideas, un SGSI Comprende una serie de procesos sistemáticos, documentados y ampliamente conocidos por toda la organización que tienen como objetivo principal preservar la confidencialidad, integridad y disponibilidad de la información, incluyendo todos los

sistemas comprometidos en su tratamiento dentro de la empresa.[28] El SGSI es el principal concepto sobre el que se crea la norma ISO/IEC 27001.

De lo anterior, se deduce que el diseño de un SGSI requiere garantizar que los riesgos de la seguridad de la información sean descubiertos, conocidos por todos, gestionados y mitigado su impacto en el evento de la materialización de cualquier incidente de seguridad, sin desconocer el dinamismo en que mueve la tecnología y las modalidades de ataques informáticos. A partir de este enfoque, se desarrolló el trabajo de "Diseñar de un Sistema de Gestión de la Seguridad de la Información (SGSI) a la empresa UNITRANSA S.A. ubicada en la ciudad de Bucaramanga". Este sistema se basa en la norma ISO/IEC 27001 y utiliza el ciclo de mejora continua PDCA, comúnmente utilizado en los sistemas de gestión de calidad.

- Planear (Plan): en esta etapa se diseña el SGSI a partir de una exhaustiva evaluación de los riesgos de seguridad de los activos de información y se definen los controles adecuados para mitigar su impacto.
- Hacer (Do): esta etapa implica la puesta en marcha del SGSI, implementar los controles definidos en la etapa anterior.
- Verificar (Check): en esta fase se inspecciona y se evalúa el desempeño del SGSI.
- Actuar (Act): en esta etapa se efectúan las mejoras necesarias para hacer el SGSI más eficiente.

4.4.2 Análisis y gestión de riesgos.

Cuando una empresa como UNITRANSA S.A. tiene la capacidad de reconocer las amenazas a las que están expuestos sus Activos de Información y la información misma, se considera que asume el reto de diseñar un SGSI que involucra el análisis de las amenazas y vulnerabilidades de sus Activos de Información, gestión de incidentes y aplicación de salvaguardas para lograr niveles de seguridad aceptables por la empresa sin que se vea afectada la continuidad del negocio [29].

En la actualidad muchas organizaciones utilizan los sistemas tecnológicos para desarrollar sus procesos en las diferentes áreas, tales como talento humano, administración, finanzas, TI, producción, etcétera, e interactuar entre ellas. Esta sistematización de procesos trae consigo una serie de riesgos de seguridad para la

[28] ¿Qué es SGSI? [25, julio, 2015] [online]. Disponible en Internet: http://www.pmg-ssi.com/2015/07/que-es-sgsi/
[29] WIKIPEDIA. Análisis de Riesgo Informático [online]. Disponible en Internet: https://es.wikipedia.org/wiki/An%C3%A1lisis_de_riesgo_inform%C3%A1tico

información que deben ser considerados en el contexto general del negocio y asumir su gestión con la mayor diligencia.

El objetivo primordial de la administración de la empresa es no solamente la protección de los Activos de Información sino proteger la organización y su destreza en el desempeño de su misión. Por tal razón, este asunto no debe ser asumido como una cuestión netamente técnica apropiada por el Departamento de Sistemas, sino como una tarea administrativa al mismo nivel de las grandes funciones de la organización y con el compromiso de todos los funcionarios.

Una evaluación de riesgos implica calcular el impacto causado en el Activo de Información la materialización de las amenazas. Este proceso se ve resumido en la Matriz de Riesgos, documento que muestra los elementos (Activos de Información), su relación, las amenazas, la probabilidad de ocurrencia y el impacto. El Riesgo Total (RT) resulta de multiplicar la Probabilidad de ocurrencia por el Impacto.

Con el análisis de riesgos se busca identificar las posibles causas, discriminar los más significativos y a partir de este pronóstico diseñar e implementar los mecanismos de control más idóneos para minimizar los efectos, además de permitir analizar el tiempo, trabajo y recursos necesarios para solventar los problemas de seguridad de la información.

4.4.3 Inventario de activos de información. Consecuente con la importancia de la información y los elementos que la soportan, procesan, transportan y almacenan, UNITRANSA S.A. requiere la adopción de un mecanismo de gestión de inventario de Activos de Información que permitan un manejo ágil y con mayor eficiencia.

Un Activo de Información es un elemento de hardware, de software, de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad[30].

Establecer los lineamientos para una adecuada gestión de los Activos de Información de UNITRANSA S.A. busca entre otros los siguientes objetivos: [31]

[30] Alcaldía Mayor de Bogotá. Inventario de activos de Información [online]. Disponible en Internet: http://secretariageneralalcaldiamayor.gov.co/sites/default/files/lineamiento_11_inventario_de_activos_de_informacion.pdf

[31] Revista ALIDE []enero, marzo, 2013]. ¿Cómo gestionar activos de información? [online]. Disponible en Internet: http://www.alide.org.pe/download/Financ_Sectorial/fn13_fin_rev1_activos.pdf

- Controlar el grado de exposición ante amenazas y minimizar las vulnerabilidades de los Activos de Información.
- Prevenir un deterioro en la imagen de la organización.
- Propiciar un esquema apropiado para la administración de recursos.
- Reducir las probabilidades de riesgo de incidentes de seguridad en los Activos de Información.
- Reducir el impacto sobre los Activos de Información en el evento de materializarse los incidentes de seguridad.
- Cumplir con los requerimientos legales vigente.
- Asignar responsabilidades.
- Desplegar acciones correctivas.
- Contribuir a la mejora continua de procesos tecnológicos.
- Concretar estrategias de seguridad de acuerdo a los requerimientos de cada activo.
- Efectuar un fácil y eficaz inventario de activos.
- Desarrollar planes de mantenimiento preventivo y/o correctivo.

4.4.4 Etiquetado de Activos de Información. UNITRANSA S.A., atendiendo los requerimientos básicos de un sistema de gestión de Activos de Información, asume el compromiso de incorporar un método de etiquetado de activos de información como el paso inicial para preservar su integridad, disponibilidad y confidencialidad. Argumento este incluido en el anexo A.8 Gestión de activos de la norma ISO/IEC 27001:20013.

- **Inventario de activos**: todos los activos de información deben estar claramente identificados y se debe elaborar y mantener un inventario de ellos.
- **Propiedad de los activos**: los activos de información del inventario deben tener un propietario.
- **Clasificación de la información**: se considera pertinente clasificar la información acorde con los requerimientos legales, su valor para la empresa, la criticidad y la susceptibilidad a ser modificada sin autorización previa.
- **Uso Aceptable de los Activos**: es deber del responsable de la seguridad de la información en una organización crear y documentar el reglamento de uso aceptable de los Activos de Información y la información, además de las instalaciones donde se procesa[32].

[32] Scribd. ISO 27001:2013 - ANEXO A [online]. Disponible en Internet: https://es.scribd.com/doc/232787821/ISO27001-2013-Anexo-a-En-Tabla-Excel

- **Etiquetado y manipulado de la información**: se considera necesario crear un procedimiento para el etiquetado de la información acorde con la metodología de clasificación de la información que tenga la empresa.

La etiqueta de Activos de Información para UNITRANSA S.A. debe incluir en cada activo:

- Nombre del activo.
- Código del Departamento al que pertenece.
- Criticidad.
- Propiedades.
- Código de barras.

Lo anterior, permite validar que el responsable de la seguridad de la información en una organización debe seguir unos criterios básicos para desarrollar la gestión y clasificación de los Activos de Información, con el propósito de determinar que activos posee, el papel que desempeñan los funcionarios sobre ellos, el reglamento de buen uso, las condiciones técnicas, el grado de eficiencia y el nivel de criticidad de la información que maneja[33].

4.4.5 Concienciación de la protección de la información y los activos. El creciente desarrollo tecnológico experimentado en la última década ha permito la creación de herramientas de seguridad informática más perfeccionadas, eficientes y veloces. Pese a esta situación, el empleado sigue siendo el factor decisivo que determina la seguridad de una organización. Implementar mecanismos de seguridad como potentes cortafuegos, control de acceso biométrico, IDS, largas y confusas contraseñas, programas "todo en 1" (antivirus, malware, antispyware, etc.), no constituyen la solución más idónea para la protección de la información, pues finalmente es el empleado el que procesa, modifica, guarda y elimina la información. Aun con la creación y aplicación de las más estrictas políticas que certifiquen los privilegios de acceso a la información, esta sea guardada de forma segura y su transferencia esté encriptada, finalmente son las personas las que la manipulan y conocen las medidas de protección, lo que implica riesgos cuando su manejo está a cargo de empleados malintencionados o inexpertos que ejecutan acciones de riesgo como visitar páginas web de contenido engañoso, desactivar el antivirus, abrir archivos adjuntos de correo electrónico y conectar pendrives desconocidos a su computadora. Ante esta situación y luego de conocidos los incidentes de seguridad, la urgente operación generalmente consiste en la restricción de las unidades de extracción, copia y borrado de archivos, la prohibición

[33] MINTIC. Guía para la Gestión y Clasificación de Activos de Información [online]. Disponible en Internet: http://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

de visitas a páginas web externas, control sobre el recibo y envío de correos electrónicos y deshabilitar los puertos USB. Las imposiciones de acciones restrictivas extremas no son muy efectivas; generan inconformismo en los usuarios por las dificultades en el ejercicio de sus labores diarias, ralentizan procesos, disminuyen la productividad, además de la dificultad que implica vigilar el cumplimiento de dichas medidas. [34]

A partir de la orientación anterior, UNITRANSA S.A, una empresa que soporta sus procesos y administra la información en medios tecnológicos, acepta el desafío de contribuir en la búsqueda de soluciones a los problemas de seguridad de la información adelantando procesos en la concienciación de sus empleados entorno a la ciberseguridad. Con solo conseguir que los usuarios del sistema desconfíen de los archivos adjuntos que llegan a su cuenta de correo, no compartan sus contraseñas, cierren su sesión al alejarse de su puesto de trabajo, no pierdan de vista sus equipos portátiles y utilicen herramientas para encriptar la información más relevante, se habrá evitado un importante número de incidentes de seguridad.

4.4.6 Políticas de Seguridad de la Información (PSI). La información como uno de los activos más importantes de una organización y elemento indispensable en el desarrollo de los procesos que contribuyen a la misión de la empresa, es el objetivo que el administrador de seguridad debe mirar para establecer las estrategias que contribuyan a mantener la integridad, disponibilidad y confidencialidad de los datos y los elementos que la procesan, transmiten o almacenan. En tal sentido la creación y puesta en conocimiento de las políticas de seguridad de la información son una herramienta esencial para proteger los sistemas de información del creciente número de amenazas a las que se exponen los dispositivos tecnológicos y la información misma para asegurar la continuidad del negocio y alcanzar las metas empresariales[35].

En consideración, UNITRANSA S.A. reconoce la relevancia de la adopción de mecanismos de seguridad que contribuyan a la protección de su información, por lo que aprueba la creación, documentación y divulgación de un pormenorizado compendio de instrucciones claras, precisas y concisas que marquen los rumbos en el uso de los Activos de Información y los datos. Las políticas de Seguridad de la Información de UNITRANSA S.A. serán de obligatorio cumplimiento para todos sus

[34] INSTITUTO NACIONAL DE CIBERSEGURIDAD. Kid de concienciación [online]. Disponible en Internet: https://www.incibe.es/protege-tu-empresa/kit-concienciacion

[35] Alcaldía de Ibagué. Política de seguridad de la información [online]. Disponible en Internter: http://www.alcaldiadeibague.gov.co/portal/admin/archivos/publicaciones/2015/11918-DOC-20151001.pdf

empleados, practicantes, socios, contratistas y terceros que hagan uso de los recursos del sistema. Su incumplimiento será motivo de acciones disciplinarias y/o penales según sea el caso.

Algunas excepciones a la aplicación de las políticas de seguridad de la información serán aprobadas por el Departamento de Sistemas siempre y cuando dicha excepción no afecte negativamente la consecución de los objetivos de la compañía y será documentada expresamente.

Las políticas de seguridad de la información se someterán a una evaluación periódica según disposición de la asamblea general y se arán las respectivas modificaciones que garanticen su efectividad.

4.5 ASPECTOS LEGALES

El diseño del SGSI en la empresa UNITRANSA S.A. se realiza con base a la legislación colombiana.

4.5.1 Ley 1341 de 2009. Artículo 1°. Objeto. La presente ley, determina el marco general para la formulación de las políticas públicas que regirán el sector de las Tecnologías de la Información y las Comunicaciones, su ordenamiento general, el régimen de competencia, la protección al usuario, así como lo concerniente a la cobertura, la calidad del servicio, la promoción de la inversión en el sector y el desarrollo de estas tecnologías, el uso eficiente de las redes y del espectro radioeléctrico, así como las potestades del Estado en relación con la planeación, la gestión, la administración adecuada y eficiente de los recursos, regulación, control y vigilancia del mismo y facilitando el libre acceso y sin discriminación de los habitantes del territorio nacional a la Sociedad de la Información[36].

4.5.2 Ley 1266 de 2008. Artículo 1°. Objeto**.** La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información establecido en el artículo 20 de la Constitución Política, particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países**[37].**

[36]COLOMBIA.CONGRESO DE LA REPUBLICA. Ley 1341(29, julio, 2009). Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones. Diario Oficial. Bogotá. D.C., 2009, no.4742.

[37]. COLOMBIA.CONGRESO DE LA REPUBLICA. Ley 1266(31, diciembre, 2008). Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales. Diario Oficial. Bogotá. D.C., 2009, no.47219

4.5.3 Ley 527 de 1999. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones[38].

4.5.4 Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones[39].

[38]COLOMBIA.CONGRESO DE LA REPUBLICA. Ley 527(18, agosto, 1999). por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales. Diario Oficial. Bogotá. D.C.,18, agosto, 1999, no.43673.

[39]COLOMBIA.CONGRESO DE LA REPUBLICA. Ley 527(5, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos". Diario Oficial. Bogotá. D.C.,2009, no.47223.

5. MARCO METODOLÓGICO

5.1 INVESTIGACIÓN APLICADA

Partiendo de una situación problemática que requiere solución, como lo es la orientación de los procesos de la organización en torno a la seguridad de la información, la metodología propuesta en el diseño de un SGSI a la empresa UNITRANSA S.A. se parte del modelo PHVA (Planear – Hacer – Verificar – Actuar) o su sigla en inglés PDCA (Plan Do Check Act), sistema que está definido en la norma ISO/IEC 27001:2013. Las técnicas de recolección de datos empleada para este proyecto fueron la observación directa, la entrevista y el cuestionario.

En la definición de los procesos relacionados en el SGSI, aunque no es parte del presente estudio establecer una metodología para el enfoque de procesos de la empresa, se establecerán guías generales o recomendaciones que permitan definir las técnicas necesarias para cumplir con este procedimiento.

Es recomendable el uso de este modelo metodológico al implementarse un sistema de gestión, de tal manera que, al aplicarla en la política de seguridad y objetivos del sistema, así como en los procesos, la probabilidad de éxito sea mayor. Puede aplicarse a todos los procesos la metodología conocida como “Planificar- Hacer-Verificar-Actuar” (PHVA). La cual se puede describir de una forma resumida como:

- **Planear:** en esta etapa se definen los objetivos y los procesos necesarios para conseguir los resultados, atendiendo las precisiones del cliente y las políticas propias de la organización.
- **Hacer:** implica la puesta en marcha de los diferentes procesos.
- **Verificar:** conlleva realizar el seguimiento continuo y las métricas de los procesos, productos y servicios con relación a las políticas, los objetivos, los requisitos y por supuesto los resultados.
- **Actuar:** acarrea la toma de decisiones para el mejoramiento continuo del desarrollo de los procesos.

5.2 POBLACION

UNITRANSA S.A es una empresa de transporte urbano que presta sus servicios al área metropolitana de la ciudad de Bucaramanga en el departamento de Santander, posee 283 funcionarios, entre directivos, accionistas, gerente, secretarios, ingeniero, conductores, mecánicos, operarios de estaciones de servicio, personal de seguridad y oficios varios. Doce empleados interactúan con el sistema validando su ingreso con una cuenta de usuario y contraseña.

5.3 MUESTRA

Para conocer los procesos de la empresa y saber de primera mano los pormenores de incidentes de seguridad al igual que medir los conocimientos básicos en seguridad de la información a través de la realización de checklist y encuestas, se

tomaron cinco oficinas en donde se entrevistó a un empleado de cada dependencia y se observó su entorno laboral.

Las oficinas a las que se les realizó el estudio fueron:

- Oficina jurídica
- Sistemas
- Secretaría de personal
- Secretaría de gerencia
- Contabilidad

5.4 DISEÑO METODOLÓGICO

La metodología usada en el desarrollo del presente estudio sigue los preceptos del Ciclo de Mejora Continua PHVA (Planear, Hacer, Verificar y Actuar). Herramienta que permite a las empresas aumentar la competitividad de los productos o servicios ofrecidos, mejorando su calidad, ampliando su participación en el mercado y disminuyendo costos, situaciones estas reflejadas en mayores utilidades. Por su dinamismo y simplicidad esta metodología puede aplicarse en los diferentes procesos de UNITRANSA S.A., incluyendo la gestión de la seguridad de la información, que haciéndola de una manera correcta es de gran aporte a las actividades propias de la empresa.

5.4.1 Técnicas de recolección de datos. La obtención de los datos necesarios para adelantar el proyecto de diseño del SGSI de UNITRANSA S.A. requirió de la aplicación de las siguientes técnicas:

5.4.2 Observación. A través de las diferentes visitas realizadas a la empresa y mediante la observación directa del entorno geográfico del edificio, las oficinas, los elementos de trabajo y los empleados, se obtuvo un panorama global de la organización.

5.4.3 Entrevistas. Por medio de entrevistas de carácter formal e informal con varios de los empleados de la empresa se obtuvo un panorama general de la manera como se administran los activos de información, se presta la seguridad a las instalaciones, se impide el acceso a ciertos lugares y se da uso a los recursos de la organización.

5.4.4 Encuestas. Mediante el llenado de tablas de encuesta y listas de chequeo por parte de los funcionarios de UNITRANSA S.A. se recolectó información relacionada con las características de hardware y software de las estaciones de trabajo y el servidor, de igual forma se obtuvo información del router, las impresoras y demás elementos de la red LAN de la empresa. Esto permite determinar las vulnerabilidades a las que están expuestos los activos de información debido al Sistema Operativo, su versión y el soporte técnico, entre otros.

6. DESARROLLO DEL PROYECTO

Para el inicio del proyecto, se contó con el beneplácito de la empresa UNITRANSA S.A., encabeza del señor gerente quien aprobó el estudio relacionado para el diseño del SGSI. La ejecución del sistema muy probablemente implica la adopción de una reglamentación diferente a la utilizada por la empresa, conllevando ello a nuevos instructivos que la guíen, por lo que la intervención y el apoyo de la entidad es indispensable en todas las etapas de este proyecto.

La norma ISO 27001 establece los compromisos que deben tener la dirección y la gestión de los recursos para lograr el funcionamiento del SGSI.

Estos compromisos se deben evidenciar mediante el establecimiento de una política, instaurar los objetivos y planes del SGSI, establecer funciones y responsabilidades de seguridad de la información, comunicar a la organización la importancia del cumplimiento de lo establecido, brindar los recursos necesarios, decidir criterios y niveles de aceptación de riesgo, asegurar que se realicen las auditorías internas y efectuar las revisiones del SGSI.

La gerencia de UNITRANSA S.A. debe asignar los recursos necesarios para establecer, implantar, aplicar, hacer seguimiento, analizar, mantener y mejorar el SGSI. Debe cerciorarse que los procedimientos de seguridad de la información brinden apoyo a los requerimientos del negocio, identificando los requisitos legales y reglamentarios, así como las obligaciones de seguridad contractuales, mantener altos niveles de seguridad aplicando correctamente todos los controles efectuados, desarrollar revisiones periódicas y mejorar la eficacia del SGSI.

6.1 ALCANCE DEL PROYECTO

UNITRANSA S.A. es una empresa privada que está situada en la ciudad de Bucaramanga (Santander) y dedicada a ofrecer servicio de transporte de pasajeros en esta ciudad y su área metropolitana, cuenta con 283 funcionarios, 12 de los cuales poseen cuenta de usuario y contraseña para ingresar al sistema y hacer uso de los recursos informáticos de la organización.

Posee una infraestructura tecnológica formada por doce (12) computadoras personales, un (1) servidor y cinco (5) impresora, conectados en red a través de un router que le permite el acceso a Internet a través de un enlace de 5 MB ofrecido por las Empresas Municipales de Bucaramanga. Conociendo esta información y la encontrada al finalizar los procesos de investigación, se pretende realizar un análisis de riesgos para determinar las vulnerabilidades y amenazas a las que están expuestos sus activos de información, afectando la integridad, confidencialidad, disponibilidad y trazabilidad de la información.

6.2 ANÁLISIS DE RESULTADOS.

A continuación, se expone un análisis de los resultados obtenidos de la observación, las entrevistas y las encuestas, actividades estas que permiten obtener la información relacionada con el entorno de la empresa, los procesos, el hardware, el software, el nivel de conocimiento sobre seguridad de la información de los empleados, entre otros.

6.2.1 Análisis de la observación. La observación directa sobre los activos de información de UNITRANSA S.A. permite conocer de primera mano su ubicación, su utilización, los mecanismos de seguridad existentes, las no conformidades y de esta forma determinar las salvaguardas necesarias para contrarrestar las amenazas a las que están expuestos. En la Figura 5 se ve la parte exterior del edificio donde funciona la empresa UNITRANSA S.A.

El SGSI para UNITRANSA S.A. se inicia con la solicitud presentada al gerente de la empresa, donde se le plantea la necesidad de realizar un estudio de seguridad de la información que permita descubrir las vulnerabilidades existentes en su sistema de información y de esta manera sugerir la implementación de mecanismos de seguridad que permitan contrarrestar dichas situaciones hasta dejarlas en niveles aceptables de riesgo que no comprometan la continuidad del negocio.

La norma internacional ISO/IEC 27001describe cómo gestionar la seguridad de la información en una empresa, su anexo A contiene, entre otros el dominio A.5 Política de Seguridad de la Información y el dominio A.8 Gestión de Activos. Estos dos dominios representan el eje central del presente estudio que busca implementar los controles de seguridad que garanticen la confidencialidad, la integridad, la disponibilidad y la trazabilidad de los activos de información de UNITRANSA S.A.

El tratamiento del dominio A.8 Gestión de Activos requiere un análisis de los activos de información de la organización que contenga un inventario de activos, un responsable de los activos y unos acuerdos sobre el uso adecuado de ellos. Cabe anotar que los activos de información deben ser valorados de acuerdo a la importancia que representen para el desarrollo de los procesos diarios de la empresa. La valoración de los riesgos permite determinar su criticidad para predecir con mayor certeza el impacto que tendría sobre la empresa la materialización de una amenaza sobre determinado activo de información.

Para el desarrollo del dominio A. 5 Política de Seguridad de la Información es indispensable involucrar a los directivos de la empresa, socios, empleados, contratistas, proveedores y practicantes, encargados de la interacción con el sistema de información para que de una manera seria y responsable hagan uso de los activos de información de la empresa sin comprometer la integridad, la disponibilidad y la confidencialidad de la información.

Figura 5. Edificio UNITRANSA S.A.

Fuente: Autor

Se observa en la parte lateral derecha que el edificio donde funciona la empresa tiene en el cuarto piso un ventanal amplio y sin ninguna protección, lo que significa una vulnerabilidad evidente, toda vez que limita con una construcción vieja donde funciona una pequeña tienda.

Figura 6. Parque Romero

Fuente: Autor

La Figura 6 muestra el parque Romero, ubicado al frente de la empresa. En este lugar es bien conocido por todos, la presencia de indigentes y consumidores de alucinógenos, principalmente en horas nocturnas, situación que representa potencial peligro para las instalaciones y las personas que allí laboran.

Figura 7. Gabinete de pared

Fuente: Autor

La Figura7 muestra el gabinete de pared que contiene las conexiones de red de la empresa y sobre la caja el router y el modem. Evidencia la imagen un desorden en la organización de estos elementos, en primer lugar, el gabinete no tiene ninguna seguridad, ya que permanece abierto y facilitaría la desconexión de la red, además de la manipulación e incluso el hurto de estos dispositivos.

Figura 8. Oficina de secretaria de gerencia

Fuente: Autor

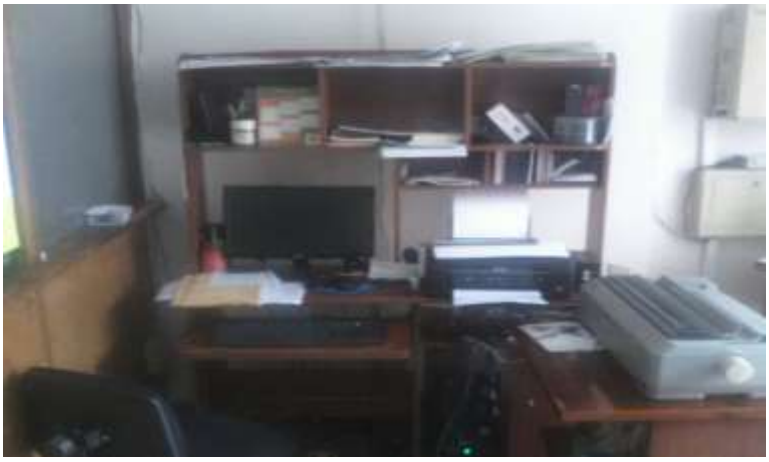
La Figura 8 expone la vulnerabilidad existente en la oficina de la secretaría de gerencia ante la posible presencia de incendio, ya que el computador y la impresora se encuentran sobre una mesa de madera que facilitaría la propagación de las llamas, al igual que la silla Rimax aledaña a los equipos. La mesa es demasiado corta para albergar tres equipos, es evidente, como lo muestra la imagen, que la impresora está a punto de caer. Los cables en la parte posterior del escritorio forman una maraña que certifican el desorden.

Figura 9. Oficina de gerencia

Fuente: Autor

La Figura9. Exhibe en la parte izquierda que los cables además de ser muy cortos, están sueltos, situación que expone cierto desorden observado en la oficina de gerencia de UNITRANSA S.A., además del peligro a enredarse y caer al pretender salir por dicho lugar.

Figura 10. Oficina del auxiliar programador



Fuente: Autor

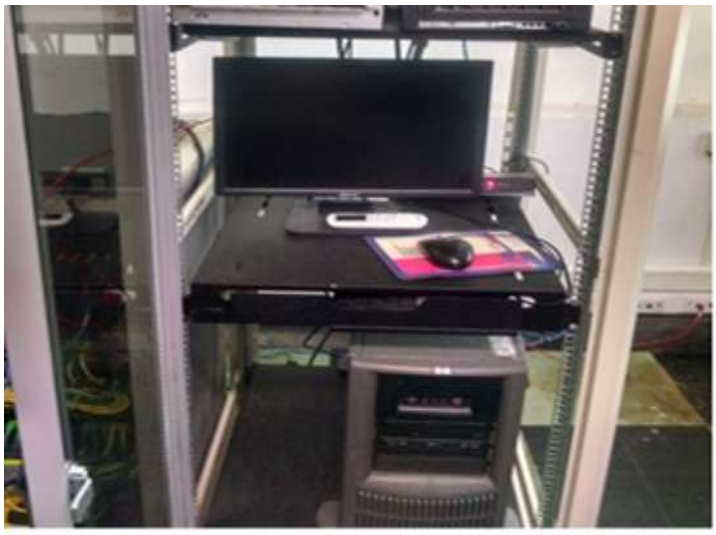
La Figura10 muestra la oficina del Auxiliar Programador. Expone el reducido espacio de trabajo y la ubicación incomoda de los elementos de oficina, además de la cantidad de material combustible como madera y papel que en la eventualidad de un incendio incrementarían las llamas.

Figura 11. Control de incendios

Fuente: Autor.

En la Figura 11 se observa que la empresa posee extintores manuales tipo A, B y C para control de fuegos básicos. Se evidencia que estos elementos no tienen gabinete apropiado para soportarlos, lo que los hace propensos a accidentes. Se recomienda la instalación de sistemas automáticos de control de incendios principalmente en el centro de cómputo y recinto del servidor.

Figura 12. Servidor



Fuente: Autor.

La Figura 12 muestra el servidor de UNITRANSA S.A. Se observa que el equipo está sobre el piso, lo que representa una vulnerabilidad en el evento de presentarse una inundación por la ruptura de un tubo del acueducto o en caso de un desastre natural.

Figura 13. UPS

Fuente: Autor.

La Figura 13 muestra la UPS de la serie UPO22 de doble conversión que ofrece gran protección a los datos y es una de las últimas inversiones hechas por la empresa en relación con la protección de los datos.

Figura 14. Cableado.

Fuente: Autor.

La Figura 14 muestra el sistema de canaletas a través de las cuales se tienden los dos métodos de cableado: el cableado regulado que proveerá de corriente a los equipos de cómputo y la no regulada para el uso cotidiano.

6.2.2 Análisis de las entrevistas. Este mecanismo de obtención de información realizado a los funcionarios de UNITRANSA S.A. y al Jefe del Departamento de Sistemas, permitió un acercamiento con los usuarios del sistema, conocedores de las vulnerabilidades, de las falencias del sistema y directamente responsables de la materialización de incidentes de seguridad. La Tabla 2 muestra la relación de Equipos hardware más relevantes de UNITRANSA S.A.

Tabla 2. Equipos hardware

EQUIPO	CANTIDAD	SISTEMA OPERATIVO		
		Windows XP	Windows 7	Windows 8
PC	11	3	4	4
Portátil	1	0	0	1
Servidor	1	0	0	1
Router	1	N/A	N/A	N/A
Switch	3	N/A	N/A	N/A
UPS	1	N/A	N/A	N/A
Gabinete de Pared	1	N/A	N/A	N/A
Patch Panel	1	N/A	N/A	N/A
Impresora	9	N/A	N/A	N/A

Fuente: Autor.

6.2.3 Análisis de resultados de encuestas. Realizado el checklist sobre los componentes de seguridad (Anexo D) al Departamento de Sistemas de UNITRANSA S.A. para establecer riesgos en el manejo de la información, se pudo determinar:

Tabla 3. Porcentaje de respuestas

ALTERNATIVA DE RESPUESTA	FRECUENCIA	PORCENTAJE
SI	9	30%
NO	21	70%
TOTAL	30	100%

Fuente: Autor.

Los datos de la Tabla 3 reflejan que los componentes de seguridad de la información actualmente implementados en UNITRANSA S.A. no son los ideales, requieren con urgencia la adopción de mecanismos de seguridad más estrictos, al igual que la generación de una cultura de seguridad más arraigada.

Realizadas las encuestas de satisfacción de servicios informáticos (Anexo E), se pudo determinar que:

Tabla 4. Respuestas de pregunta abierta

ALTERNATIVA DE RESPUESTA	FRECUENCIA	PORCENTAJE
Correcta	21	42%
Incorrecta	29	58%
Total, respuestas	50	100%

Fuente: Autor.

Los resultados de la Tabla 4 muestran que se desconoce en más del 50% de los conceptos básicos de seguridad de la información, además determina que se debe adelantar un plan de sensibilización de la seguridad de la Información a los funcionarios de UNITRANSA S.A. con el fin de que se asuma un verdadero compromiso con la seguridad de la información de la organización.

La Tabla 5 muestra que el 45% de las situaciones necesarias para un adecuado manejo de la seguridad de la información de UNITRANSA S.A. no están dadas. No se debe esperar la materialización de las amenazas para implementar verdaderos mecanismos de protección.

Tabla 5. Satisfacción de servicios

ALTERNATIVA DE RESPUESTA	FRECUENCIA	PORCENTAJE
SI	85	54.83%
NO	70	45.16%
TOTAL	155	100%

Fuente: Autor.

6.2.4 Técnicas de análisis de datos. Las técnicas de análisis de datos utilizada para el proyecto de gestión de riesgos de UNITRANSA S.A. fue la utilización de tablas para la obtención sencilla de resultados, tal como lo estipula la metodología MAGERIT en su versión 3.0.

El análisis de riesgos implica trabajar con una cantidad considerable de elementos que se deben combinar dentro de un sistema ordenado según la importancia, evitando que muchos perjudiquen la visión de conjunto.

La utilización de métodos simples de análisis como el uso de tablas ha demostrado su eficiencia, ya que, sin ser muy exactas, sí descubren la importancia relativa de los Activos de Información expuestos a amenazas.

MAGERIT utiliza la siguiente escala para asignar un valor relativo a los activos de información a analizar. Este valor permite además calificar la magnitud del impacto y la magnitud del riesgo.

- ✓ **MB:** Muy Baja
- ✓ **B:** Baja

- ✓ **M:** Media
- ✓ **A:** Alta
- ✓ **MA:** Muy Alta

6.3 ANÁLISIS Y EVALUACIÓN DE RIESGOS DE LOS ACTIVOS DE INFORMACIÓN.

La evaluación de riesgos pretende identificar y examinar con imparcialidad los peligros a los que se exponen los sistemas de información, los activos y servicios con el objetivo de identificar y recomendar los controles apropiados.

La norma ISO/IEC 27001:2013 recomienda la adopción de una Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información que identifique claramente los activos de información y determine los riesgos a los que se exponen, siguiendo un proceso sistemático que permita una certificación en caso de ser requerida.

El primer paso para el análisis y gestión de riesgos usando la metodología MAGERIT lo constituye la determinación de los activos relevantes para la organización, su interrelación y su valor en el sentido del perjuicio que tendría para la empresa su degradación. A través de la observación directa, entrevistas y los cuadros de entrevista donde se registran las características más relevantes de los equipos informáticos, aplicaciones de software, equipamiento auxiliar, redes de comunicación e instalaciones de la organización, se puede identificar los activos de información más significativos que forman parte de la empresa.

El segundo paso de la gestión de riesgos lo establece la determinación de amenazas a que están expuestos los activos de información. Posteriormente se debe determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo, para luego estimar el impacto, definido como el daño causado al activo, producido por la materialización de dichas amenazas. Por último, se estima el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

6.3.1 Identificación de activos. A la hora de realizar una gestión de riesgos, MAGERIT determina la "caracterización de los activos" como la primera tarea a realizar (MAR.1). Para el Sistema de Gestión de la Seguridad de la Información de UNITRANSA S.A. se tomó en consideración el conjunto de dependencias relacionadas con todos los departamentos de la empresa que funcionan en el edificio central y se procedió a clasificar los activos.

La consolidación de grupos de activos, como lo propone la metodología adoptada para el presente proyecto, permite establecer cuáles son los más significativos, cuales más susceptibles a recibir un ataque informático y de materializarse, cuan afectada se vería la organización**.** La Tabla 6 muestra el inventario de Activos de Información de UNITRANSA S.A.

Tabla 6. Inventario de Activos

CODIGO DE ACTIVO MAGERIT	NOMBRE DE ACTIVO MAGERIT	CODIGO DE ACTIVO UNITRANSA S.A.	DESCRIPCION
[essential] Activos esenciales			
[vr]	Datos vitales	[INFO_SOC]	Información Socios y proveedores
		[INFO_NIIF]	Información Contable de la empresa
[classified]	Datos clasificados	[COD_FTE]	Código fuente de aplicativos
		[DOC_PROY]	Documentación de proyectos
		[DOC_EST]	Documentación estratégica
[P]Personal			
[ui]	Usuarios internos	[U_INTER]	Usuarios Internos de UNITRANSA S.A. (empleados).
[adm]	administradores	[ADMIN_UN]	Administrador de la empresa.
[prov]	Proveedores	[PROV_UN]	Proveedores de UNITRANSA S.A.
[soc]	Socios	[SOC_UN]	Socios UNITRANSA S.A.
[D] Datos/Información			
[files]	Ficheros	[F_VARIOS]	Archivos varios de UNITRANSA S.A.
[backup]	Copias de respaldo	[BACK_UN]	Archivos de respaldo de información de la empresa
[conf]	Datos de configuración	[CONF_EQ]	Datos de configuración de equipos
[password]	Credenciales	[PSW_US]	Credenciales de usuarios del sistema
[log]	Registro de actividad	[LOG_UN]	Registro de actividad del sistema
[int]	Datos de gestión interna	[GEST_INT]	Datos de gestión de la empresa
[S] Servicios			
[internet]	Internet	[INT_UNIT]	Internet de la empresa
[telnet]	acceso remoto a cuenta local	[TELN_UNIT]	Acceso remoto
[email]	correo electrónico	[E_UNIT]	Correo electrónico de UNITRANSA S.A.

Tabla 6. (Continuación)

CODIGO DE ACTIVO MAGERIT	NOMBRE DE ACTIVO MAGERIT	CODIGO DE ACTIVO UNITRANSA S.A.	DESCRIPCION
[file]	almacenamiento de ficheros	[FILE_UNIT]	Almacenamiento de archivos de la empresa.
[ftp]	transferencia de ficheros	[FTP_UNIT]	Transferencia de archivos de la empresa
[edi]	intercambio electrónico de datos	[EDI_UNIT]	Intercambio de datos de la empresa
[dir]	servicio de directorio	[DIR_UNIT]	Servicio de directorio de UNITRANSA S.A.
[idm]	gestión de identidades	[IDM_UNIT]	Gestión de identidades de UNITRANSA S.A.
[ipm]	gestión de privilegios	[IMP_UNIT]	gestión de privilegios de la empresa.
[HW] Hardware			
[host]	Grandes equipos	[SRV_BD]	Equipo Servidor de Bases de Datos
[mid]	Equipos medios	[PC1]	Computadora de Gerencia
[pc]	Informática personal	[PC2]	Computadora de Dpto. Jurídico
[pc]	Informática personal	[PC3]	Puestos de trabajo
[print]	Medios de impresión	[IMP]	Impresora
[switch]	Conmutadores	[SW_P1]	Switch Ethernet Gigabit Linksys SE4008 WRT de 8 puertos (1er. Piso).
		[SW_P2]	Switch Linksys SE3016 de 16 puertos (2º. Piso).
		[SW_P3]	Switch Linksys SE4008 WRT de 8 puertos (3er. Piso)
[router]	Encaminadores	[RTR]	Router Netgear 4g Lte Router Lg2200d
[SW]Aplicaciones			
[app]	Servidor de aplicaciones	[SRV_APP]	Servidor de aplicaciones utilizadas en la empresa
[dbms]	Sistema de gestión de bases de datos	[BD_ORC]	Manejador de Base de Datos Oracle

Tabla 6. (Continuación)

CODIGO DE ACTIVO MAGERIT	NOMBRE DE ACTIVO MAGERIT	CODIGO DE ACTIVO UNITRANSA S.A.	DESCRIPCION
[os]	Sistema Operativo	[SO_WIND7]	Sistema Operativo Windows 7 Profesional
[os]	Sistema Operativo	[SO_WIND8]	Sistema Operativo Windows 8
[os]	Sistema Operativo	[SO_WINDXP]	Sistema Operativo Windows XP
[office]	Ofimática	[ADOB_DW]	Editor HTML: Adobe Dreamweaver
[office]	Ofimática	[ARTIS]	Plantillas web: Artister
[office]	Ofimática	[ADOB_FW]	Editor de imágenes web: Adobe Fireworks
[office]	Ofimática	[LOG_CR]	Diseño de logos: Logo Creator
[email_client]	Cliente de correo electrónico	[CLT_FTP]	Cliente FTP: Filezilla
[prp]	Desarrollo propio	[DES_PROPIO]	Aplicaciones de desarrollo propio
[av]	Anti virus	[ANT_VIRUS]	Antivirus
[AUX]Equipamiento auxiliar			
[ups]	Sistemas de alimentación ininterrumpida	[UPS]	Sistema de alimentación ininterrumpida
[cabling]	Cableado	[CABL]	Cableado
[ac]	Equipos de climatización	[CTR_TEMP]	Equipos de climatización
[gen]	Generadores eléctricos	[GEN_ELECT]	Generador de energia
[COM]Redes de comunicación			
[lan]	Red local	[NET_UNIT]	Red local de UNITRANSA S.A.
[L]Instalaciones			
[building]	edificio	[EDIF_SEDE]	Edificio sede de la empresa.

Fuente: Autor.

6.3.2 Valoración de activos. Valorar los activos de información de una organización, teóricamente es pertinente mediante la utilización de cualquier escala de valores. Sin embargo, en la práctica es recomendable la utilización de una escala común para todas las dimensiones, de esta manera es posible comparar riesgos, además de lograr cierta homogeneidad de criterios que faciliten confrontar trabajos de análisis realizados separadamente.

La valoración cualitativa, dispuesta para este proyecto, deja cierta discrecionalidad al analista, pues permite aplicar juicios subjetivos. MAGERIT establece una escala de diez valores, donde el cero determina un valor despreciable, es decir no constituye riesgo alguno.

Debe asignarse a los activos un valor ajustado al servicio que prestan a la empresa, medido por el impacto que tendría excluir dicho activo a efectos de la materialización de alguna amenaza. La Tabla7 establece los criterios MAGERIT utilizados para la gestión de riesgos.

Tabla 7. Valoración del impacto

VALOR		**CRITERIO**	
10	Extremo	Daño extremadamente grave	5
9	Muy alto	Daño muy grave	4
6-8	Alto	Daño grave	3
3-5	Medio	Daño importante	2
1-2	Bajo	Daño menor	1
0	Despreciable	Irrelevante a efectos prácticos	0

Fuente: http://datateca.unad.edu.co/

6.3.3 Dimensiones de valoración. Una dimensión es un aspecto o característica de un activo que lo hace diferente de otro y permite valorar las consecuencias de la materialización de las amenazas. Esta valoración apunta a la afectación de cada uno de los pilares de la seguridad de la información de cada activo.

- ✓ **[D]Disponibilidad**. Dimensiona el impacto generado a UNITRANSA S.A. que un activo no pudiera ser accedido o no prestara el servicio requerido.

- ✓ **[I]Integridad**. Determina el efecto causado a la empresa el hecho de que la información transmitida y/o almacenada sufra alguna modificación.

- ✓ **[C]Confidencialidad.** Estipula el daño generado a la organización que la información procesada por UNITRANSA S.A. fuera conocida por todos.

- ✓ **[A]Autenticidad.** Establece el perjuicio producido al no garantizar que quien utiliza un activo o servicio sea quien realmente está autorizado para hacerlo.

- ✓ **[T]Trazabilidad**. Constituye el impacto causado a la empresa el hecho de que no quede constancia fehaciente del uso de un servicio o activo. Pertinente en el caso de investigaciones de carácter disciplinario o penal.

La Tabla 8 muestra los activos de información de UNITRANSA S.A. y el impacto que ocasionaría en cada una de sus dimensiones la materialización de las amenazas.

Tabla 8. Impacto sobre los activos

CODIGO DE ACTIVO MAGERIT	NOMBRE DE ACTIVO MAGERIT	CODIGO DE ACTIVO UNITRANSA S.A.	DESCRIPCION	VALOR /DIMENSION				
				D	I	C	A	T
GRUPO: Activos esenciales								
[vr]	Datos vitales	[INFO_SOC]	Información Socios y proveedores	8	10	10	10	7
		[INFO_NIIF]	Información Contable de la empresa	10	10	10	10	8
[classified]	Datos clasificados	[COD_FTE]	Código fuente de aplicativos	6	7	8	6	3
		[DOC_PROY]	Documentación de proyectos	10	9	10	5	3
		[DOC_EST]	Documentación estratégica	8	9	10	5	3
[P]Personal								
[ui]	Usuarios internos	[U_INTER]	Usuarios Internos de UNITRANSA S.A. (empleados).	10	7	5	9	0
[adm]	administradores	[ADMIN_UN]	Administrador de la empresa.	9	5	9	1	0
[prov]	Proveedores	[PROV_UN]	Proveedores de UNITRANSA S.A.	6	5	7	1	0
[soc]	Socios	[SOC_UN]	Socios UNITRANSA S.A.	2	5	1	1	0
[D] Datos/Información								
[files]	Ficheros	[F_VARIOS]	Archivos varios de UNITRANSA S.A.	10	2	2	5	0
[backup]	Copias de respaldo	[BACK_UN]	Archivos de respaldo de información de la empresa	9	1	2	1	0
[conf]	Datos de configuración	[CONF_EQ]	Datos de configuración de equipos	6	1	2	0	0
[password]	Credenciales	[PSW_US]	Credenciales de usuarios del sistema	9	10	10	10	0

Tabla 8. (continuación)

CODIGO DE ACTIVO MAGERIT	NOMBRE DE ACTIVO MAGERIT	CODIGO DE ACTIVO UNITRANSA S.A.	DESCRIPCION	VALOR /DIMENSION				
				D	I	C	A	T
[log]	Registro de actividad	[LOG_UN]	Registro de actividad del sistema	5	1	1	0	0
[int]	Datos de gestión interna	[GEST_INT]	Datos de gestión de la empresa	9	9	9	8	1
[S] Servicios								
[internet]	Internet	[INT_UNIT]	Internet de la empresa	8	0	0	0	0
[telnet]	acceso remoto a cuenta local	[TELN_UNIT]	Acceso remoto	8	0	0	0	0
[email]	correo electrónico	[E_UNIT]	Correo electrónico de UNITRANSA S.A.	8	0	1	1	0
[file]	almacenamiento de ficheros	[FILE_UNIT]	Almacenamiento de archivos de la empresa.	10	5	2	0	0
[ftp]	transferencia de ficheros	[FTP_UNIT]	Transferencia de archivos de la empresa	9	5	5	2	0
[edi]	intercambio electrónico de datos	[EDI_UNIT]	Intercambio de datos de la empresa	8	5	8	5	0
[dir]	servicio de directorio	[DIR_UNIT]	Servicio de directorio de UNITRANSA S.A.	2	2	5	6	0
[idm]	gestión de identidades	[IDM_UNIT]	Gestión de identidades de UNITRANSA S.A.	1	9	9	10	0
[ipm]	gestión de privilegios	[IMP_UNIT]	gestión de privilegios de la empresa.	9	8	9	10	0
[HW] Hardware								
[host]	Grandes equipos	[SRV_BD]	Equipo Servidor de Bases de Datos	10	10	10	10	8
[mid]	Equipos medios	[PC1]	Computadora de Gerencia	8	9	10	6	5
[pc]	Informática personal	[PC2]	Computadora de Dpto. Jurídico	8	8	9	7	5
[pc]	Informática personal	[PC3]	Puestos de trabajo	4	2	4	3	2

Tabla 8. (continuación)

CODIGO DE ACTIVO MAGERIT	NOMBRE DE ACTIVO MAGERIT	CODIGO DE ACTIVO UNITRANSA S.A.	DESCRIPCION	VALOR /DIMENSION				
				D	I	C	A	T
[print]	Medios de impresión	[IMP]	Impresora	3	0	1	1	0
[firewall]	Cortafuegos	[FRW]	Firewall	1	8	8	10	0
[switch]	Conmutadores	[SW_P1]	Switch Ethernet Gigabit Linksys SE4008 WRT de 8 puertos (1er. Piso	8	2	2	3	0
		[SW_P2]	Switch Linksys SE3016 de 16 puertos (2º. Piso)	8	2	2	3	0
		[SW_P3]	Switch Linksys SE4008 WRT de 8 puertos (3er. Piso)	8	2	2	3	0
[router]	Encaminadores	[RTR]	Router Netgear 4g Lte Router Lg2200d	9	8	7	8	5
GRUPO: Aplicaciones								
[app]	Servidor de aplicaciones	[SRV_APP]	Servidor de aplicaciones utilizadas en la empresa	10	8	8	7	9
[dbms]	Sistema de gestión de bases de datos	[BD_ORC]	Manejador de Base de Datos Oracle	10	8	8	7	6
[os]	Sistema Operativo	[SO_WIND7]	Sistema Operativo Windows 7 Profesional	5	4	4	3	4
[os]	Sistema Operativo	[SO_WIND8]	Sistema Operativo Windows 8	5	4	4	3	4
[os]	Sistema Operativo	[SO_WINDXP]	Sistema Operativo Windows XP	5	4	4	3	4
[office]	Ofimática	[ADOB_DW]	Editor HTML: Adobe Dreamweaver	2	1	0	1	0
[office]	Ofimática	[ARTIS]	Plantillas web: Artister	2	1	0	1	0
[office]	Ofimática	[ADOB_FW]	Editor de imágenes web: Adobe Fireworks	2	1	0	1	0
[office]	Ofimática	[LOG_CR]	Diseño de logos: Logo Creator	1	1	0	0	0
[email_client]	Cliente de correo electrónico	[CLT_FTP]	Cliente FTP: Filezilla	8	3	2	2	2
[prp]	Desarrollo propio	[DES_PROPIO]	Aplicaciones de desarrollo propio	5	2	8	6	5

Tabla 8. (continuación)

CODIGO DE ACTIVO MAGERIT	NOMBRE DE ACTIVO MAGERIT	CODIGO DE ACTIVO UNITRANSA S.A.	DESCRIPCION	VALOR /DIMENSION				
				D	I	C	A	T
[av]	Anti virus	[ANT_VIRUS]	Antivirus	2	9	9	8	8
[AUX]Equipamiento auxiliar								
[ups]	Sistemas de alimentación ininterrumpida	[UPS]	Sistema de alimentación ininterrumpida	2	0	0	0	0
[cabling]	Cableado	[CABL]	Cableado	10	2	1	0	2
[ac]	Equipos de climatización	[CTR_TEMP]	Equipos de climatización	2	0	0	0	2
[gen]	Generadores eléctricos	[GEN_ELECT]	Generador de energía	8	0	0	0	3
[COM]Redes de comunicación								
[lan]	Red local	[NET_UNIT]	Red local de UNITRANSA S.A.	8	3	3	2	6
[L]Instalaciones								
[building]	Edificio	[EDIF_SEDE]	Edificio sede de la empresa.	10	0	0	0	0

Fuente: Autor.

6.3.4. Amenazas sobre los activos de información. Los activos de información de UNITRANSA S.A. al igual que cualquier organización, están expuestos a una serie de amenazas que, aunque muchas de ellas tienen una probabilidad de ocurrencia muy baja, bien vale la pena no descartarlas de plano.

6.3.5 Probabilidad de ocurrencia de las amenazas. Para medir la probabilidad de materialización de una amenaza sobre cada uno de los activos de información de UNITRANSA S.A.se utilizó la siguiente escala de valores que toma como valor de referencia un año, de tal manera que determine la ocurrencia como medida de la probabilidad

La Tabla 9 muestra el rango de frecuencia probable de ocurrencia de una amenaza sobre los activos de información de UNITRANASA S.A.

Tabla 9. Escala de probabilidad de amenaza

VULNERABILIDAD	RANGO	VALOR
Probabilidad muy alta	1 vez al día	100
Probabilidad alta	1 vez cada semana	70
Probabilidad media	1 vez cada 2 meses	50
Probabilidad baja	1 vez cada 6 meses	10
Probabilidad muy baja	1 vez cada año	5

Fuente: Valoración de amenazas (2016), obtenido de: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/3232_valoracin_de_amenazas.html

La Tabla10 muestra el rango porcentual del impacto sobre los activos de información de UNITRANSA S.A. en caso de materializarse una amenaza.

Tabla10. Rango de impacto

IMPACTO	VALOR
Muy alto	100%
Alto	75%
Medio	50%
Bajo	20%
Muy bajo	5%

Fuente: Valoración de amenazas (2016), obtenido de: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/3232_valoracin_de_amenazas.html

La Tabla11 muestra las amenazas sobre cada activo de información de UNITRANSA S.A. y el rango porcentual del impacto sobre cada una de las dimensiones del mismo.

Tabla11. Estimación de amenazas sobre activos

GRUPO DE ACTIVOS UNITRANSA S.A.	CLASIFICACIÓN DE AMENAZA (MAGERIT)	FRECUENCIA DE AMENAZA	AFECTACIÓN/DIMENSION				
			D	I	C	A	T
[essential] Activos esenciales							
Información Socios y proveedores	[E.1] Errores de los usuarios	10	5%	75%	75%		
	[E.2] Errores del administrador	10	20%	50%	75%		
	[E.15] Alteración accidental de la información	50		50%			
	[E.18] Destrucción de información (accidental)	5	100%				
	[E.19] Fugas de información	10			100%		
	[A.5] Suplantación de la identidad del usuario	5		100%	100%	100%	
	[A.6] Abuso de privilegios de acceso	5	20%	50%	100%		
	[A.11] Acceso no autorizado	10		50%	100%		
	[A.15] Modificación deliberada de la información	5		100%	50%		
	[A.18] Destrucción de información (intencional)	5	50%				
	[A.19] Divulgación de información	10			50%		
Información Contable de la empresa	[E.1] Errores de los usuarios	10	20%	50%	100%		
	[E.2] Errores del administrador	10	5%	50%	100%		
	[E.8] Difusión de software dañino	70	50%	75%	75%		
	[E.15] Alteración accidental de la información	50		50%	50%		
	[E.18] Destrucción de información (accidental)	5	100%				
	[E.19] Fugas de información	10			100%		
	[A.5] Suplantación de la identidad del usuario	5		100%	100%	100%	
	[A.6] Abuso de privilegios de acceso	5	20%	75%	100%		
	[A.11] Acceso no autorizado	10		50%	100%		
	[A.15] Modificación deliberada de la información	5		100%	50%		
	[A.18] Destrucción de información (intencional)	5	100%				
	[A.19] Divulgación de información	10			75%		

Tabla 11. (Continuación)

GRUPO DE ACTIVOS UNITRANSA S.A.	CLASIFICACIÓN DE AMENAZA (MAGERIT)	FRECUENCIA DE AMENAZA	AFECTACIÓN/DIMENSION				
			D	I	C	A	T
Código fuente de aplicativos	[E.1] Errores de los usuarios	5	5%	20%	50%		
	[E.2] Errores del administrador	5	5%	50%	50%		
	[E.8] Difusión de software dañino	10	5%	50%	20%		
	[E.15] Alteración accidental de la información	5		20%	20%		
	[E.18] Destrucción de información (accidental)	5	20%				
	[E.19] Fugas de información	5			50%		
	[A.5] Suplantación de la identidad del usuario	5		50%	50%	50%	
	[A.6] Abuso de privilegios de acceso	5	20%	50%	75%		
	[A.11] Acceso no autorizado	5		50%	50%		
	[A.15] Modificación deliberada de la información	5		50%			
	[A.18] Destrucción de información(intencional)	5	100%				
	[A.19] Divulgación de información	5			50%		
Documentación de proyectos	[E.1] Errores de los usuarios	50	5%	50%	75%		
	[E.2] Errores del administrador	5	5%	20%	75%		
	[E.8] Difusión de software dañino	10	20%	50%	75%		
	[E.15] Alteración accidental de la información	50		50%			
	[E.18] Destrucción de información (accidental)	5	75%				
	[E.19] Fugas de información	5			100%		
	[A.5] Suplantación de la identidad del usuario	5		50%	100%	100%	
	[A.6] Abuso de privilegios de acceso	5	20%	50%	100%		
	[A.11] Acceso no autorizado	5		50%	100%		
	[A.15] Modificación deliberada de la información	5		50%			
	[A.18] Destrucción de información (intencional)	5	100%				
	[A.19] Divulgación de información	5			50%		
	[E.1] Errores de los usuarios	50	5%	50%	75%		
	[E.2] Errores del administrador	5	5%	50%	75%		
	[E.8] Difusión de software dañino	10	5%	50%	75%		

Tabla 11. (Continuación)

GRUPO DE ACTIVOS UNITRANSA S.A.	CLASIFICACIÓN DE AMENAZA (MAGERIT)	FRECUENCIA DE AMENAZA	AFECTACIÓN/DIMENSION				
			D	I	C	A	T
Documentación estratégica	[E.15] Alteración accidental de la información	10		50%	50%		
	[E.18] Destrucción de información (accidental)	5	100%				
	[E.19] Fugas de información	5			100%		
	[A.5] Suplantación de la identidad del usuario	5		75%	100%	100%	
	[A.6] Abuso de privilegios de acceso	5	20%	20%	100%		
	[A.11] Acceso no autorizado	5		50%	100%		
	[A.15] Modificación deliberada de la información	5		75%	75%		
	[A.18] Destrucción de información (intencional)	5	100%				
	[A.19] Divulgación de información	5			100%		
[P]Personal							
Usuarios Internos de UNITRANSA S.A. (empleados).	[E.19] Fugas de información	5			100%		
	[A.28] Indisponibilidad del personal	50	50%				
	[A.29] Extorsión	5	50%	75%	100%		
	[A.30] Ingeniería social (picaresca)	10	50%	50%	50%		
Administrador de la empresa.	[E.7] Deficiencias en la organización	10	50%				
	[E.19] Fugas de información	5			20%		
	[A.29] Extorsión	5	50%	50%	75%		
Proveedores de UNITRANSA S.A.	[E.19] Fugas de información	5	20%	20%	20%		
	[A.29] Extorsión	5	20%	20%	75%		
	[A.30] Ingeniería social (picaresca)	5	20%	20%	20%		
Socios UNITRANSA S.A.	[E.19] Fugas de información	10			75%		
	[A.29] Extorsión	5	20%	20%	50%		
[D] Datos/Información							
Archivos varios de UNITRANSA S.A.	[E.1] Errores de los usuarios	10	5%	50%	75%		
	[E.2] Errores del administrador	5	20%	20%	50%		
	[E.8] Difusión de software dañino	10	20%	50%	50%		
	[E.9] Errores de [re-]encaminamiento	10			20%		

Tabla 11. (Continuación)

GRUPO DE ACTIVOS UNITRANSA S.A.	CLASIFICACIÓN DE AMENAZA (MAGERIT)	FRECUENCIA DE AMENAZA	AFECTACIÓN/DIMENSION				
			D	I	C	A	T
	[E.15] Alteración accidental de la información	50		50%			
	[E.18] Destrucción de información (accidental)	5	75%				
	[E.19] Fugas de información	5			75%		
	[A.5] Suplantación de la identidad del usuario	5		50%	50%	50%	
	[A.6] Abuso de privilegios de acceso	5	20%	50%	100%		
	[A.11] Acceso no autorizado	5		50%	75%		
	[A.15] Modificación deliberada de la información	5		50%	50%		
	[A.18] Destrucción de información (intencional)	5	75%				
	[A.19] Divulgación de información	5			50%		
Archivos de respaldo de información de la empresa	[E.1] Errores de los usuarios	10	5%	20%	50%		
	[E.2] Errores del administrador	5	5%	20%	50%		
	[E.8] Difusión de software dañino	10	50%	20%	75%		
	[E.9] Errores de [re-]encaminamiento	10			20%		
	[E.15] Alteración accidental de la información	10	20%	75%	20%		
	[E.18] Destrucción de información (accidental)	5	75%				
	[E.19] Fugas de información	5			75%		
	[A.5] Suplantación de la identidad del usuario	5		50%	50%	50%	
	[A.6] Abuso de privilegios de acceso	5	20%	50%	100%		
	[A.11] Acceso no autorizado	5		50%	50%		
	[A.15] Modificación deliberada de la información	5		50%			
	[A.18] Destrucción de información (intencional)	5	50%				
	[A.19] Divulgación de información	5			50%		
Datos de configuración de equipos	[E.1] Errores de los usuarios	5	20%	20%	5%		
	[E.2] Errores del administrador	5	5%	20%	20%		
	[E.4] Errores de configuración	50	50%	75%			
	[E.8] Difusión de software dañino	10	20%	50%	75%		
	[E.15] Alteración accidental de la información	5	50%	50%			

Tabla 11. (Continuación)

GRUPO DE ACTIVOS UNITRANSA S.A.	CLASIFICACIÓN DE AMENAZA (MAGERIT)	FRECUENCIA DE AMENAZA	AFECTACIÓN/DIMENSION				
			D	I	C	A	T
	[E.18] Destrucción de información (accidental)	5	20%				
	[E.19] Fugas de información	5			50%		
	[E.21] Errores de mantenimiento / actualización de programas (software)	5	20%	20%			
	[A.6] Abuso de privilegios de acceso	5	20%	20%	50%		
	[A.11] Acceso no autorizado	5		50%	20%		
	[A.15] Modificación deliberada de la información	5		20%			
	[A.18] Destrucción de información(intencional)	5	20%				
Credenciales de usuarios del sistema	[E.1] Errores de los usuarios	5	5%	75%	100%		
	[E.2] Errores del administrador	5	5%	75%	100%		
	[E.9] Errores de [re-]encaminamiento	10			20%		
	[E.15] Alteración accidental de la información	5		75%			
	[E.18] Destrucción de información (accidental)	5	75%				
	[E.19] Fugas de información	5			100%		
	[A.5] Suplantación de la identidad del usuario	5		75%	100%	100%	
	[A.11] Acceso no autorizado	5		100%	100%		
	[A.15] Modificación deliberada de la información	5		100%			
	[A.18] Destrucción de información (intencional)	5	75%				
Registro de actividad del sistema	[E.1] Errores de los usuarios	5	5%	20%	20%		
	[E.2] Errores del administrador	5	5%	20%	20%		
	[E.3] Errores de monitorización (log)	70		50%			100 %
	[E.9] Errores de [re-]encaminamiento	10			20%		
	[E.18] Destrucción de información (accidental)	5	75%				
	[E.19] Fugas de información	5			75%		
	[E.21] Errores de mantenimiento / actualización de programas (software)	5	20%	20%			

Tabla 11. (Continuación).

GRUPO DE ACTIVOS UNITRANSA S.A.	CLASIFICACIÓN DE AMENAZA (MAGERIT)	FRECUENCIA DE AMENAZA	AFECTACIÓN/DIMENSION				
			D	I	C	A	T
	[A.3] Manipulación de los registros de actividad (log)	5		50%	50%		100 %
	[A.4] Manipulación de la configuración	5	5%	20%	50%		
	[A.5] Suplantación de la identidad del usuario	5		20%	50%	50%	
	[A.6] Abuso de privilegios de acceso	5	20%	20%	50%		
	[A.11] Acceso no autorizado	5		50%	50%		
	[A.13] Repudio	10		20%			50%
	[A.18] Destrucción de información (intencional)	5	20%				
Datos de gestión de la empresa	[E.1] Errores de los usuarios	5	5%	20%	50%		
	[E.8] Difusión de software dañino	10	20%	50%	50%		
	[E.9] Errores de [re-]encaminamiento	10			20%		
	[E.15] Alteración accidental de la información	5		50%			
	[E.18] Destrucción de información (accidental)	5	100%				
	[E.19] Fugas de información	5			75%		
	[A.5] Suplantación de la identidad del usuario	5		50%	50%	75%	
	[A.6] Abuso de privilegios de acceso	5	20%	20%	75%		
	[A.11] Acceso no autorizado	5		50%	75%		
	[A.15] Modificación deliberada de la información	5		50%	50%		
	[A.18] Destrucción de información (intencional)	5	50%				
[S] Servicios							
Internet	[I.8] Fallo de servicios de comunicaciones	50	75%				
	[E.2] Errores del administrador	5	75%	20%	50%		
	[E.9] Errores de [re-]encaminamiento	10			75%		
	[E.15] Alteración accidental de la información	10		50%			
	[E.19] Fugas de información	10			50%		
	[A.5] Suplantación de la identidad del usuario	10	20%	75%	75%		
	[A.6] Abuso de privilegios de acceso	10	50%	50%	50%		
	[A.7] Uso no previsto	50	50%	50%	50%		

Tabla 11. (Continuación).

GRUPO DE ACTIVOS UNITRANSA S.A.	CLASIFICACIÓN DE AMENAZA (MAGERIT)	FRECUENCIA DE AMENAZA	AFECTACIÓN/DIMENSION				
			D	I	C	A	T
Acceso remoto a cuenta local	[I.8] Fallo de servicios de comunicaciones	50	100%				
	[E.1] Errores de los usuarios	10	5%	50%	50%		
	[E.2] Errores del administrador	5	5%	5%	5%		
	[E.9] Errores de [re-]encaminamiento	10			50%		
	[E.10] Errores de secuencia	5		20%			
	[E.15] Alteración accidental de la información	5		20%			
	[E.18] Destrucción de información	5	5%				
	[E.19] Fugas de información	5			20%		
	[E.24] Caída del sistema por agotamiento de recursos	5	5%				
	[A.5] Suplantación de la identidad del usuario	10		20%	20%	20%	
	[A.6] Abuso de privilegios de acceso	10	5%	5%	50%		
	[A.7] Uso no previsto	5	5%	5%	5%		
	[A.9] [Re-]encaminamiento de mensajes	5			5%		
	[A.10] Alteración de secuencia	5		5%			
	[A.11] Acceso no autorizado	5		5%	5%		
	[A.13] Repudio	5		5%			20%
	[A.18] Destrucción de información	5	5%				
	[A.19] Divulgación de información	5			50%		
	[A.24] Denegación de servicio	5	5%				
Correo electrónico	[I.8] Fallo de servicios de comunicaciones	10	100%				
	[E.1] Errores de los usuarios	5	5%	5%	5%		
	[E.2] Errores del administrador	5	5%	5%	5%		
	[E.9] Errores de [re-]encaminamiento	5			20%		
	[E.15] Alteración accidental de la información	5		20%			
	[E.19] Fugas de información	5			20%		
	[E.24] Caída del sistema por agotamiento de recursos	5	5%				
	[A.5] Suplantación de la identidad del usuario	10		20%	20%	20%	
	[A.7] Uso no previsto	5	5%	5%	5%		

Tabla 11. (Continuación)

GRUPO DE ACTIVOS UNITRANSA S.A.	CLASIFICACIÓN DE AMENAZA (MAGERIT)	FRECUENCIA DE AMENAZA	AFECTACIÓN/DIMENSION				
			D	I	C	A	T
	[A.9] [Re-]encaminamiento de mensajes	5			20%		
	[A.13] Repudio	5		20%			20%
	[A.19] Divulgación de información	5			20%		
	[A.24] Denegación de servicio	5	5%				
Almacenamiento de ficheros	[I.8] Fallo de servicios de comunicaciones	5	50%				
	[E.1] Errores de los usuarios	10	5%	50%	50%		
	[E.15] Alteración accidental de la información	5		20%			
	[E.18] Destrucción de información	5	5%				
	[E.19] Fugas de información	5			20%		
	[A.9] [Re-]encaminamiento de mensajes	5			5%		
	[A.11] Acceso no autorizado	5		5%	5%		
	[A.13] Repudio	5		5%			20%
	[A.18] Destrucción de información	5	5%				
	[A.19] Divulgación de información	5			50%		
	[A.24] Denegación de servicio	5	5%				
Transferencia de ficheros	[I.8] Fallo de servicios de comunicaciones	5	20%				
	[E.1] Errores de los usuarios	10	5%	20%	20%		
	[E.9] Errores de [re-]encaminamiento	10			50%		
	[E.19] Fugas de información	5			20%		
	[E.24] Caída del sistema por agotamiento de recursos	5	5%				
	[A.9] [Re-]encaminamiento de mensajes	5			5%		
	[A.10] Alteración de secuencia	5		5%			
	[A.19] Divulgación de información	5			50%		
Intercambio electrónico de datos	[I.8] Fallo de servicios de comunicaciones	10	50%				
	[E.1] Errores de los usuarios	10	5%	50%	50%		
	[E.10] Errores de secuencia	5		20%			
	[E.15] Alteración accidental de la información	5		20%			

Tabla 11. (Continuación).

GRUPO DE ACTIVOS UNITRANSA S.A.	CLASIFICACIÓN DE AMENAZA (MAGERIT)	FRECUENCIA DE AMENAZA	AFECTACIÓN/DIMENSION				
			D	I	C	A	T
	[E.18] Destrucción de información	5	5%				
	[E.19] Fugas de información	5			20%		
	[E.24] Caída del sistema por agotamiento de recursos	5	5%				
	[A.10] Alteración de secuencia	5		5%			
	[A.19] Divulgación de información	5			50%		
Servicio de directorio	[I.8] Fallo de servicios de comunicaciones	50	50%				
	[E.1] Errores de los usuarios	10	5%	50%	50%		
	[E.2] Errores del administrador	5	5%	5%	5%		
	[A.5] Suplantación de la identidad del usuario	10		20%	20%	20%	
	[A.7] Uso no previsto	5	5%	5%	5%		
	[A.9] [Re-]encaminamiento de mensajes	5			5%		
	[A.11] Acceso no autorizado	5		5%	5%		
	[A.13] Repudio	5		5%			20%
Gestión de identidades	[E.1] Errores de los usuarios	10	5%	50%	50%		
	[E.2] Errores del administrador	5	5%	5%	5%		
	[E.15] Alteración accidental de la información	5		20%			
	[E.18] Destrucción de información (accidental)	5	75%				
	[E.19] Fugas de información	5			20%		
	[A.11] Acceso no autorizado	5			20%		
	[A.18] Destrucción de información (intencional)	5	75%				
	[A.19] Divulgación de información	5			75%		
Gestión de privilegios	[E.1] Errores de los usuarios	10	5%	50%	50%		
	[E.2] Errores del administrador	5	5%	5%	5%		
	[E.15] Alteración accidental de la información	5		20%			
	[E.18] Destrucción de información (accidental)	5	75%				
	[E.19] Fugas de información	5			20%		
	[A.11] Acceso no autorizado	5			20%		
	[A.18] Destrucción de información (intencional)	5	75%				

Tabla 11. (Continuación).

GRUPO DE ACTIVOS UNITRANSA S.A.	CLASIFICACIÓN DE AMENAZA (MAGERIT)	FRECUENCIA DE AMENAZA	AFECTACIÓN/DIMENSION				
			D	I	C	A	T
	[A.19] Divulgación de información	5			75%		
[HW] Hardware							
Equipo Servidor de Bases de Datos	[N.1] Fuego	5	100%				
	[N.2] Daños por agua (inundaciones)	5	100%				
	[I.2] Daños por agua (escapes, fugas)	5	100%				
	[I.6] Corte del suministro eléctrico	5	5%				
	[I.7] Condiciones inadecuadas de temperatura o humedad	5	5%				
	[E.2] Errores del administrador	5	5%	50%	50%		
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	100%	50%	50%		
	[I.5] Avería de origen físico o lógico	50	50%	20%	20%		
	[E.24] Caída del sistema por agotamiento de recursos	5	100%				
	[E.25] Pérdida de equipos	5	100%		100%		
	[A.6] Abuso de privilegios de acceso	5	20%	75%	100%		
	[A.7] Uso no previsto	5	20%	5%	5%		
	[A.11] Acceso no autorizado	5		100%	100%		
	[A.23] Manipulación de los equipos	10	50%	50%	50%		
	[A.24] Denegación de servicio	10	50%				
	[A.25] Robo	5	100%		100%		
	[A.26] Ataque destructivo	5	100%				
Computadora de Gerencia	[N.1] Fuego	5	100%				
	[N.2] Daños por agua (inundaciones naturales)	5	100%				
	[I.2] Daños por agua (escapes, fugas)	5	100%				
	[I.5] Avería de origen físico y lógico	50	20%	20%	20%		
	[I.6] Corte del suministro eléctrico	5	5%				

Tabla 11. (Continuación).

GRUPO DE ACTIVOS UNITRANSA S.A.	CLASIFICACIÓN DE AMENAZA (MAGERIT)	FRECUENCIA DE AMENAZA	AFECTACIÓN/DIMENSION				
			D	I	C	A	T
	[I.7] Condiciones inadecuadas de temperatura o humedad	5	5%				
	[E.2] Errores del administrador	5	5%	20%	75%		
	[I.7] Condiciones inadecuadas de temperatura o humedad						
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	20%	20%	20%		
	[I.5] Avería de origen físico o lógico	10	50%				
	[E.24] Caída del sistema por agotamiento de recursos	5	5%				
	[E.25] Pérdida de equipos	5	100%		100%		
	[A.6] Abuso de privilegios de acceso	5	20%	50%	100%		
	[A.7] Uso no previsto	5	5%	5%	5%		
	[A.11] Acceso no autorizado	5		50%	100%		
	[A.23] Manipulación de los equipos	5	20%		100%		
	[A.24] Denegación de servicio	5	20%				
	[A.25] Robo	5	50%		100%		
	[A.26] Ataque destructivo	5	50%				
Computadora de Dpto. Jurídico	[N.1] Fuego	5	100%				
	[N.2] Daños por agua (inundaciones)	5	100%				
	[I.2] Daños por agua (inundaciones, escapes)	5	100%				
	[I.5] Avería de origen físico o lógico	50	20%	20%	20%		
	[I.6] Corte del suministro eléctrico	5	5%				
	[E.2] Errores del administrador	5	5%	20%	75%		
	[I.7] Condiciones inadecuadas de temperatura o humedad	5	20%				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	50%				
	[E.24] Caída del sistema por agotamiento de recursos	5	20%				

Tabla 11. (Continuación).

GRUPO DE ACTIVOS UNITRANSA S.A.	CLASIFICACIÓN DE AMENAZA (MAGERIT)	FRECUENCIA DE AMENAZA	AFECTACIÓN/DIMENSION				
			D	I	C	A	T
	[E.25] Pérdida de equipos	5	100%		100%		
	[A.6] Abuso de privilegios de acceso	5	20%	75%	100%		
	[A.7] Uso no previsto	5	20%	20%	20%		
	[A.11] Acceso no autorizado	5		75%	100%		
	[A.23] Manipulación de los equipos	5	50%		100%		
	[A.24] Denegación de servicio	5	20%				
	[A.25] Robo	5	50%		100%		
	[A.26] Ataque destructivo	5	75%				
Puestos de trabajo	[N.1] Fuego	5	100%				
	[N.2] Daños por agua (inundaciones)	5	100%				
	[I.2] Daños por agua (escapes, fugas)	5	100%				
	[I.5] Avería de origen físico o lógico	50	20%	20%	20%		
	[I.6] Corte del suministro eléctrico	5	5%				
	[I.7] Condiciones inadecuadas de temperatura o humedad	5	20%				
	[E.2] Errores del administrador	5	5%	5%	20%		
	[E.23] Errores de mantenimiento/actualización de equipos (hardware)	5	50%				
	[E.24] Caída del sistema por agotamiento de recursos	5	20%				
	[E.25] Pérdida de equipos	5	50%	50%	50%		
	[A.6] Abuso de privilegios de acceso	10	20%	50%	75%		
	[A.7] Uso no previsto	50	50%	50%	50%		
	[A.11] Acceso no autorizado	10		50%	50%		
	[A.23] Manipulación de los equipos	10	20%	20%	20%		
	[A.24] Denegación de servicio	5	20%				
	[A.25] Robo	5	20%	20%	20%		
	[A.26] Ataque destructivo	10	20%				
	[N.1] Fuego	5	100%				
	[N.2] Daños por agua (inundaciones)	5	100%				

Tabla 11. (Continuación).

GRUPO DE ACTIVOS UNITRANSA S.A.	CLASIFICACIÓN DE AMENAZA (MAGERIT)	FRECUENCIA DE AMENAZA	AFECTACIÓN/DIMENSION				
			D	I	C	A	T
Impresora	[I.2] Daños por agua (accidentalidad)	5	50%				
	[I.5] Avería de origen físico o lógico	50	5%				
	[I.6] Corte del suministro eléctrico	5	5%				
	[I.7] Condiciones inadecuadas de temperatura o humedad	5	50%				
	[E.2] Errores del administrador	5	5%	5%	5%		
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	75%				
	[E.24] Caída del sistema por agotamiento de recursos	10	50%				
	[E.25] Pérdida de equipos	5	5%		5%		
	[A.7] Uso no previsto	5	50%	5%	5%		
	[A.23] Manipulación de los equipos	5	5%		5%		
	[A.25] Robo	5	5%		5%		
	[A.26] Ataque destructivo	10	20%				
Firewall	[N.1] Fuego	5	100%				
	[N.2] Daños por agua (inundaciones)	5	100%				
	[I.2] Daños por agua (escapes, fugas)	5	100%				
	[I.5] Avería de origen físico o lógico	5	5%				
	[I.6] Corte del suministro eléctrico	5	20%				
	[E.2] Errores del administrador	5	5%	5%	5%		
	[I.7] Condiciones inadecuadas de temperatura o humedad	5	50%				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	20%				
	[E.25] Pérdida de equipos	5	50%		5%		
	[A.23] Manipulación de los equipos	5	20%		20%		
	[A.25] Robo	5	5%		5%		
	[A.26] Ataque destructivo	5	5%				

Tabla 11. (Continuación).

GRUPO DE ACTIVOS UNITRANSA S.A.	CLASIFICACIÓN DE AMENAZA (MAGERIT)	FRECUENCIA DE AMENAZA	AFECTACIÓN/DIMENSION				
			D	I	C	A	T
Switch Ethernet Gigabit Linksys SE4008 WRT de 8 puertos (1er. Piso).	[N.1] Fuego	5	100%				
	[N.2] Daños por agua (inundaciones)	5	100%				
	[I.2] Daños por agua (escapes en el acueducto)	5	50%				
	[I.5] Avería de origen físico o lógico	10	20%				
	[I.6] Corte del suministro eléctrico	5	5%				
	[I.7] Condiciones inadecuadas de temperatura o humedad	5	5%				
	[E.2] Errores del administrador	5	5%	5%	5%		
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	50%				
	[E.25] Pérdida de equipos	5	50%		5%		
	[A.23] Manipulación de los equipos	5	20%	20%	20%		
	[A.25] Robo	5	5%		5%		
	[A.26] Ataque destructivo	5	5%				
Switch Linksys SE3016 de 16 puertos (2º. Piso).	[N.1] Fuego	5	100%				
	[N.2] Daños por agua (inundaciones)	5	100%				
	[I.2] Daños por agua	5	20%				
	[I.5] Avería de origen físico o lógico	10	20%	20%			
	[I.6] Corte del suministro eléctrico	5	5%				
	[I.7] Condiciones inadecuadas de temperatura o humedad	5	5%				
	[E.2] Errores del administrador	5	5%	5%	5%		
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	50%				

Tabla 11. (Continuación).

GRUPO DE ACTIVOS UNITRANSA S.A.	CLASIFICACIÓN DE AMENAZA (MAGERIT)	FRECUENCIA DE AMENAZA	AFECTACIÓN/DIMENSION				
			D	I	C	A	T
	[E.25] Pérdida de equipos	5	20%		5%		
	[A.23] Manipulación de los equipos	5	20%	20%	20%		
	[A.25] Robo	5	5%				
	[A.26] Ataque destructivo	5	5%				
Switch Linksys SE4008 WRT de 8 puertos (3er. Piso)	[N.1] Fuego	5	100%				
	[N.2] Daños por agua (inundaciones)	5	100%				
	[I.2] Daños por agua (escapes, fugas)	5	100%				
	[I.5] Avería de origen físico o lógico	10	20%	20%			
	[I.6] Corte del suministro eléctrico	5	5%				
	[I.7] Condiciones inadecuadas de temperatura o humedad	5	5%				
	[E.2] Errores del administrador	5	5%	5%	5%		
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	50%				
	[E.25] Pérdida de equipos	10	20%		5%		
	[A.23] Manipulación de los equipos	5	20%		20%		
	[A.25] Robo	5	20%				
	[A.26] Ataque destructivo	5	5%				
Router Netgear 4g Lte Router Lg2200d	[N.1] Fuego	5	100%				
	[N.2] Daños por agua (inundaciones)	5	100%				
	[I.2] Daños por agua (fugas, escapes)	5	100%				
	[I.5] Avería de origen físico o lógico	10	50%	20%	50%		
	[I.6] Corte del suministro eléctrico	5	5%				
	[I.7] Condiciones inadecuadas de temperatura o humedad	5	20%				
	[E.2] Errores del administrador	5	75%	20%	20%		

Tabla 11. (Continuación).

GRUPO DE ACTIVOS UNITRANSA S.A.	CLASIFICACIÓN DE AMENAZA (MAGERIT)	FRECUENCIA DE AMENAZA	AFECTACIÓN/DIMENSION				
			D	I	C	A	T
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	75%	50%	50%		
	[E.25] Pérdida de equipos	5	75%		5%		
	[A.5] Suplantación de la identidad del usuario	5		20%	50%	100%	
	[A.6] Abuso de privilegios de acceso	5	20%	50%	50%		
	[A.11] Acceso no autorizado	10		20%	50%		
	[A.23] Manipulación de los equipos	10	50%	50%	50%		
	[A.24] Denegación de servicio	5	50%				
	[A.25] Robo	5	50%		5%		
	[A.26] Ataque destructivo	5	50%				
[SW]Aplicaciones							
Servidor de aplicaciones utilizadas en la empresa	[I.5] Avería de origen físico o lógico	5	50%	50%	50%		
	[E.1] Errores de los usuarios	10	20%	50%	50%		
	[E.2] Errores del administrador	5	75%	20%	20%		
	[E.9] Errores de [re-]encaminamiento	10			50%		
	[E.20] Vulnerabilidades de los programas (software)	5	50%	50%	75%		
	[E.21] Errores de mantenimiento / actualización de programas (software)	5	75%	75%	50%		
	[A.5] Suplantación de la identidad del usuario	5		20%	100%	100%	
	[A.6] Abuso de privilegios de acceso	5	20%	50%	100%		
	[A.8] Difusión de software dañino	10	20%	50%	50%		
	[A.11] Acceso no autorizado	5		75%	75%		
	[A.18] Destrucción de información (intencional)	5	50%				
	[A.22] Manipulación de programas	5	50%	50%	20%		
	[A.24] Denegación de servicio	5	75%				
	[I.5] Avería de origen físico o lógico	5	50%				
	[E.1] Errores de los usuarios	5	20%	50%	50%		
	[E.2] Errores del administrador	5	75%	20%	5%		

Tabla 11. (Continuación).

GRUPO DE ACTIVOS UNITRANSA S.A.	CLASIFICACIÓN DE AMENAZA (MAGERIT)	FRECUENCIA DE AMENAZA	AFECTACIÓN/DIMENSION				
			D	I	C	A	T
Manejador de Base de Datos Oracle	[E.9] Errores de [re-]encaminamiento	10			50%		
	[E.18] Destrucción de información	5	100%				
	[E.19] Fugas de información	5			100%		
	[E.20] Vulnerabilidades de los programas (software)	5	75%	50%	75%		
	[E.21] Errores de mantenimiento / actualización de programas (software)	5	75%	75%	50%		
	[A.5] Suplantación de la identidad del usuario	5	20%	50%	100%		
	[A.6] Abuso de privilegios de acceso	5	50%	50%	100%		
	[A.8] Difusión de software dañino	10	20%	50%	50%		
	[A.11] Acceso no autorizado	5		100%	100%		
	[A.18] Destrucción de información (intencional)	5	100%				
	[A.19] Divulgación de información	5			50%		
	[A.22] Manipulación de programas	5	50%	75%	100%		
	[A.24] Denegación de servicio	5	75%				
Sistema Operativo Windows 7 Profesional	[I.5] Avería de origen físico o lógico	5	50%	50%	50%		
	[E.1] Errores de los usuarios	10	50%	50%	50%		
	[E.2] Errores del administrador	5	5%	20%	20%		
	[E.9] Errores de [re-]encaminamiento	10			50%		
	[E.18] Destrucción de información	5	50%				
	[E.20] Vulnerabilidades de los programas (software)	5	50%	50%	75%		
	[E.21] Errores de mantenimiento / actualización de programas (software)	10	50%	50%	20%		
	[A.5] Suplantación de la identidad del usuario	5	20%	50%	75%		
	[A.6] Abuso de privilegios de acceso	5	20%	50%	75%		
	[A.8] Difusión de software dañino	10	20%	50%	50%		
	[A.11] Acceso no autorizado	10		50%	50%		
	[A.18] Destrucción de información (intencional)	5	20%				
	[A.22] Manipulación de programas	5	20%	20%	20%		

Tabla 11. (Continuación).

GRUPO DE ACTIVOS UNITRANSA S.A.	CLASIFICACIÓN DE AMENAZA (MAGERIT)	FRECUENCIA DE AMENAZA	AFECTACIÓN/DIMENSION				
			D	I	C	A	T
Sistema Operativo Windows 8	[I.5] Avería de origen físico o lógico	10	50%	20%	20%		
	[E.1] Errores de los usuarios	10	50%	20%	50%		
	[E.2] Errores del administrador	5	5%	20%	20%		
	[E.9] Errores de [re-]encaminamiento	10			50%		
	[E.18] Destrucción de información (accidental)	5	50%				
	[E.20] Vulnerabilidades de los programas (software)	5	50%	50%	75%		
	[E.21] Errores de mantenimiento / actualización de programas (software)	10	50%	50%			
	[A.5] Suplantación de la identidad del usuario	5	20%	50%	50%		
	[A.6] Abuso de privilegios de acceso	5	20%	50%	75%		
	[A.8] Difusión de software dañino	10	20%	50%	50%		
	[A.11] Acceso no autorizado	10		50%	50%		
	[A.18] Destrucción de información (intencional)	5	50%				
	[A.22] Manipulación de programas	5	20%	20%	20%		
Sistema Operativo Windows XP	[I.5] Avería de origen físico o lógico	70	75%	50%	50%		
	[E.1] Errores de los usuarios	10	20%	50%	50%		
	[E.2] Errores del administrador	5	5%	20%	20%		
	[E.9] Errores de [re-]encaminamiento	10			50%		
	[E.18] Destrucción de información (accidental)	5	50%				
	[E.20] Vulnerabilidades de los programas (software)	70	50%	50%	75%		
	[E.21] Errores de mantenimiento / actualización de programas (software)	70	50%	50%	75%		
	[A.5] Suplantación de la identidad del usuario	5	20%	50%	50%		
	[A.6] Abuso de privilegios de acceso	5	20%	50%	75%		
	[A.8] Difusión de software dañino	50	20%	50%	50%		
	[A.11] Acceso no autorizado	10		75%	75%		
	[A.18] Destrucción de información (intencional)	5	20%				

Tabla 11. (Continuación).

GRUPO DE ACTIVOS UNITRANSA S.A.	CLASIFICACIÓN DE AMENAZA (MAGERIT)	FRECUENCIA DE AMENAZA	AFECTACIÓN/DIMENSION				
			D	I	C	A	T
	[A.22] Manipulación de programas	10	50%	50%	50%		
Editor HTML: Adobe Dreamweaver	[I.5] Avería de origen físico o lógico	50	50%				
	[E.1] Errores de los usuarios	5	5%	5%	5%		
	[E.2] Errores del administrador	5	20%	20%	5%		
	[E.9] Errores de [re-]encaminamiento	10			50%		
	[A.18] Destrucción de información (intencional)	5	20%				
	[A.22] Manipulación de programas	5	20%	20%	20%		
Plantillas web: Artister	[I.5] Avería de origen físico o lógico	5	50%				
	[E.1] Errores de los usuarios	5	20%	5%	5%		
	[E.2] Errores del administrador	5	5%	5%	5%		
	[E.9] Errores de [re-]encaminamiento	10			50%		
	[E.20] Vulnerabilidades de los programas (software)	5	20%	20%	50%		
	[A.18] Destrucción de información (intencional)	5	20%				
Editor de imágenes web: Adobe Fireworks	[I.5] Avería de origen físico o lógico	5	20%				
	[E.1] Errores de los usuarios	5	20%	5%	5%		
	[E.2] Errores del administrador	5	5%	5%	5%		
	[E.9] Errores de [re-]encaminamiento	10			50%		
	[A.18] Destrucción de información (intencional)	5	20%				
Diseño de logos: Logo Creator	[I.5] Avería de origen físico o lógico	5	20%				
	[E.1] Errores de los usuarios	5	20%	5%	5%		
	[E.2] Errores del administrador	5	5%	5%	5%		
	[E.9] Errores de [re-]encaminamiento	10			50%		
	[A.18] Destrucción de información (intencional)	5	20%				
Cliente FTP: Filezilla	[I.5] Avería de origen físico o lógico	5	20%				
	[E.1] Errores de los usuarios	5	20%	5%	5%		
	[E.2] Errores del administrador	5	5%	5%	5%		
	[E.9] Errores de [re-]encaminamiento	10			75%		

Tabla 11. (Continuación).

GRUPO DE ACTIVOS UNITRANSA S.A.	CLASIFICACIÓN DE AMENAZA (MAGERIT)	FRECUENCIA DE AMENAZA	AFECTACIÓN/DIMENSION				
			D	I	C	A	T
	[A.22] Manipulación de programas	5	50%	20%	50%		
Aplicaciones de desarrollo propio	[I.5] Avería de origen físico o lógico	5	20%				
	[E.1] Errores de los usuarios	5	20%	5%	5%		
	[E.2] Errores del administrador	5	5%	20%	20%		
	[E.9] Errores de [re-]encaminamiento	10			20%		
	[E.18] Destrucción de información (accidental)	5	50%				
	[E.20] Vulnerabilidades de los programas (software)	5	50%	50%	50%		
	[E.21] Errores de mantenimiento / actualización de programas (software)	5	50%	50%			
	[A.5] Suplantación de la identidad del usuario	5	20%	20%	100%		
	[A.8] Difusión de software dañino	5	5%	20%	50%		
	[A.18] Destrucción de información (intencional)	5	20%				
	[A.19] Divulgación de información	5			50%		
	[A.22] Manipulación de programas	5	20%	20%	20%		
Antivirus	[I.5] Avería de origen físico o lógico	5	50%				
	[E.1] Errores de los usuarios	5	20%	50%	50%		
	[E.2] Errores del administrador	5	5%	75%	75%		
	[E.21] Errores de mantenimiento / actualización de programas (software)	5	50%	75%	20%		
	[A.18] Destrucción de información (intencional)	5	50%				
	[A.22] Manipulación de programas	5	20%	20%	50%		
[AUX]Equipamiento auxiliar							
	[N.1] Fuego	5	100%				
	[N.2] Daños por agua (inundaciones)	5	100%				
	[I.2] Daños por agua (fugas, escapes)	5	100%				

Tabla 11. (Continuación).

GRUPO DE ACTIVOS UNITRANSA S.A.	CLASIFICACIÓN DE AMENAZA (MAGERIT)	FRECUENCIA DE AMENAZA	AFECTACIÓN/DIMENSION				
			D	I	C	A	T
Sistema de alimentación ininterrumpidaUPS de la serie UPO22	[I.5] Avería de origen físico o lógico	10	5%	5%			
	[I.6] Corte del suministro eléctrico	5	5%				
	[I.7] Condiciones inadecuadas de temperatura o humedad	5	5%				
	[E.2] Errores del administrador	5	5%	5%	5%		
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	20%				
	[E.25] Pérdida de equipos	5	20%		5%		
	[A.23] Manipulación de los equipos	5	5%	5%			
	[A.25] Robo	5	5%				
	[A.26] Ataque destructivo	5	5%				
	[I.1] Fuego	5	100%				
	[I.2] Daños por agua	5	5%				
	[I.5] Avería de origen físico o lógico	5	5%				
	[I.6] Corte del suministro eléctrico	5	5%				
	[I.7] Condiciones inadecuadas de temperatura o humedad	5	5%				
	[E.2] Errores del administrador	5	20%	5%	5%		
	[E.25] Pérdida de equipos	5	5%		5%		
	[A.25] Robo	5	5%		5%		
Equipos de climatización	[N.1] Fuego	5	100%				
	[N.2] Daños por agua (inundaciones)	5	100%				
	[I.2] Daños por agua	5	50%				
	[I.5] Avería de origen físico o lógico	10	5%				
	[I.6] Corte del suministro eléctrico	5	20%				
	[I.7] Condiciones inadecuadas de temperatura o humedad	5	50%				

Tabla 11. (Continuación).

GRUPO DE ACTIVOS UNITRANSA S.A.	CLASIFICACIÓN DE AMENAZA (MAGERIT)	FRECUENCIA DE AMENAZA	AFECTACIÓN/DIMENSION				
			D	I	C	A	T
	[E.2] Errores del administrador	5	5%	5%	5%		
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	20%				
	[E.25] Pérdida de equipos	5	20%		5%		
	[A.23] Manipulación de los equipos	5	5%				
	[A.25] Robo	5	20%		5%		
	[A.26] Ataque destructivo	5	5%				
Generador de energia	[N.1] Fuego	5	50%				
	[N.2] Daños por agua	5	50%				
	[I.2] Daños por agua (inundaciones)	5	100%				
	[I.5] Avería de origen físico o lógico	10	20%				
	[I.7] Condiciones inadecuadas de temperatura o humedad	5	20%				
	[E.2] Errores del administrador	5	50%	5%	5%		
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	50%				
	[E.25] Pérdida de equipos	5	50%		5%		
	[A.23] Manipulación de los equipos	5	20%		20%		
	[A.25] Robo	5	20%		5%		
	[A.26] Ataque destructivo	5	20%				
[COM]Redes de comunicación							
Red local de UNITRANSA S.A.	[I.8] Fallo de servicios de comunicaciones	70	75%	50%	75%		
	[E.2] Errores del administrador	5	20%	50%	50%		
	[E.9] Errores de [re-]encaminamiento	10			75%		
	[E.15] Alteración accidental de la información	10		50%			
	[E.19] Fugas de información	50			50%		
	[A.5] Suplantación de la identidad del usuario	10	20%	20%	100%		
	[A.6] Abuso de privilegios de acceso	10	50%	50%	75%		

Tabla 11. (Continuación).

GRUPO DE ACTIVOS UNITRANSA S.A.	CLASIFICACIÓN DE AMENAZA (MAGERIT)	FRECUENCIA DE AMENAZA	AFECTACIÓN/DIMENSION				
			D	I	C	A	T
	[A.7] Uso no previsto	50	50%	50%	50%		
	[A.9] [Re-]encaminamiento de mensajes	10			75%		
	[A.11] Acceso no autorizado	50		75%	75%		
	[A.14] Interceptación de información (escucha)	70			100%		
[L]Instalaciones							
Edificio sede de la empresa.	[N.1] Fuego	5	100%				
	[N.2] Daños por agua (inundaciones)	5	100%				
	[I.2] Daños por agua (accidental)	5	50%				
	[E.19] Fugas de información	5			50%		
	[A.11] Acceso no autorizado	5		20%	20%		
	[A.26] Ataque destructivo	5	20%				
	[A.27] Ocupación enemiga	5	100%		50%		

Fuente: Autor.

7. ESTIMACIÓN DEL ESTADO DE RIESGO DEL SISTEMA

El análisis de riesgos es la herramienta que determina la exposición real a los riesgos que están expuestos los activos de información en una organización. Se busca con esto, individualizar los riesgos a través de la identificación de sus elementos y obtener el riesgo total para posteriormente establecer el riesgo residual luego de establecidas las salvaguardas.

El riesgo total está dado por dos factores: el impacto sobre el activo, que corresponde a la degradación ocasionada por la materialización de la amenaza y la probabilidad de ocurrencia de dicha amenaza.

Obtener el impacto sobre los activos es posible a través de la utilización de tablas de doble entrada. Los activos catalogados con impacto Muy Alto (MA) requieren de atención prioritaria.

Tabla12. Estimación impacto

Impacto		**degradación**		
		1%	10%	10%
valor	MA	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

Fuente: MAGERIT_V3

El impacto, la probabilidad y el riesgo se modelan por medio de la Tabla 14 de escalas cualitativas.

Tabla13. Escala de impacto, probabilidad y riesgo

ESCALAS		
Impacto	Probabilidad	Riesgo
MA: muy alto	MA: prácticamente seguro	MA: crítico
A: alto	A: probable	A: importante
M: medio	M: posible	M: apreciable
B: bajo	B: poco probable	B: bajo
MB: muy bajo	MB: muy raro	MB: despreciable

Fuente: MAGERIT_V3

Calcular el riesgo es factible combinando impacto y frecuencia, como lo muestra la Tabla14.

Tabla14. Combinación impacto-probabilidad.

Riesgo		Probabilidad				
		MB	B	M	A	MA
Impacto	MA	B	M	A	MA	MA
	A	B	M	A	A	MA
	M	MB	B	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Fuente: MAGERIT_ V3

7.1 CONCLUSIONES DEL ANÁLISIS DE RIESGOS DE LOS ACTIVOS DE INFORMACIÓN

Efectuado el análisis de riesgos de los activos de información de UNITRANSA S.A., se puede concluir:

- El 92% de los activos de información presentan un riesgo bajo o muy bajo.
- Solo el 8% de los activos presentan riesgo de amenaza muy alta en alguna de sus dimensiones.
- El activo Windows XP constituye una vulnerabilidad muy alta que pondría en riesgo a la información almacenada y/o procesada en equipos con este sistema operativo, lo que requiere con urgencia migrar a plataformas más modernas y seguras luego del anuncio de Microsoft de finalizar el soporte técnico a esta versión de Windows.
- La red LAN de la empresa, al igual que la conexión a Internet constituyen el segundo factor de riesgo de la información de la empresa; demanda con premura la adopción de medidas de seguridad en el uso de la red interna y la conexión con la red global.

7.2 MATRIZ DE RIESGOS

La Matriz de Riesgos de UNITRANSA S.A. no muestra un análisis detallado de los riesgos a los que están expuestos los activos de información de la empresa, ni el impacto real que causaría la materialización de las amenazas, más bien vislumbra un panorama aproximado de las situaciones más relevantes que podrían afectar la información de la organización.

Un profundo análisis de riesgos consiste en determinar las amenazas y vulnerabilidades que afectan a cada uno de los activos de información de manera independiente, especificando los posibles daños y consecuencias, para de esta manera establecer los controles necesarios para contrarrestar sus efectos. La implementación de este tipo de análisis conllevaría una inversión importante en recursos financieros y técnicos que una PYME difícilmente está dispuesta a asumir.

El objetivo de la Matriz de Riesgos es ubicar y mostrar los Activos de Información más representativos que estén en peligro de ser impactados negativamente y con base a esta premisa tomar las medidas necesarias para evitar, mitigar, transferir o en caso extremo eliminar el activo.

El riesgo del activo de información está dado por el producto entre la Probabilidad de Amenaza y el impacto sobre el activo.

Lo importante de la realización de la Matriz de Riesgos es la visión macro de los Activos más vulnerables y las medidas a tomarse prioritariamente luego del análisis de la gráfica cuando el objetivo es combatir los riesgos más graves.

La Matriz de riesgos se obtiene a partir de las tablas de probabilidad estándar e impacto estándar, como se muestran a continuación.

Tabla15. Probabilidad estándar

VULNERABILIDAD	RANGO	VALOR ESTANDAR
Frecuencia muy alta	1 vez al día	5
Frecuencia alta	1 vez cada semana	4
Frecuencia media	1 vez cada 2 meses	3
Frecuencia baja	1 vez cada 6 meses	2
Frecuencia muy baja	1 vez cada año	1

Fuente: Tabares Rendón, J. D., implementación de un sistema de gestión de seguridad informática en la confederación de cámaras de comercio confecámaras. (2015). UNAD.

Tabla16. Impacto estándar.

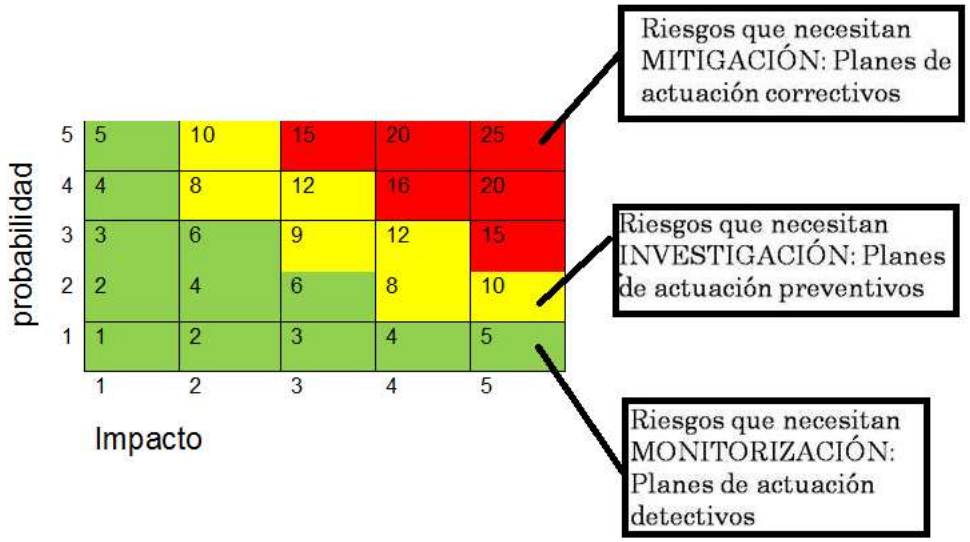
IMPACTO	CRITERIO	VALOR ESTANDAR
Extremo	Daño extremadamente grave	5
Muy alto	Daño muy grave	4
Alto	Daño grave	3
Medio	Daño importante	2
Bajo	Daño menor	1
Despreciable	Irrelevante a efectos prácticos	0

Fuente: Tabares Rendón, J. D., implementación de un sistema de gestión de seguridad informática en la confederación de cámaras de comercio confecámaras. (2015). UNAD

El nivel de riesgos está agrupado en tres rangos que para una mejor compresión se muestra en tres colores (Tabla 17).

- Riesgo Bajo. Valores entre 1 y 6 (color verde).
- Riesgo Medio. Valores entre 8 y 12 (color amarillo).
- Riesgo Alto. Valores entre 15 y 25 (color rojo).

Tabla 17. Esquema de valorización de riesgos.



Fuente: Benavides Ruano, M. del C. y Solarte Solarte, F. N. J. (2012). Curso Riesgos y Control Informático. Código 233004. unad.edu.co

Tabla18. Matriz de riesgos.

NOMBRE Y DESCRIPCION DEL ACTIVO	PROBABILIDAD DE LA AMENAZA		IMPACTO EN SUS DIMENSIONES					RIESGO EN SUS DIMENSIONES				
	AMENAZA SEGÚN MAGERIT	VALOR	D	I	C	A	T	D	I	C	A	T
[INFO_SOC] Información Socios y proveedores	[E.1] Errores de los usuarios	2	3	5	5	5	3	6	10	10	10	6
	[E.2] Errores del administrador	2	3	5	5	5	3	6	10	10	10	6
	[E.15] Alteración accidental de la información	3	3	5	5	5	3	9	15	15	15	9
	[E.18] Destrucción de información (accidental)	1	3	5	5	5	3	3	5	5	5	3
	[E.19] Fugas de información	2	3	5	5	5	3	6	10	10	10	6
	[A.5] Suplantación de la identidad del usuario	1	3	5	5	5	3	3	5	5	5	3
	[A.6] Abuso de privilegios de acceso	1	3	5	5	5	3	3	5	5	5	3
	[A.11] Acceso no autorizado	2	3	5	5	5	3	6	10	10	10	6
	[A.15] Modificación deliberada de la información	1	3	5	5	5	3	3	5	5	5	3
	[A.18] Destrucción de información (intencional)	1	3	5	5	5	3	3	5	5	5	3
	[A.19] Divulgación de información	2	3	5	5	5	3	6	10	10	10	6
[INFO_NIIF] Información Contable de la empresa	[E.1] Errores de los usuarios	2	5	5	5	5	3	10	10	10	10	6
	[E.2] Errores del administrador	2	5	5	5	5	3	10	10	10	10	6
	[E.8] Difusión de software dañino	4	5	5	5	5	3	20	20	20	20	12
	[E.15] Alteración accidental de la información	3	5	5	5	5	3	15	15	15	15	9
	[E.18] Destrucción de información (accidental)	1	5	5	5	5	3	5	5	5	5	3
	[E.19] Fugas de información	2	5	5	5	5	3	10	10	10	10	6
	[A.5] Suplantación de la identidad del usuario	1	5	5	5	5	3	5	5	5	5	3
	[A.6] Abuso de privilegios de acceso	1	5	5	5	5	3	5	5	5	5	3

Tabla 18. (Continuación).

NOMBRE Y DESCRIPCION DEL ACTIVO	PROBABILIDAD DE LA AMENAZA		IMPACTO EN SUS DIMENSIONES					RIESGO EN SUS DIMENSIONES				
	AMENAZA SEGÚN MAGERIT	VALOR	D	I	C	A	T	D	I	C	A	T
	[A.11] Acceso no autorizado	2	5	5	5	5	3	10	10	10	10	6
	[A.15] Modificación deliberada de la información	1	5	5	5	5	3	5	5	5	5	3
	[A.18] Destrucción de información (intencional)	1	5	5	5	5	3	5	5	5	5	3
	[A.19] Divulgación de información	2	5	5	5	5	3	10	10	10	10	6
[COD_FTE] Código fuente de aplicativos.	[E.1] Errores de los usuarios	1	3	3	3	3	2	3	3	3	3	2
	[E.2] Errores del administrador	1	3	3	3	3	2	3	3	3	3	2
	[E.8] Difusión de software dañino	2	3	3	3	3	2	6	6	6	6	4
	[E.15] Alteración accidental de la información	1	3	3	3	3	2	3	3	3	3	2
	[E.18] Destrucción de información (accidental)	1	3	3	3	3	2	3	3	3	3	2
	[E.19] Fugas de información	1	3	3	3	3	2	3	3	3	3	2
	[A.5] Suplantación de la identidad del usuario	1	3	3	3	3	2	3	3	3	3	2
	[A.6] Abuso de privilegios de acceso	1	3	3	3	3	2	3	3	3	3	2
	[A.11] Acceso no autorizado	1	3	3	3	3	2	3	3	3	3	2
	[A.15] Modificación deliberada de la información	1	3	3	3	3	2	3	3	3	3	2
	[A.18] Destrucción de información(intencional)	1	3	3	3	3	2	3	3	3	3	2
	[A.19] Divulgación de información	1	3	3	3	3	2	3	3	3	3	2
[DOC_PROY] Documentación de proyectos	[E.1] Errores de los usuarios	3	5	4	5	2	2	15	12	15	6	6
	[E.2] Errores del administrador	1	5	4	5	2	2	5	4	5	2	2

Tabla 18. (Continuación).

NOMBRE Y DESCRIPCION DEL ACTIVO	PROBABILIDAD DE LA AMENAZA		IMPACTO EN SUS DIMENSIONES					RIESGO EN SUS DIMENSIONES				
	AMENAZA SEGÚN MAGERIT	VALOR	D	I	C	A	T	D	I	C	A	T
	[E.8] Difusión de software dañino	2	5	4	5	2	2	10	8	10	4	4
	[E.15] Alteración accidental de la información	3	5	4	5	2	2	15	12	15	6	6
	[E.18] Destrucción de información (accidental)	1	5	4	5	2	2	5	4	5	2	2
	[E.19] Fugas de información	1	5	4	5	2	2	5	4	5	2	2
	[A.5] Suplantación de la identidad del usuario	1	5	4	5	2	2	5	4	5	2	2
	[A.6] Abuso de privilegios de acceso	1	5	4	5	2	2	5	4	5	2	2
	[A.11] Acceso no autorizado	1	5	4	5	2	2	5	4	5	2	2
	[A.15] Modificación deliberada de la información	1	5	4	5	2	2	5	4	5	2	2
	[A.18] Destrucción de información (intencional)	1	5	4	5	2	2	5	4	5	2	2
	[A.19] Divulgación de información	1	5	4	5	2	2	5	4	5	2	2
[DOC_EST] Documentación estratégica	[E.1] Errores de los usuarios	3	3	4	5	2	2	9	12	15	6	6
	[E.2] Errores del administrador	1	3	4	5	2	2	3	4	5	2	2
	[E.8] Difusión de software dañino	2	3	4	5	2	2	6	8	10	4	4
	[E.15] Alteración accidental de la información	2	3	4	5	2	2	6	8	10	4	4
	[E.18] Destrucción de información (accidental)	1	3	4	5	2	2	3	4	5	2	2
	[E.19] Fugas de información	1	3	4	5	2	2	3	4	5	2	2
	[A.5] Suplantación de la identidad del usuario	1	3	4	5	2	2	3	4	5	2	2
	[A.6] Abuso de privilegios de acceso	1	3	4	5	2	2	3	4	5	2	2
	[A.11] Acceso no autorizado	1	3	4	5	2	2	3	4	5	2	2

Tabla 18. (Continuación).

NOMBRE Y DESCRIPCION DEL ACTIVO	PROBABILIDAD DE LA AMENAZA		IMPACTO EN SUS DIMENSIONES					RIESGO EN SUS DIMENSIONES				
	AMENAZA SEGÚN MAGERIT	VALOR	D	I	C	A	T	D	I	C	A	T
	[A.15] Modificación deliberada de la información	1	3	4	5	2	2	3	4	5	2	2
	[A.18] Destrucción de información (intencional)	1	3	4	5	2	2	3	4	5	2	2
	[A.19] Divulgación de información	1	3	4	5	2	2	3	4	5	2	2
[U_INTER] Usuarios Internos de UNITRANSA S.A. (empleados).	[E.19] Fugas de información	2	5	4	4	4	0	10	8	4	8	0
	[A.28] Indisponibilidad del personal	3	5	3	2	4	0	15	9	6	12	0
	[A.29] Extorsión	1	5	3	2	4	0	5	3	2	4	0
	[A.30] Ingeniería social (picaresca)	2	5	3	4	4	3	10	6	8	8	6
[ADMIN_UN] Administrador de la empresa.	[E.7] Deficiencias en la organización	2	4	2	4	1	0	8	4	8	2	0
	[E.19] Fugas de información	1	4	2	4	1	0	4	2	4	1	0
	[A.29] Extorsión	1	4	2	4	1	0	4	2	4	1	0
[PROV_UN] Proveedores de UNITRANSA S.A.	[E.19] Fugas de información	1	3	2	3	1	0	3	2	3	1	0
	[A.29] Extorsión	1	3	2	3	1	0	3	2	3	1	0
	[A.30] Ingeniería social (picaresca)	1	3	2	3	1	3	3	2	3	1	3
[SOC_UN] Socios UNITRANSA S.A.	[E.19] Fugas de información	2	1	2	1	1	0	2	4	2	2	0
	[A.29] Extorsión	1	1	2	1	1	0	1	2	1	1	0
[SRV_BD] Equipo Servidor de Bases de Datos.	[N.1] Fuego	1	5	5	5	5	3	5	5	5	5	3
	[N.2] Daños por agua (inundaciones)	1	5	5	5	5	3	5	5	5	5	3
	[I.2] Daños por agua (escapes, fugas)	1	5	5	5	5	3	5	5	5	5	3
	[I.6] Corte del suministro eléctrico	1	5	5	5	5	3	5	5	5	5	3
	[I.7] Condiciones inadecuadas de temperatura o humedad	1	5	5	5	5	3	5	5	5	5	3
	[E.2] Errores del administrador	1	5	5	5	5	3	5	5	5	5	3

Tabla 18. (Continuación).

NOMBRE Y DESCRIPCION DEL ACTIVO	PROBABILIDAD DE LA AMENAZA		IMPACTO EN SUS DIMENSIONES					RIESGO EN SUS DIMENSIONES				
	AMENAZA SEGÚN MAGERIT	VALOR	D	I	C	A	T	D	I	C	A	T
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	5	5	5	5	3	5	5	5	5	3
	[I.5] Avería de origen físico o lógico	3	5	5	5	5	3	15	15	15	15	9
	[E.24] Caída del sistema por agotamiento de recursos		5	5	5	5	3	5	5	5	5	3
	[E.25] Pérdida de equipos	1	5	5	5	5	3	5	5	5	5	3
	[A.6] Abuso de privilegios de acceso	1	5	5	5	5	3	5	5	5	5	3
	[A.7] Uso no previsto	1	5	5	5	5	3	5	5	5	5	3
	[A.11] Acceso no autorizado	1	5	5	5	5	3	5	5	5	5	3
	[A.23] Manipulación de los equipos	2	5	5	5	5	3	5	5	5	5	3
	[A.24] Denegación de servicio	2	5	5	5	5	3	10	10	10	10	6
	[A.25] Robo	1	5	5	5	5	3	5	5	5	5	3
	[A.26] Ataque destructivo	1	5	5	5	5	3	5	5	5	5	3
[PC1] Computadora de Gerencia	[N.1] Fuego	1	3	4	5	3	2	3	4	5	3	2
	[N.2] Daños por agua (inundaciones naturales)	1	3	4	5	3	2	3	4	5	3	2
	[I.2] Daños por agua (escapes, fugas)	1	3	4	5	3	2	3	4	5	3	2
	[I.5] Avería de origen físico y lógico	3	3	4	5	3	2	9	12	15	9	6
	[I.6] Corte del suministro eléctrico	1	3	4	5	3	2	3	4	5	3	2
	[I.7] Condiciones inadecuadas de temperatura o humedad	1	3	4	5	3	2	3	4	5	3	2
	[E.2] Errores del administrador	1	3	4	5	3	2	3	4	5	3	2
	[I.7] Condiciones inadecuadas de temperatura o humedad	1	3	4	5	3	2	3	4	5	3	2
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	3	4	5	3	2	3	4	5	3	2

Tabla 18. (Continuación).

NOMBRE Y DESCRIPCION DEL ACTIVO	PROBABILIDAD DE LA AMENAZA		IMPACTO EN SUS DIMENSIONES					RIESGO EN SUS DIMENSIONES				
	AMENAZA SEGÚN MAGERIT	VALOR	D	I	C	A	T	D	I	C	A	T
	[I.5] Avería de origen físico o lógico	2	3	4	5	3	2	6	8	10	6	4
	[E.24] Caída del sistema por agotamiento de recursos	1	3	4	5	3	2	3	4	5	3	2
	[E.25] Pérdida de equipos	1	3	4	5	3	2	3	4	5	3	2
	[A.6] Abuso de privilegios de acceso	1	3	4	5	3	2	3	4	5	3	2
	[A.7] Uso no previsto	1	3	4	5	3	2	3	4	5	3	2
	[A.11] Acceso no autorizado	1	3	4	5	3	2	3	4	5	3	2
	[A.23] Manipulación de los equipos	1	3	4	5	3	2	3	4	5	3	2
	[A.24] Denegación de servicio	1	3	4	5	3	2	3	4	5	3	2
	[A.25] Robo	1	3	4	5	3	2	3	4	5	3	2
	[A.26] Ataque destructivo	1	3	4	5	3	2	3	4	5	3	2
[PC2] Computadora de Dpto. Jurídico	[N.1] Fuego	1	3	3	4	3	2	3	3	4	3	2
	[N.2] Daños por agua (inundaciones)	1	3	3	4	3	2	3	3	4	3	2
	[I.2] Daños por agua (inundaciones, escapes)	1	3	3	4	3	2	3	3	4	3	2
	[I.5] Avería de origen físico o lógico	3	3	3	4	3	2	9	9	12	9	6
	[I.6] Corte del suministro eléctrico	1	3	3	4	3	2	3	3	4	3	2
	[E.2] Errores del administrador	1	3	3	4	3	2	3	3	4	3	2
	[I.7] Condiciones inadecuadas de temperatura o humedad	1	3	3	4	3	2	3	3	4	3	2
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	3	3	4	3	2	3	3	4	3	2
	[E.24] Caída del sistema por agotamiento de recursos	1	3	3	4	3	2	3	3	4	3	2
	[E.25] Pérdida de equipos	1	3	3	4	3	2	3	3	4	3	2

Tabla 18. (Continuación).

NOMBRE Y DESCRIPCION DEL ACTIVO	PROBABILIDAD DE LA AMENAZA		IMPACTO EN SUS DIMENSIONES					RIESGO EN SUS DIMENSIONES				
	AMENAZA SEGÚN MAGERIT	VALOR	D	I	C	A	T	D	I	C	A	T
	[A.6] Abuso de privilegios de acceso	1	3	3	4	3	2	3	3	4	3	2
	[A.7] Uso no previsto	1	3	3	4	3	2	3	3	4	3	2
	[A.11] Acceso no autorizado	1	3	3	4	3	2	3	3	4	3	2
	[A.23] Manipulación de los equipos	1	3	3	4	3	2	3	3	4	3	2
	[A.24] Denegación de servicio	1	3	3	4	3	2	3	3	4	3	2
	[A.25] Robo	1	3	3	4	3	2	3	3	4	3	2
	[A.26] Ataque destructivo	1	3	3	4	3	2	3	3	4	3	2
[PC3] Puestos de trabajo	[N.1] Fuego	1	2	1	2	2	1	2	1	2	2	1
	[N.2] Daños por agua (inundaciones)	1	2	1	2	2	1	2	1	2	2	1
	[I.2] Daños por agua (escapes, fugas)	1	2	1	2	2	1	2	1	2	2	1
	[I.5] Avería de origen físico o lógico	3	2	1	2	2	2	6	3	6	6	6
	[I.6] Corte del suministro eléctrico	1	2	1	2	2	1	2	1	2	2	1
	[I.7] Condiciones inadecuadas de temperatura o humedad	1	2	1	2	2	1	2	1	2	2	1
	[E.2] Errores del administrador	1	2	1	2	2	2	2	1	2	2	2
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	2	1	2	2	2	2	1	2	2	2
	[E.24] Caída del sistema por agotamiento de recursos	1	2	1	2	2	1	2	1	2	2	1
	[E.25] Pérdida de equipos	1	2	1	2	2	1	2	1	2	2	1
	[A.6] Abuso de privilegios de acceso	2	2	1	2	2	1	4	2	4	4	2
	[A.7] Uso no previsto	3	2	1	2	2	1	6	3	6	6	3
	[A.11] Acceso no autorizado	2	2	1	2	2	1	4	2	4	4	2
	[A.23] Manipulación de los equipos	2	2	1	2	2	3	4	2	4	4	6
	[A.24] Denegación de servicio	1	2	1	2	2	1	2	1	2	2	1
	[A.25] Robo	1	2	1	2	2	1	2	1	2	2	1

Tabla 18. (Continuación).

NOMBRE Y DESCRIPCION DEL ACTIVO	PROBABILIDAD DE LA AMENAZA		IMPACTO EN SUS DIMENSIONES					RIESGO EN SUS DIMENSIONES				
	AMENAZA SEGÚN MAGERIT	VALOR	D	I	C	A	T	D	I	C	A	T
	[A.26] Ataque destructivo	2	2	1	2	2	1	4	2	4	4	2
[IMP] Impresora	[N.1] Fuego	1	2	0	1	1	0	2	0	1	1	0
	[N.2] Daños por agua (inundaciones)	1	2	0	1	1	0	2	0	1	1	0
	[I.2] Daños por agua (accidentalidad)	1	2	0	1	1	0	2	0	1	1	0
	[I.5] Avería de origen físico o lógico	3	2	0	1	1	0	6	0	3	3	0
	[I.6] Corte del suministro eléctrico	1	2	0	1	1	0	2	0	1	1	0
	[I.7] Condiciones inadecuadas de temperatura o humedad	1	2	0	1	1	0	2	0	1	1	0
	[E.2] Errores del administrador	1	2	0	1	1	0	2	0	1	1	0
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	2	0	1	1	0	2	0	1	1	0
	[E.24] Caída del sistema por agotamiento de recursos	2	2	0	1	1	0	4	0	2	2	0
	[E.25] Pérdida de equipos	1	2	0	1	1	0	2	0	1	1	0
	[A.7] Uso no previsto	1	2	0	1	1	0	2	0	1	1	0
	[A.23] Manipulación de los equipos	1	2	0	1	1	0	2	0	1	1	0
	[.25] Robo	1	2	0	1	1	0	2	0	1	1	0
	[A.26] Ataque destructivo	2	2	0	1	1	0	4	0	2	2	0
[FRW] Firewall	[N.1] Fuego	1	1	3	3	5	3	1	3	3	5	3
	[N.2] Daños por agua (inundaciones)	1	1	3	3	5	3	1	3	3	5	3
	[I.2] Daños por agua (escapes, fugas)	1	1	3	3	5	3	1	3	3	5	3
	[I.5] Avería de origen físico o lógico	1	1	3	3	5	3	1	3	3	5	3
	[I.6] Corte del suministro eléctrico	1	1	3	3	5	3	1	3	3	5	3
	[E.2] Errores del administrador	1	1	3	3	5	3	1	3	3	5	3
	[I.7] Condiciones inadecuadas de temperatura o humedad	1	1	3	3	5	3	1	3	3	5	3

Tabla 18. (Continuación).

NOMBRE Y DESCRIPCION DEL ACTIVO	PROBABILIDAD DE LA AMENAZA		IMPACTO EN SUS DIMENSIONES					RIESGO EN SUS DIMENSIONES				
	AMENAZA SEGÚN MAGERIT	VALOR	D	I	C	A	T	D	I	C	A	T
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	1	3	3	5	3	1	3	3	5	3
	[E.25] Pérdida de equipos	1	1	3	3	5	3	1	3	3	5	3
	[A.23] Manipulación de los equipos	1	1	3	3	5	3	1	3	3	5	3
	[A.25] Robo	1	1	3	3	5	3	1	3	3	5	3
	[A.26] Ataque destructivo	1	1	3	3	5	3	1	3	3	5	3
[SW_P1] Switch Ethernet Gigabit Linksys SE4008 WRT de 8 puertos (1er. Piso).	[N.1] Fuego	1	3	1	1	2	2	3	1	1	2	2
	[N.2] Daños por agua (inundaciones)	1	3	1	1	2	2	3	1	1	2	2
	[I.2] Daños por agua	1	3	1	1	2	2	3	1	1	2	2
	[I.5] Avería de origen físico o lógico	2	3	1	1	2	2	6	2	2	4	4
	[I.6] Corte del suministro eléctrico	1	3	1	1	2	2	3	1	1	2	2
	[I.7] Condiciones inadecuadas de temperatura o humedad	1	3	1	1	2	0	3	1	1	2	0
	[E.2] Errores del administrador	1	3	1	1	2	2	3	1	1	2	2
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	3	1	1	2	2	3	1	1	2	2
	[E.25] Pérdida de equipos	1	3	1	1	2	3	3	1	1	2	3
	[A.23] Manipulación de los equipos	1	3	1	1	2	2	3	1	1	2	2
	[A.25] Robo	1	3	1	1	2	3	3	1	1	2	3
	[A.26] Ataque destructivo	1	3	1	1	2	3	3	1	1	2	3
[SW_P2] Switch Linksys SE3016 de 16 puertos (2º. Piso).	[N.1] Fuego	1	3	1	1	2	3	3	1	1	2	3
	[N.2] Daños por agua (inundaciones)	1	3	1	1	2	3	3	1	1	2	3
	[I.2] Daños por agua	1	3	1	1	2	3	3	1	1	2	3
	[I.5] Avería de origen físico o lógico	2	3	1	1	2	3	6	2	2	4	6
	[I.6] Corte del suministro eléctrico	1	3	1	1	2	0	3	1	1	2	0

Tabla 18. (Continuación).

NOMBRE Y DESCRIPCION DEL ACTIVO	PROBABILIDAD DE LA AMENAZA		IMPACTO EN SUS DIMENSIONES					RIESGO EN SUS DIMENSIONES				
	AMENAZA SEGÚN MAGERIT	VALOR	D	I	C	A	T	D	I	C	A	T
	[I.7] Condiciones inadecuadas de temperatura o humedad	1	3	1	1	2	0	3	1	1	2	0
	[E.2] Errores del administrador	1	3	1	1	2	2	3	1	1	2	2
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	3	1	1	2	2	3	1	1	2	2
	[E.25] Pérdida de equipos	1	3	1	1	2	3	3	1	1	2	3
	[A.23] Manipulación de los equipos	1	3	1	1	2	3	3	1	1	2	3
	[A.25] Robo	1	3	1	1	2	3	3	1	1	2	3
	[A.26] Ataque destructivo	1	3	1	1	2	3	3	1	1	2	3
[SW_P3] Switch Linksys SE4008 WRT de 8 puertos (3er. Piso)	[N.1] Fuego	1	3	1	1	2	3	3	1	1	2	3
	[N.2] Daños por agua (inundaciones)	1	3	1	1	2	3	3	1	1	2	3
	[I.2] Daños por agua (escapes, fugas)	1	3	1	1	2	3	3	1	1	2	3
	[I.5] Avería de origen físico o lógico	2	3	1	1	2	3	6	2	2	4	6
	[I.6] Corte del suministro eléctrico	1	3	1	1	2	0	3	1	1	2	0
	[I.7] Condiciones inadecuadas de temperatura o humedad	1	3	1	1	2	0	3	1	1	2	0
	[E.2] Errores del administrador	1	3	1	1	2	2	3	1	1	2	2
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	3	1	1	2	3	3	1	1	2	3
	[E.25] Pérdida de equipos	2	3	1	1	2	3	6	2	2	4	6
	[A.23] Manipulación de los equipos	1	3	1	1	2	3	3	1	1	2	3
	[A.25] Robo	1	3	1	1	2	3	3	1	1	2	3
	[A.26] Ataque destructivo	1	3	1	1	2	3	3	1	1	2	3
[RTR] Router Netgear 4g Lte Router Lg2200d	[N.1] Fuego	1	4	3	3	3	2	4	3	3	3	2
	[N.2] Daños por agua (inundaciones)	1	4	3	3	3	2	4	3	3	3	2
	[I.2] Daños por agua (fugas, escapes)	1	4	3	3	3	2	4	3	3	3	2
	[I.5] Avería de origen físico o lógico	2	4	3	3	3	2	8	6	6	6	4

Tabla 18. (Continuación).

NOMBRE Y DESCRIPCION DEL ACTIVO	PROBABILIDAD DE LA AMENAZA		IMPACTO EN SUS DIMENSIONES					RIESGO EN SUS DIMENSIONES				
	AMENAZA SEGÚN MAGERIT	VALOR	D	I	C	A	T	D	I	C	A	T
	[I.6] Corte del suministro eléctrico	1	4	3	3	3	2	4	3	3	3	2
	[I.7] Condiciones inadecuadas de temperatura o humedad	1	4	3	3	3	2	4	3	3	3	2
	[E.2] Errores del administrador	1	4	3	3	3	2	4	3	3	3	2
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	4	3	3	3	2	4	3	3	3	2
	[E.25] Pérdida de equipos	1	4	3	3	3	2	4	3	3	3	2
	[A.5] Suplantación de la identidad del usuario	1	4	3	3	3	2	4	3	3	3	2
	[A.6] Abuso de privilegios de acceso	1	4	3	3	3	2	4	3	3	3	2
	[A.11] Acceso no autorizado	2	4	3	3	3	2	8	6	6	6	4
	[A.23] Manipulación de los equipos	2	4	3	3	3	2	8	6	6	6	4
	[A.24] Denegación de servicio	1	4	3	3	3	2	4	3	3	3	2
	[A.25] Robo	1	4	3	3	3	2	4	3	3	3	2
	[A.26] Ataque destructivo	1	4	3	3	3	2	4	3	3	3	2
[INT_UNIT] Internet de la empresa	[I.8] Fallo de servicios de comunicaciones	3	2	0	0	0	0	6	0	0	0	0
	[E.2] Errores del administrador	1	2	0	0	0	0	2	0	0	0	0
	[E.9] Errores de [re-]encaminamiento	2	2	0	0	0	0	4	0	0	0	0
	[E.15] Alteración accidental de la información	2	2	0	0	0	0	4	0	0	0	0
	[E.19] Fugas de información	2	2	0	0	0	0	4	0	0	0	0
	[A.5] Suplantación de la identidad del usuario	2	2	0	0	0	0	4	0	0	0	0
	[A.6] Abuso de privilegios de acceso	2	2	0	0	0	0	4	0	0	0	0
	[A.7] Uso no previsto	3	2	0	0	0	0	6	0	0	0	0
	[I.8] Fallo de servicios de comunicaciones	3	3	0	0	0	0	9	0	0	0	0
	[E.1] Errores de los usuarios	2	3	0	0	0	0	6	0	0	0	0

Tabla 18. (Continuación).

NOMBRE Y DESCRIPCION DEL ACTIVO	PROBABILIDAD DE LA AMENAZA		IMPACTO EN SUS DIMENSIONES					RIESGO EN SUS DIMENSIONES				
	AMENAZA SEGÚN MAGERIT	VALOR	D	I	C	A	T	D	I	C	A	T
[TELN_UNIT] Acceso remoto a cuenta local (PUTTY)	[E.2] Errores del administrador	1	3	0	0	0	0	3	0	0	0	0
	[E.9] Errores de [re-]encaminamiento	2	3	0	0	0	0	6	0	0	0	0
	[E.10] Errores de secuencia	1	3	0	0	0	0	3	0	0	0	0
	[E.15] Alteración accidental de la información	1	3	0	0	0	0	3	0	0	0	0
	[E.18] Destrucción de información	1	3	0	0	0	0	3	0	0	0	0
	[E.19] Fugas de información	1	3	0	0	0	0	3	0	0	0	0
	[E.24] Caída del sistema por agotamiento de recursos	1	3	0	0	0	0	3	0	0	0	0
	[A.5] Suplantación de la identidad del usuario	2	3	0	0	0	0	6	0	0	0	0
	[A.6] Abuso de privilegios de acceso	2	3	0	0	0	0	6	0	0	0	0
	[A.7] Uso no previsto	1	3	0	0	0	0	3	0	0	0	0
	[A.9] [Re-]encaminamiento de mensajes	1	3	0	0	0	0	3	0	0	0	0
	[A.10] Alteración de secuencia	1	3	0	0	0	0	3	0	0	0	0
	[A.11] Acceso no autorizado	1	3	0	0	0	0	3	0	0	0	0
	[A.13] Repudio	1	3	0	0	0	0	3	0	0	0	0
	[A.18] Destrucción de información	1	3	0	0	0	0	3	0	0	0	0
	[A.19] Divulgación de información	1	3	0	0	0	0	3	0	0	0	0
	[A.24] Denegación de servicio	1	3	0	0	0	0	3	0	0	0	0
[E_UNIT] Correo electrónico Empresarial.	[I.8] Fallo de servicios de comunicaciones	2	3	0	1	1	0	6	0	2	2	0
	[E.1] Errores de los usuarios	1	3	0	1	1	0	3	0	1	1	0
	[E.2] Errores del administrador	1	3	0	1	1	0	3	0	1	1	0
	[E.9] Errores de [re-]encaminamiento	1	3	0	1	1	0	3	0	1	1	0
	[E.15] Alteración accidental de la información	1	3	0	1	1	0	3	0	1	1	0

Tabla 18. (Continuación).

NOMBRE Y DESCRIPCION DEL ACTIVO	PROBABILIDAD DE LA AMENAZA		IMPACTO EN SUS DIMENSIONES					RIESGO EN SUS DIMENSIONES				
	AMENAZA SEGÚN MAGERIT	VALOR	D	I	C	A	T	D	I	C	A	T
	[E.19] Fugas de información	1	3	0	1	1	0	3	0	1	1	0
	[E.24] Caída del sistema por agotamiento de recursos	1	3	0	1	1	0	3	0	1	1	0
	[A.5] Suplantación de la identidad del usuario	2	3	0	1	1	0	6	0	2	2	0
	[A.7] Uso no previsto	1	3	0	1	1	0	3	0	1	1	0
	[A.9] [Re-]encaminamiento de mensajes	1	3	0	1	1	0	3	0	1	1	0
	[A.13] Repudio	1	3	0	1	1	0	3	0	1	1	0
	[A.19] Divulgación de información	1	3	0	1	1	0	3	0	1	1	0
	[A.24] Denegación de servicio	1	3	0	1	1	0	3	0	1	1	0
[FILE_UNIT] Almacenamiento de ficheros (OneDrive)	[I.8] Fallo de servicios de comunicaciones	1	5	2	1	0	0	5	2	1	0	0
	[E.1] Errores de los usuarios	2	5	2	1	0	0	10	4	2	0	0
	[E.15] Alteración accidental de la información	1	5	2	1	0	0	5	2	1	0	0
	[E.18] Destrucción de información	1	5	2	1	0	0	5	2	1	0	0
	[E.19] Fugas de información	1	5	2	1	0	0	5	2	1	0	0
	[A.9] [Re-]encaminamiento de mensajes	1	5	2	1	0	0	5	2	1	0	0
	[A.11] Acceso no autorizado	1	5	2	1	0	0	5	2	1	0	0
	[A.13] Repudio	1	5	2	1	0	0	5	2	1	0	0
	[A.18] Destrucción de información	1	5	2	1	0	0	5	2	1	0	0
	[A.19] Divulgación de información	1	5	2	1	0	0	5	2	1	0	0
	[A.24] Denegación de servicio	1	5	2	1	0	0	5	2	1	0	0
[FTP_UNIT] Transferencia de ficheros (Servidor FTP en Windows)	[I.8] Fallo de servicios de comunicaciones	1	4	2	2	1	0	4	2	2	1	0
	[E.1] Errores de los usuarios	2	4	2	2	1	0	8	4	4	2	0

Tabla 18. (Continuación).

NOMBRE Y DESCRIPCION DEL ACTIVO	PROBABILIDAD DE LA AMENAZA		IMPACTO EN SUS DIMENSIONES					RIESGO EN SUS DIMENSIONES				
	AMENAZA SEGÚN MAGERIT	VALOR	D	I	C	A	T	D	I	C	A	T
	[E.9] Errores de [re-]encaminamiento	2	4	2	2	1	0	8	4	4	2	0
	[E.19] Fugas de información	1	4	2	2	1	0	4	2	2	1	0
	[E.24] Caída del sistema por agotamiento de recursos	1	4	2	2	1	0	4	2	2	1	0
	[A.9] [Re-]encaminamiento de mensajes	1	4	2	2	1	0	4	2	2	1	0
	[A.10] Alteración de secuencia	1	4	2	2	1	0	4	2	2	1	0
	[A.19] Divulgación de información	1	4	2	2	1	0	4	2	2	1	0
[EDI_UNIT] Intercambio electrónico de datos. Sistema ERP (sistema de planificación de recursos empresariales)	[I.8] Fallo de servicios de comunicaciones	2	3	2	3	2	0	6	4	6	4	0
	[E.1] Errores de los usuarios	2	3	2	3	2	0	6	4	6	4	0
	[E.10] Errores de secuencia	1	3	2	3	2	0	3	2	3	2	0
	[E.15] Alteración accidental de la información	1	3	2	3	2	0	3	2	3	2	0
	[E.18] Destrucción de información	1	3	2	3	2	0	3	2	3	2	0
	[E.19] Fugas de información	1	3	2	3	2	0	3	2	3	2	0
	[E.24] Caída del sistema por agotamiento de recursos	1	3	2	3	2	0	3	2	3	2	0
	[A.10] Alteración de secuencia	1	3	2	3	2	0	3	2	3	2	0
	[A.19] Divulgación de información	1	3	2	3	2	0	3	2	3	2	0
[DIR_UNIT] Servicio de Directorio	[I.8] Fallo de servicios de comunicaciones	3	1	1	2	3	0	3	3	6	9	0
	[E.1] Errores de los usuarios	2	1	1	2	3	0	2	2	4	6	0
	[E.2] Errores del administrador	1	1	1	2	3	0	1	1	2	3	0
	[A.5] Suplantación de la identidad del usuario	2	1	1	2	3	0	2	2	4	6	0
	[A.7] Uso no previsto	1	1	1	2	3	0	1	1	2	3	0
	[A.9] [Re-]encaminamiento de mensajes	1	1	1	2	3	0	1	1	2	3	0

Tabla 18. (Continuación).

NOMBRE Y DESCRIPCION DEL ACTIVO	PROBABILIDAD DE LA AMENAZA		IMPACTO EN SUS DIMENSIONES					RIESGO EN SUS DIMENSIONES				
	AMENAZA SEGÚN MAGERIT	VALOR	D	I	C	A	T	D	I	C	A	T
	[A.11] Acceso no autorizado	1	1	1	2	3	0	1	1	2	3	0
	[A.13] Repudio	1	1	1	2	3	0	1	1	2	3	0
[IDM_UNIT] Gestión de identidades	[E.1] Errores de los usuarios	1	1	4	4	5	0	1	4	4	5	0
	[E.2] Errores del administrador	1	1	4	4	5	0	1	4	4	5	0
	[E.15] Alteración accidental de la información	1	1	4	4	5	0	1	4	4	5	0
	[E.18] Destrucción de información (accidental)	1	1	4	4	5	0	1	4	4	5	0
	[E.19] Fugas de información	1	1	4	4	5	0	1	4	4	5	0
	[A.11] Acceso no autorizado	1	1	4	4	5	0	1	4	4	5	0
	[A.18] Destrucción de información (intencional)	1	1	4	4	5	0	1	4	4	5	0
	[A.19] Divulgación de información	1	1	4	4	5	0	1	4	4	5	0
[IMP_UNIT] Gestión de privilegios	[E.1] Errores de los usuarios	2	4	3	4	5	0	8	6	8	10	0
	[E.2] Errores del administrador	1	4	3	4	5	0	4	3	4	5	0
	[E.15] Alteración accidental de la información	1	4	3	4	5	0	4	3	4	5	0
	[E.18] Destrucción de información (accidental)	1	4	3	4	5	0	4	3	4	5	0
	[E.19] Fugas de información	1	4	3	4	5	0	4	3	4	5	0
	[A.11] Acceso no autorizado	1	4	3	4	5	0	4	3	4	5	0
	[A.18] Destrucción de información (intencional)	1	4	3	4	5	0	4	3	4	5	0
	[A.19] Divulgación de información	1	4	3	4	5	0	4	3	4	5	0
[SRV_APP] Servidor de aplicaciones utilizadas en la empresa	[A.13] Repudio	1	5	3	3	3	4	5	3	3	3	4
	[A.18] Destrucción de información	2	5	3	3	3	4	10	6	6	6	8
	[A.19] Divulgación de información	1	5	3	3	3	4	5	3	3	3	4
	[E.9] Errores de [re-]encaminamiento	2	5	3	3	3	4	10	6	6	6	8

Tabla 18. (Continuación).

NOMBRE Y DESCRIPCION DEL ACTIVO	PROBABILIDAD DE LA AMENAZA		IMPACTO EN SUS DIMENSIONES					RIESGO EN SUS DIMENSIONES				
	AMENAZA SEGÚN MAGERIT	VALOR	D	I	C	A	T	D	I	C	A	T
	[E.20] Vulnerabilidades de los programas (software)	1	5	3	3	3	4	5	3	3	3	4
	[E.21] Errores de mantenimiento / actualización de programas (software)	1	5	3	3	3	4	5	3	3	3	4
	[A.5] Suplantación de la identidad del usuario	1	5	3	3	3	4	5	3	3	3	4
	[A.6] Abuso de privilegios de acceso	1	5	3	3	3	4	5	3	3	3	4
	[A.8] Difusión de software dañino	2	5	3	3	3	4	10	6	6	6	12
	[A.11] Acceso no autorizado	1	5	3	3	3	4	5	3	3	3	4
	[A.18] Destrucción de información (intencional)	1	5	3	3	3	4	5	3	3	3	4
	[A.22] Manipulación de programas	1	5	3	3	3	4	5	3	3	3	4
	[A.24] Denegación de servicio	1	5	3	3	3	4	5	3	3	3	4
[BD_ORC] Manejador de Base de Datos Oracle	[I.5] Avería de origen físico o lógico	1	5	3	3	3	3	5	3	3	3	3
	[E.1] Errores de los usuarios	1	5	3	3	3	3	5	3	3	3	3
	[E.2] Errores del administrador	1	5	3	3	3	3	5	3	3	3	3
	[E.9] Errores de [re-]encaminamiento	2	5	3	3	3	3	10	6	6	6	6
	[E.18] Destrucción de información	1	5	3	3	3	3	5	3	3	3	3
	[E.19] Fugas de información	1	5	3	3	3	3	5	3	3	3	3
	[E.20] Vulnerabilidades de los programas (software)	1	5	3	3	3	3	5	3	3	3	3
	[E.21] Errores de mantenimiento / actualización de programas (software)	1	5	3	3	3	3	5	3	3	3	3
	[A.5] Suplantación de la identidad del usuario	1	5	3	3	3	3	5	3	3	3	3
	[A.6] Abuso de privilegios de acceso	1	5	3	3	3	3	5	3	3	3	3
	[A.8] Difusión de software dañino	2	5	3	3	3	3	10	6	6	6	6

Tabla 18. (Continuación).

NOMBRE Y DESCRIPCION DEL ACTIVO	PROBABILIDAD DE LA AMENAZA		IMPACTO EN SUS DIMENSIONES					RIESGO EN SUS DIMENSIONES				
	AMENAZA SEGÚN MAGERIT	VALOR	D	I	C	A	T	D	I	C	A	T
	[A.11] Acceso no autorizado	1	5	3	3	3	3	5	3	3	3	3
	[A.18] Destrucción de información (intencional)	1	5	3	3	3	3	5	3	3	3	3
	[A.19] Divulgación de información	1	5	3	3	3	3	5	3	3	3	3
	[A.22] Manipulación de programas	1	5	3	3	3	3	5	3	3	3	3
	[A.24] Denegación de servicio	1	5	3	3	3	3	5	3	3	3	3
[SO_WIND7] Sistema Operativo Windows 7 Profesional	[I.5] Avería de origen físico o lógico	1	2	2	2	2	2	2	2	2	2	2
	[E.1] Errores de los usuarios	2	2	2	2	2	2	4	4	4	4	4
	[E.2] Errores del administrador	1	2	2	2	2	2	2	2	2	2	2
	[E.9] Errores de [re-]encaminamiento	2	2	2	2	2	2	4	4	4	4	4
	[E.18] Destrucción de información	1	2	2	2	2	2	2	2	2	2	2
	[E.20] Vulnerabilidades de los programas (software)	1	2	2	2	2	2	2	2	2	2	2
	[E.21] Errores de mantenimiento / actualización de programas (software)	2	2	2	2	2	2	4	4	4	4	4
	[A.5] Suplantación de la identidad del usuario	3	2	3	4	4	2	6	9	12	12	6
	[A.6] Abuso de privilegios de acceso	1	2	2	2	2	2	2	2	2	2	2
	[A.8] Difusión de software dañino	2	2	2	2	2	2	4	4	4	4	4
	[A.11] Acceso no autorizado	2	2	2	2	2	2	4	4	4	4	4
	[A.18] Destrucción de información (intencional)	1	2	2	2	2	2	2	2	2	2	2
	[A.22] Manipulación de programas	1	2	2	2	2	2	2	2	2	2	2
	[I.5] Avería de origen físico o lógico	2	2	2	2	2	2	4	4	4	4	4
	[E.1] Errores de los usuarios	2	2	2	2	2	2					
	[E.2] Errores del administrador	1	2	2	2	2	2	2	2	2	2	2

Tabla 18. (Continuación).

NOMBRE Y DESCRIPCION DEL ACTIVO	PROBABILIDAD DE LA AMENAZA		IMPACTO EN SUS DIMENSIONES					RIESGO EN SUS DIMENSIONES				
	AMENAZA SEGÚN MAGERIT	VALOR	D	I	C	A	T	D	I	C	A	T
[SO_WIND8] Sistema Operativo Windows 8	[E.9] Errores de [re-]encaminamiento	2	2	2	2	2	2	4	4	4	4	4
	[E.18] Destrucción de información (accidental)	1	2	2	2	2	2	2	2	2	2	2
	[E.20] Vulnerabilidades de los programas (software)	1	2	2	2	2	2	2	2	2	2	2
	[E.21] Errores de mantenimiento / actualización de programas (software)	2	2	2	2	2	2	4	4	4	4	4
	[A.5] Suplantación de la identidad del usuario	1	2	2	2	2	2	2	2	2	2	2
	[A.6] Abuso de privilegios de acceso	1	2	2	2	2	2	2	2	2	2	2
	[A.8] Difusión de software dañino	2	2	2	2	2	2	4	4	4	4	4
	[A.11] Acceso no autorizado	2	2	2	2	2	2					
	[A.18] Destrucción de información (intencional)	1	2	2	2	2	2	2	2	2	2	2
	[A.22] Manipulación de programas	1	2	2	2	2	2	2	2	2	2	2
[SO_WINDXP] Sistema Operativo Windows XP	[I.5] Avería de origen físico o lógico	4	2	2	2	2	2	8	8	8	8	8
	[E.1] Errores de los usuarios	2	2	2	2	2	2	4	4	4	4	4
	[E.2] Errores del administrador	1	2	2	2	2	2	2	2	2	2	2
	[E.9] Errores de [re-]encaminamiento	2	2	2	2	2	2	4	4	4	4	4
	[E.18] Destrucción de información (accidental)	1	2	2	2	2	2	2	2	2	2	2
	[E.20] Vulnerabilidades de los programas (software)	3	2	2	2	2	2	6	6	6	6	6
	[E.21] Errores de mantenimiento / actualización de programas (software)	2	2	2	2	2	2	4	4	4	4	4
	[A.5] Suplantación de la identidad del usuario	5	2	2	2	2	2	10	10	10	10	10

Tabla 18. (Continuación).

NOMBRE Y DESCRIPCION DEL ACTIVO	PROBABILIDAD DE LA AMENAZA		IMPACTO EN SUS DIMENSIONES					RIESGO EN SUS DIMENSIONES				
	AMENAZA SEGÚN MAGERIT	VALOR	D	I	C	A	T	D	I	C	A	T
	[A.6] Abuso de privilegios de acceso	5	2	2	2	2	2	10	10	10	10	10
	[A.8] Difusión de software dañino	3	2	2	2	2	2	6	6	6	6	6
	[A.11] Acceso no autorizado	2	2	2	2	2	2	4	4	4	4	4
	[A.18] Destrucción de información (intencional)	1	2	2	2	2	2	2	2	2	2	2
	[A.22] Manipulación de programas	2	2	2	2	2	2	4	4	4	4	4
[ADOB_DW] Editor HTML: Adobe Dreamweaver	[I.5] Avería de origen físico o lógico	3	1	1	0	1	0	3	3	0	3	0
	[E.1] Errores de los usuarios	1	1	1	0	1	0	1	1	0	1	0
	[E.2] Errores del administrador	1	1	1	0	1	0	1	1	0	1	0
	[E.9] Errores de [re-]encaminamiento	2	1	1	0	1	0	2	2	0	2	0
	[A.18] Destrucción de información (intencional)	1	1	1	0	1	0	1	1	0	1	0
	[A.22] Manipulación de programas	1	1	1	0	1	0	1	1	0	1	0
[ARTIS] Plantillas web: Artister	[I.5] Avería de origen físico o lógico	1	1	1	0	1	0	1	1	0	1	0
	[E.1] Errores de los usuarios	1	1	1	0	1	0	1	1	0	1	0
	[E.2] Errores del administrador	1	1	1	0	1	0	1	1	0	1	0
	[E.9] Errores de [re-]encaminamiento	2	1	1	0	1	0	2	2	0	2	0
	[E.20] Vulnerabilidades de los programas (software)	1	1	1	0	1	0	1	1	0	1	0
	[A.18] Destrucción de información (intencional)	1	1	1	0	1	0	1	1	0	1	0
[ADOB_FW] Editor de imágenes web: Adobe Fireworks	[I.5] Avería de origen físico o lógico	1	1	1	0	1	0	1	1	0	1	0
	[E.1] Errores de los usuarios	1	1	1	0	1	0	1	1	0	1	0
	[E.2] Errores del administrador	1	1	1	0	1	0	1	1	0	1	0
	[E.9] Errores de [re-]encaminamiento	2	1	1	0	1	0	2	2	0	2	0
	[A.18] Destrucción de información (intencional)	1	1	1	0	1	0	1	1	0	1	0

Tabla 18. (Continuación).

NOMBRE Y DESCRIPCION DEL ACTIVO	PROBABILIDAD DE LA AMENAZA		IMPACTO EN SUS DIMENSIONES					RIESGO EN SUS DIMENSIONES				
	AMENAZA SEGÚN MAGERIT	VALOR	D	I	C	A	T	D	I	C	A	T
[LOG_CR] Diseño de logos: Logo Creator	[I.5] Avería de origen físico o lógico	1	1	1	0	0	0	1	1	0	0	0
	[E.1] Errores de los usuarios	1	1	1	0	0	0	1	1	0	0	0
	[E.2] Errores del administrador	1	1	1	0	0	0	1	1	0	0	0
	[E.9] Errores de [re-]encaminamiento	2	1	1	0	0	0	2	2	0	0	0
	[A.18] Destrucción de información (intencional)	1	1	1	0	0	0	1	1	0	0	0
[CLT_FTP] Cliente FTP: Filezilla	[I.5] Avería de origen físico o lógico	1	3	2	1	1	1	3	2	1	1	1
	[E.1] Errores de los usuarios	1	3	2	1	1	1	3	2	1	1	1
	[E.2] Errores del administrador	1	3	2	1	1	1	3	2	1	1	1
	[E.9] Errores de [re-]encaminamiento	2	3	2	1	1	1	6	4	2	2	2
	[A.22] Manipulación de programas	1	3	2	1	1	1	3	2	1	1	1
[DES_PROPIO] Aplicaciones de desarrollo propio	[I.5] Avería de origen físico o lógico	1	2	1	3	3	2	2	1	3	3	2
	[E.1] Errores de los usuarios	1	2	1	3	3	2	2	1	3	3	2
	[E.2] Errores del administrador	1	2	1	3	3	2	2	1	3	3	2
	[E.9] Errores de [re-]encaminamiento	2	2	1	3	3	2	4	2	6	6	4
	[E.18] Destrucción de información (accidental)	1	2	1	3	3	2	2	1	3	3	2
	[E.20] Vulnerabilidades de los programas (software)	1	2	1	3	3	2	2	1	3	3	2
	[E.21] Errores de mantenimiento / actualización de programas (software)	1	2	1	3	3	2	2	1	3	3	2
	[A.5] Suplantación de la identidad del usuario	1	2	1	3	3	2	2	1	3	3	2
	[A.8] Difusión de software dañino	1	2	1	3	3	2	2	1	3	3	2
	[A.18] Destrucción de información (intencional)	1	2	1	3	3	2	2	1	3	3	2
	[A.19] Divulgación de información	1	2	1	3	3	2	2	1	3	3	2

Tabla 18. (Continuación).

NOMBRE Y DESCRIPCION DEL ACTIVO	PROBABILIDAD DE LA AMENAZA		IMPACTO EN SUS DIMENSIONES					RIESGO EN SUS DIMENSIONES				
	AMENAZA SEGÚN MAGERIT	VALOR	D	I	C	A	T	D	I	C	A	T
	[A.22] Manipulación de programas	1	2	1	3	3	2	2	1	3	3	2
[ANT_VIRUS] Antivirus AVAST	[I.5] Avería de origen físico o lógico	1	1	4	4	3	3	1	4	4	3	3
	[E.1] Errores de los usuarios	1	1	4	4	3	3	1	4	4	3	3
	[E.2] Errores del administrador	1	1	4	4	3	3	1	4	4	3	3
	[E.21] Errores de mantenimiento / actualización de programas (software)	1	1	4	4	3	3	1	4	4	3	3
	[A.18] Destrucción de información (intencional)	1	1	4	4	3	3	1	4	4	3	3
	[A.22] Manipulación de programas	1	1	4	4	3	3	1	4	4	3	3
[UPS] Sistema de alimentación ininterrumpida	[N.1] Fuego	1	1	0	0	0	0	1	0	0	0	0
	[N.2] Daños por agua (inundaciones)	1	1	0	0	0	0	1	0	0	0	0
	[I.2] Daños por agua (fugas, escapes)	1	1	0	0	0	0	1	0	0	0	0
	[I.5] Avería de origen físico o lógico	2	1	0	0	0	0	2	0	0	0	0
	[I.6] Corte del suministro eléctrico	1	1	0	0	0	0	1	0	0	0	0
	[I.7] Condiciones inadecuadas de temperatura o humedad	1	1	0	0	0	0	1	0	0	0	0
	[E.2] Errores del administrador	1	1	0	0	0	0	1	0	0	0	0
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	1	0	0	0	0	1	0	0	0	0
	[E.25] Pérdida de equipos	1	1	0	0	0	0	1	0	0	0	0
	[A.23] Manipulación de los equipos	1	1	0	0	0	0	1	0	0	0	0
	[A.25] Robo	1	1	0	0	0	0	1	0	0	0	0
	[A.26] Ataque destructivo	1	1	0	0	0	0	1	0	0	0	0
	[I.1] Fuego	1	1	0	0	0	0	1	0	0	0	0
	[I.2] Daños por agua	1	1	0	0	0	0	1	0	0	0	0

Tabla 18. (Continuación).

NOMBRE Y DESCRIPCION DEL ACTIVO	PROBABILIDAD DE LA AMENAZA		IMPACTO EN SUS DIMENSIONES					RIESGO EN SUS DIMENSIONES				
	AMENAZA SEGÚN MAGERIT	VALOR	D	I	C	A	T	D	I	C	A	T
	[I.5] Avería de origen físico o lógico	1	1	0	0	0	0	1	0	0	0	0
	[I.6] Corte del suministro eléctrico	1	1	0	0	0	0	1	0	0	0	0
	[I.7] Condiciones inadecuadas de temperatura o humedad	1	1	0	0	0	0	1	0	0	0	0
	[E.2] Errores del administrador	1	1	0	0	0	0	1	0	0	0	0
	[E.25] Pérdida de equipos	1	1	0	0	0	0	1	0	0	0	0
	[A.25] Robo	1	1	0	0	0	0	1	0	0	0	0
[CTR_TEMP] Equipos de climatización	[N.1] Fuego	1	1	0	0	0	1	1	0	0	0	1
	[N.2] Daños por agua (inundaciones)	1	1	0	0	0	1	1	0	0	0	1
	[I.2] Daños por agua	1	1	0	0	0	1	1	0	0	0	1
	[I.5] Avería de origen físico o lógico	2	1	0	0	0	1	2	0	0	0	2
	[I.6] Corte del suministro eléctrico	1	1	0	0	0	1	1	0	0	0	1
	[I.7] Condiciones inadecuadas de temperatura o humedad	1	1	0	0	0	1	1	0	0	0	1
	[E.2] Errores del administrador	1	1	0	0	0	1	1	0	0	0	1
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	1	0	0	0	1	1	0	0	0	1
	[E.25] Pérdida de equipos	1	1	0	0	0	1	1	0	0	0	1
	[A.23] Manipulación de los equipos	1	1	0	0	0	1	1	0	0	0	1
	[A.25] Robo	1	1	0	0	0	1	1	0	0	0	1
	[A.26] Ataque destructivo	1	1	0	0	0	1	1	0	0	0	1
[GEN_ELECT] Generador de energia	[N.1] Fuego	1	3	0	0	0	2	3	0	0	0	2
	[N.2] Daños por agua	1	3	0	0	0	2	3	0	0	0	2
	[I.2] Daños por agua (inundaciones)	1	3	0	0	0	2	3	0	0	0	2
	[I.5] Avería de origen físico o lógico	2	3	0	0	0	2	6	0	0	0	4

Tabla 18. (Continuación).

NOMBRE Y DESCRIPCION DEL ACTIVO	PROBABILIDAD DE LA AMENAZA		IMPACTO EN SUS DIMENSIONES					RIESGO EN SUS DIMENSIONES				
	AMENAZA SEGÚN MAGERIT	VALOR	D	I	C	A	T	D	I	C	A	T
	[I.7] Condiciones inadecuadas de temperatura o humedad	1	3	0	0	0	2	3	0	0	0	2
	[E.2] Errores del administrador	1	3	0	0	0	2	3	0	0	0	2
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	3	0	0	0	2	3	0	0	0	2
	[E.25] Pérdida de equipos	1	3	0	0	0	2	3	0	0	0	2
	[A.23] Manipulación de los equipos	1	3	0	0	0	2	3	0	0	0	2
	[A.25] Robo	1	3	0	0	0	2	3	0	0	0	2
	[A.26] Ataque destructivo	1	3	0	0	0	2	3	0	0	0	2
[NET_UNIT] Red local de UNITRANSA S.A.	[I.8] Fallo de servicios de comunicaciones	2	3	2	2	1	3	6	4	4	2	6
	[E.2] Errores del administrador	1	3	2	2	1	3	3	2	2	1	3
	[E.9] Errores de [re-]encaminamiento	2	3	2	2	1	3	6	4	4	2	6
	[E.15] Alteración accidental de la información	2	3	2	2	1	3	6	4	4	2	6
	[E.19] Fugas de información	2	3	2	2	1	3	6	4	4	2	6
	[A.5] Suplantación de la identidad del usuario	2	3	2	2	1	3	6	4	4	2	6
	[A.6] Abuso de privilegios de acceso	2	3	2	2	1	3	6	4	4	2	6
	[A.7] Uso no previsto	2	3	2	2	1	3	6	4	4	2	6
	[A.9] [Re-]encaminamiento de mensajes	2	3	2	2	1	3	6	4	4	2	6
	[A.11] Acceso no autorizado	2	3	2	2	1	3	6	4	4	2	6
	[A.14] Interceptación de información (escucha)	3	3	2	2	1	3	9	6	6	3	9
[INT_UNIT] Internet de la empresa	[I.8] Fallo de servicios de comunicaciones	2	3	0	0	0	0	6	0	0	0	0
	[E.2] Errores del administrador	1	3	0	0	0	0	3	0	0	0	0

Tabla 18. (Continuación).

NOMBRE Y DESCRIPCION DEL ACTIVO	PROBABILIDAD DE LA AMENAZA		IMPACTO EN SUS DIMENSIONES					RIESGO EN SUS DIMENSIONES				
	AMENAZA SEGÚN MAGERIT	VALOR	D	I	C	A	T	D	I	C	A	T
	[E.9] Errores de [re-]encaminamiento	2	3	0	0	0	0	6	0	0	0	0
	[E.15] Alteración accidental de la información	2	3	0	0	0	0	6	0	0	0	0
	[E.19] Fugas de información	2	3	0	0	0	0	6	0	0	0	0
	[A.5] Suplantación de la identidad del usuario	2	3	0	0	0	0	6	0	0	0	0
	[A.6] Abuso de privilegios de acceso	2	3	0	0	0	0	6	0	0	0	0
	[A.7] Uso no previsto	2	3	0	0	0	0	6	0	0	0	0
[EDIF_SEDE] Edificio sede de la empresa.	[N.1] Fuego	1	5	0	0	0	0	5	0	0	0	0
	[N.2] Daños por agua (inundaciones)	1	5	0	0	0	0	5	0	0	0	0
	[I.2] Daños por agua (accidental)	1	5	0	0	0	0	5	0	0	0	0
	[E.19] Fugas de información	1	5	0	0	0	0	5	0	0	0	0
	[A.11] Acceso no autorizado	1	5	0	0	0	0	5	0	0	0	0
	[A.26] Ataque destructivo	1	5	0	0	0	0	5	0	0	0	0
	[A.27] Ocupación enemiga	1	5	0	0	0	0	5	0	0	0	0

Fuente: Autor.

7.3 CONTROLES PARA MITIGAR LOS RIESGOS.

Luego de efectuado el análisis de riesgos de los activos de información de UNITRANSA S.A. se puede finiquitar que la mayoría de ellos poseen un nivel de riesgo Muy Bajo (MB) seguido del nivel Bajo (B) y solo un pequeño porcentaje tienen un nivel Alto (A) o Muy Alto(MA).

Para efectos de determinar los controles necesarios para mitigar los riesgos más relevantes siguiendo la Norma ISO 27002, se tuvieron en cuenta los activos con clasificación de riesgos B, M, A y MA, toda vez que estamos ante una empresa pequeña y podrían solventarse estos riesgos con relativa factibilidad. Cabe anotar que el presente trabajo está enmarcado dentro del Control 5. Política y el Control 8. Activos. La Tabla21 muestra los activos a gestionar y los controles de la norma ISO 27002 que se deben aplicar.

Tabla 19. Controles ISO 27002 a aplicar a los riesgos.

NOMBRE Y DESCRIPCION DEL ACTIVO	AMENAZA SEGÚN MAGERIT	RIESGO SEGÚN DIMENSION			CONTROL SEGÚN ISO 27002
		D	I	C	
[INFO_SOC] Información Socios y proveedores	[E.19] Fugas de información			B	5. Políticas. 7. Recursos humanos.
	[A.19] Divulgación de información.			B	5. Políticas.
[INFO_NIIF] Información Contable de la empresa	[E.19] Fugas de información			B	5. Políticas. 7. Recursos humanos.
	[A.19] Divulgación de información			B	5. Políticas.
[COD_FTE] Código fuente de aplicativos.	[E.15] Alteración accidental de la información		B	B	7. Recursos humanos.
	[E.19] Fugas de información			B	5. Políticas. 7. Recursos humanos.
[DOC_PROY] Documentación de proyectos	[E.19] Fugas de información			B	5. Políticas. 7. Recursos humanos.
	[A.19] Divulgación de información			B	7. Recursos humanos.
[DOC_EST] Documentación estratégica	[E.19] Fugas de información			B	5. Políticas. 7. Recursos humanos.
	[A.19] Divulgación de información			B	7. Recursos humanos.
[U_INTER] Usuarios Internos de UNITRANSA S.A. (empleados	[E.19] Fugas de información			B	5. Políticas. 7. Recursos humanos.
	[A.28] Indisponibilidad del personal	B			7. Recursos humanos.
	[A.30] Ingeniería social (picaresca)		MB	B	5. Políticas. 7. Recursos humanos.
	[E.1] Errores de los usuarios		B	B	7. Recursos humanos.
	[E.15] Alteración accidental de la información		B	B	7. Recursos humanos.

Tabla 19. (Continuación).

NOMBRE Y DESCRIPCION DEL ACTIVO	AMENAZA SEGÚN MAGERIT	RIESGO SEGÚN DIMENSION			CONTROL SEGÚN ISO 27002
		D	I	C	
[F_VARIOS] Archivos varios de UNITRANSA S.A	[E.19] Fugas de información			B	5. Políticas.
	[A.5] Suplantación de la identidad del usuario			B	5. Políticas.
	[A.15] Modificación deliberada de la información		B	B	5. Políticas.
	[A.18] Destrucción de información (intencional)	B			5. Políticas.
	[A.19] Divulgación de información			B	5. Políticas.
[LOG_UN] Registro de actividades del sistema	[E.18] Destrucción de información (accidental)	B			7. Recursos humanos.
	[A.18] Destrucción de información (intencional)	B			5. Políticas.
[GEST_INT] Datos de gestión de la empresa	[E.18] Destrucción de información (accidental)	B			7. Recursos humanos.
	[E.19] Fugas de información			B	5. Políticas.
[SRV_BD] Equipo Servidor de Bases de Datos	[N.1] Fuego	B			11. Física y ambiental.
	[N.2] Daños por agua (inundaciones)	B			11. Física y ambiental.
	[A.25] Robo	B			8. Activos. 11. Física y ambiental.
	[A.26] Ataque destructivo	B			11. Física y ambiental.
[PC1] Computadora de Gerencia	[N.1] Fuego	B			11. Física y ambiental.
	[I.2] Daños por agua (escapes, fugas)	B			11. Física y ambiental.
	[A.25] Robo	B			8. Activos. 11. Física y ambiental.
	[A.26] Ataque destructivo	B			11. Física y ambiental.
[PC2] Computadora de Dpto. Jurídico	[A.25] Robo	B			8. Activos. 11. Física y ambiental.
	[A.26] Ataque destructivo	B			11. Física y ambiental.
[PC3] Puestos de trabajo	[N.1] Fuego	B			11. Física y ambiental.
	[I.2] Daños por agua (escapes, fugas)	B			11. Física y ambiental.
	[I.5] Avería de origen físico o lógico	B	B	MB	5. Políticas. 8. Activos. 7. Recursos humanos.
	[A.26] Ataque destructivo	B			11. Física y ambiental.
[FRW] Firewall	[A.26] Ataque destructivo	B			11. Física y ambiental.
	[A.24] Denegación de servicio	B			5. Políticas.
		B			7. Recursos humanos

Tabla 19. (Continuación).

NOMBRE Y DESCRIPCION DEL ACTIVO	AMENAZA SEGÚN MAGERIT	RIESGO SEGÚN DIMENSION			CONTROL SEGÚN ISO 27002
		D	I	C	
[RTR] Router Netgear 4g Lte Router Lg2200d	[A.24] Denegación de servicio	B			5. Políticas. 7. Recursos humanos.
	[A.25] Robo	B			8. Activos 11. Física y ambiental.
	[A.26] Ataque destructivo	B			11.Física y ambiental.
[SRV_APP] Servidor de aplicaciones utilizadas en la empresa	[I.5] Avería de origen físico o lógico	B	B	MB	5. Políticas.
	[A.11] Acceso no autorizado	B	B	B	5. Políticas. 7. Recursos humanos.
	[A.24] Denegación de servicio	B			5. Políticas.
[BD_ORC] Manejador de Base de Datos Oracle	[A.19] Divulgación de información			B	14. Adquisición desarrollo y mantenimiento.
[SO_WINDXP] Sistema Operativo Windows XP	[I.5] Avería de origen físico o lógico	M	M	M	7. Recursos humanos. 14. Adq. desarrollo y mantenimiento.
	[E.18] Destrucción de información (accidental)	M			14. Adq. desarrollo y mantenimiento.
	[E.20] Vulnerabilidades de los programas (software)	MA	MA	MA	14. Adq. desarrollo y mantenimiento
	[E.21] Errores de mantenimiento / actualización de programas (software)	MA	MA	MA	5. Políticas. 7. Recursos humanos 14. Adq. desarrollo y mantenimiento.
	[A.22] Manipulación de programas	M	M	M	11. Física y ambiental.
[CTR_TEMP] Equipos de climatización	[N.1] Fuego	B			14. Adq. desarrollo y mantenimiento.
	[I.5] Avería de origen físico o lógico	B			11. Física y ambiental.
	[A.25] Robo	B			11. Física y ambiental.
	[A.26] Ataque destructivo				11. Física y ambiental.
[UPS] Sistema de alimentación ininterrumpida	[N.1] Fuego	B			11. Física y ambiental.
	[A.25] Robo		B		11. Física y ambiental.
[GEN_ELECT] Generador de energia	[N.1] Fuego	B	B		11. Física y ambiental.
	[N.2] Daños por agua	B	B		14. Adq. desarrollo y mantenimiento.
	[I.5] Avería de origen físico o lógico	B	B		13. Telecomunicaciones.
	[I.8] Fallo de servicios de comunicaciones	A	M	M	7. Recursos humanos. 13. Telecomunicaciones.

Tabla 19. (Continuación).

NOMBRE Y DESCRIPCION DEL ACTIVO	AMENAZA SEGÚN MAGERIT	RIESGO SEGÚN DIMENSION			CONTROL SEGÚN ISO 27002
		D	I	C	
[NET_UNIT] Red local de UNITRANSA S.A.	[E.2] Errores del administrador	B	B	B	13. Telecomunicaciones.
	[E.9] Errores de [re-]encaminamiento		M	A	5. Políticas 13. Telecomunicaciones.
	[E.19] Fugas de información			A	5. Políticas y 13. Telecomunicaciones.
	[A.5] Suplantación de la identidad del usuario		A	A	5. Políticas. 13. Telecomunicaciones.
	[A.6] Abuso de privilegios de acceso	A	A	A	5. Políticas.
	[A.7] Uso no previsto	A			5. Políticas.
	[A.11] Acceso no autorizado		A	A	5. Políticas. 13. Telecomunicaciones.
	[A.14] Interceptación de información (escucha)			MA	13. Telecomunicaciones.
[INT_UNIT] Internet de la empresa	[I.8] Fallo de servicios de comunicaciones	A	M	M	7. Recursos humanos.
	[E.2] Errores del administrador	B	B	B	5. Recursos humanos. 13. Telecomunicaciones.
	[E.9] Errores de [re-]encaminamiento		M	A	5. Políticas. 13. Telecomunicaciones.
	[A.5] Suplantación de la identidad del usuario		A	A	5. Políticas. 13. Telecomunicaciones
	[A.6] Abuso de privilegios de acceso		A	A	5. Políticas.
	[A.7] Uso no previsto	B	MA	MA	11. Físico y ambiental.
[EDIF_SEDE] Edificio sede de la empresa.	[N.1] Fuego	B			11. Físico y ambiental.
	[A.26] Ataque destructivo	B	B		11. Físico y ambiental.

Fuente: Autor.

7.4 SALVAGUARDAS.

Las salvaguardas o contramedidas son todas las acciones o componentes tecnológicos que reducen el riesgo al que están sometidos los activos de información. No es común encontrar sistemas desprotegidos en absoluto; hay amenazas que se mitigan solamente con una organización adecuada, otras necesitan de equipos o elementos software, algunas requieren de seguridad física y otras demandan de una Política de Seguridad de la Información (PSI).

Para mitigar las amenazas de los Activos de Información de UNITRANSA S.A. se tomó el libro 2 de la metodología MAGERIT que presenta una serie de salvaguardas empleadas para cada tipo de activo. Cabe anotar que las salvaguardas afectan el riesgo de dos maneras:

- Reduciendo la probabilidad de amenazas (Salvaguardas preventivas).
- Limitando el daño causado. Este tipo de salvaguardas limitan la posible degradación o detectan el ataque para evitar que la degradación avance.[40] La Tabla 20 muestra las salvaguardas que debe imponerse a cada activo y su descripción.

Tabla 20. Salvaguardas

CODIGO DE ACTIVO MAGERIT	NOMBRE DE ACTIVO MAGERIT	CODIGO DE ACTIVO UNITRANSA S.A.	DESCRIPCION	SALVAGUARDAS	DESCRIPCION
[essential] Activos esenciales					
[vr]	Datos vitales	[INFO_SOC]	Información Socios y proveedores	H.AC	Control de acceso lógico.
				D.A	Copia de seguridad de los datos(backup).
		[IN.FO_NIIF]	Información Contable de la empresa	H.AC	Control de acceso lógico
				D.A	Copia de seguridad de los datos (backup).
				H.tools.AV	Herramientas contra código dañino.
[classified]	Datos clasificados	[COD_FTE]	Código fuente de aplicativos	H.AC	Control de acceso lógico.
				SW.A	Copias de seguridad (backup).
				H.tools.AV	Herramientas contra condigo dañino.
		[DOC_PROY]	Documentación de proyectos	H.AC	Control de acceso lógico.
				H.tools.AV	Herramientas contra código dañino.
				D.A	Copias de seguridad de los datos(backup).

[40]Consejo Superior de Administración Electrónica. MAGERIT_V3_libro1_capitulo 3. 31p

Tabla 20. (Continuación).

CODIGO DE ACTIVO MAGERIT	NOMBRE DE ACTIVO MAGERIT	CODIGO DE ACTIVO UNITRANSA S.A.	DESCRIPCION	SALVAGUARDAS	DESCRIPCION
				D.I	Aseguramiento de la integridad.
		[DOC_EST]	Documentación estratégica	H.AC	Control de acceso lógico.
				H.tools.AV	Herramientas contra código dañino.
				D.A	Copias de seguridad de los datos(backup).
				D.I	Aseguramiento de la integridad.
[P]Personal					
[ui]	Usuarios internos	[U_INTER]	Usuarios Internos de UNITRANSA S.A. (empleados).	PS.AT	Formación y concienciación
				PS.A	Aseguramiento de la disponibilidad.
[adm]	administradores	[ADMIN_UN]	Administrador de la empresa.	PS.AT	Formación y concienciación.
[prov]	Proveedores	[PROV_UN]	Proveedores de UNITRANSA S.A.	PS.AT	Formación y concienciación.
[soc]	Socios	[SOC_UN]	Socios UNITRANSA S.A.	PS.AT	Formación y concienciación.
[D] Datos/Información					
[files]	Ficheros	[F_VARIOS]	Archivos varios de UNITRANSA S.A.	H.AC	Control de acceso lógico.
				H.tools.AV	Herramientas contra código dañino.
				D.A	Copias de seguridad de los datos (backup).

Tabla 20. (Continuación).

CODIGO DE ACTIVO MAGERIT	NOMBRE DE ACTIVO MAGERIT	CODIGO DE ACTIVO UNITRANSA S.A.	DESCRIPCION	SALVAGUARDAS	DESCRIPCION
[backup]	Copias de respaldo	[BACK_UN]	Archivos de respaldo de información de la empresa	H.AC	Control de acceso lógico.
				D.A	Copias de seguridad de los datos (backup)
				D.I	Aseguramiento de la integridad.
[conf]	Datos de configuración	[CONF_EQ]	Datos de configuración de equipos	H.tools.CC	Herramienta de chequeo de configuración.
[password]	Credenciales	[PSW_US]	Credenciales de usuarios del sistema	H.tools.AV	Herramientas contra código dañino.
				H.AC	Control de acceso lógico.
				D.I	Aseguramiento de la integridad.
[log]	Registro de actividad	[LOG_UN]	Registro de actividad del sistema	H.tools.LA	Herramienta para el análisis de logs.
[int]	Datos de gestión interna	[GEST_INT]	Datos de gestión de la empresa	H.AC	Control de acceso lógico.
				D.A	Copias de seguridad de los datos (backup)
				D.I	Aseguramiento de la integridad.
[HW]Equipos Informáticos					
[host]	Grandes equipos	[SRV_BD]	Equipo Servidor de Bases de Datos	HW.A	Aseguramiento de la disponibilidad.
				HW. Op.	Operación.
				HW.CM	Cambios (actualizaciones y mantenimiento).
				H.AC	Control de acceso lógico.

Tabla 20. (Continuación).

CODIGO DE ACTIVO MAGERIT	NOMBRE DE ACTIVO MAGERIT	CODIGO DE ACTIVO UNITRANSA S.A.	DESCRIPCION	SALVAGUARDAS	DESCRIPCION
[mid]	Equipos medios	[PC1]	Computadora de Gerencia	H.AC	Control de acceso lógico.
				HW.A	Aseguramiento de la disponibilidad.
				HW.CM	Cambios (actualizaciones y mantenimiento).
				HW.SC	Se aplican perfiles de seguridad.
[pc]	Informática personal	[PC2]	Computadora de Dpto. Jurídico	H.AC	Control de acceso lógico.
				HW.A	Aseguramiento de la disponibilidad.
				HW.CM	Cambios (actualizaciones y mantenimiento).
				HW.SC	Se aplican perfiles de seguridad.
[pc]	Informática personal	[PC3]	Puestos de trabajo	H.AC	Control de acceso lógico.
				HW.CM	Cambios (actualizaciones y mantenimiento).
				HW.A	Aseguramiento de la disponibilidad.
[print]	Medios de impresión	[IMP]	Impresora	HW.print	Reproducción de documentos.

Tabla 20. (Continuación).

CODIGO DE ACTIVO MAGERIT	NOMBRE DE ACTIVO MAGERIT	CODIGO DE ACTIVO UNITRANSA S.A.	DESCRIPCION	SALVAGUARDAS	DESCRIPCION
[firewall]	Cortafuegos	[FRW]	Firewall	HW.A	Aseguramiento de la disponibilidad.
[switch]	Conmutadores	[SW_P1]	Switch Ethernet Gigabit Linksys SE4008 WRT de 8 puertos (1er. Piso).	HW.A	Aseguramiento de la disponibilidad.
		[SW_P2]	Switch Linksys SE3016 de 16 puertos (2º. Piso).	HW.A	Aseguramiento de la disponibilidad.
		[SW_P3]	Switch Linksys SE4008 WRT de 8 puertos (3er. Piso)	HW.A	Aseguramiento de la disponibilidad.
[router]	Encaminadores	[RTR]	Router Netgear 4g Lte Router Lg2200d	HW.A	Aseguramiento de la disponibilidad.
				H.tools.IDS	IDS/IPS: Herramienta de detección / prevención de intrusión.
				HW.CM	Cambios (actualizaciones y mantenimiento).
[SW]Aplicaciones					
[app]	Servidor de aplicaciones	[SRV_APP]	Servidor de aplicaciones utilizadas en la empresa	S.A	Aseguramiento de la disponibilidad.
				S.emael	Protección del correo electrónico.
				S.dir	Protección del directorio.

Tabla 20. (Continuación).

CODIGO DE ACTIVO MAGERIT	NOMBRE DE ACTIVO MAGERIT	CODIGO DE ACTIVO UNITRANSA S.A.	DESCRIPCION	SALVAGUARDAS	DESCRIPCION
				S.dns	Protección del servidor de nombre de doniminio (DNS).
[dbms]	Sistema de gestión de bases de datos	[BD_ORC]	Manejador de Base de Datos Oracle	SW.A	Copias de seguridad (backup).
				SW.CM	Cambios (actualizaciones y mantenimiento).
				H.AC	Control de acceso lógico.
				H.tools.AV	Herramienta contra código dañino.
[os]	Sistema Operativo	[SO_WIND7]	Sistema Operativo Windows 7 Profesional	H.tools.CC	Herramienta de chequeo de configuración.
				H.tools.VA	Herramienta de analisis de vulnerabilidades.
				SW.A	Copias de seguridad (backup).
				SW.CM	Cambios (actualizaciones y mantenimiento).
[os]	Sistema Operativo	[SO_WIND8]	Sistema Operativo Windows 8	H.tools.CC	Herramienta de chequeo de configuración.
				H.tools.VA	Herramienta de analisis de vulnerabilidades.
				SW.A	Copias de seguridad (backup).

Tabla 20. (Continuación).

CODIGO DE ACTIVO MAGERIT	NOMBRE DE ACTIVO MAGERIT	CODIGO DE ACTIVO UNITRANSA S.A.	DESCRIPCION	SALVAGUARDAS	DESCRIPCION
				SW.CM	Cambios (actualizaciones y mantenimiento).
[os]	Sistema Operativo	[SO_WINDXP]	Sistema Operativo Windows XP	H.tools.CC	Herramienta de chequeo de configuración.
				H.tools.VA	Herramienta de analisis de vulnerabilidades.
				SW.A	Copias de seguridad (backup).
				SW.CM	Cambios (actualizaciones y mantenimiento).
[office]	Ofimática	[ADOB_DW]	Editor HTML: Adobe Dreamweaver	H.tools.AV	Herramienta contra código dañino.
				SW.A	Copias de seguridad (backup).
				SW.CM	Cambios (actualizaciones y mantenimiento).
[office]	Ofimática	[ARTIS]	Plantillas web: Artister	H.tools.AV	Herramienta contra código dañino.
				SW.A	Copias de seguridad (backup).
				SW.CM	Cambios (actualizaciones y mantenimiento).

Tabla 20. (Continuación).

CODIGO DE ACTIVO MAGERIT	NOMBRE DE ACTIVO MAGERIT	CODIGO DE ACTIVO UNITRANSA S.A.	DESCRIPCION	SALVAGUARDAS	DESCRIPCION
[office]	Ofimática	[ADOB_FW]	Editor de imágenes web: Adobe Fireworks	H.tools.AV	Herramienta contra código dañino.
				SW.A	Copias de seguridad (backup).
				SW.CM	Cambios (actualizaciones y mantenimiento).
[office]	Ofimática	[LOG_CR]	Diseño de logos: Logo Creator	H.tools.AV	Herramienta contra código dañino.
				SW.A	Copias de seguridad (backup).
				SW.CM	Cambios (actualizaciones y mantenimiento).
[email_client]	Cliente de correo electrónico	[CLT_FTP]	Cliente FTP: Filezilla	S.email	Protección del correo electrónico
				H.tools.AV	Herramienta contra código dañino.
[prp]	Desarrollo propio	[DES_PROPIO]	Aplicaciones de desarrollo propio	SW.A	Copias de seguridad (backup).
				SW.start	Puesta en producción.
				H.AC	Control de acceso lógico.
[av]	Anti virus	[ANT_VIRUS]	Antivirus	SW.A	Copias de seguridad (backup).
				SW.CM	Cambios (actualizaciones y mantenimiento).

Tabla 20. (Continuación).

CODIGO DE ACTIVO MAGERIT	NOMBRE DE ACTIVO MAGERIT	CODIGO DE ACTIVO UNITRANSA S.A.	DESCRIPCION	SALVAGUARDAS	DESCRIPCION
[AUX]Equipamiento auxiliar					
[ups]	Sistemas de alimentación ininterrumpida	[UPS]	Sistema de alimentación ininterrumpida	AUX.A	Aseguramiento de la disponibilidad.
[cabling]	Cableado	[CABL]	Cableado	AUX.wires	Protección del cableado.
[ac]	Equipos de climatización	[CTR_TEMP]	Equipos de climatización	AUX.A	Aseguramiento de la disponibilidad.
[gen]	Generadores eléctricos	[GEN_ELECT]	Generador de energia	AUX.power	Suministro eléctrico.
[COM]Redes de comunicación					
[lan]	Red local	[NET_UNIT]	Red local de UNITRANSA S.A.	COM.A	Aseguramiento de la disponibilidad.
				COM.I	Protección de la integridad de los datos intercambiados.
				COM.CM	Cambios (actualizaciones y mantenimiento).
[internet]	Internet	[INT_UNIT]	Internet de la empresa	COM.A	Aseguramiento de la disponibilidad.
				COM.I	Protección de la integridad de los datos intercambiados.

Tabla 20. (Continuación).

CODIGO DE ACTIVO MAGERIT	NOMBRE DE ACTIVO MAGERIT	CODIGO DE ACTIVO UNITRANSA S.A.	DESCRIPCION	SALVAGUARDAS	DESCRIPCION
				COM.CM	Cambios (actualizaciones y mantenimiento)
[L]Instalaciones					
[building]	edificio	[EDIF_SEDE]	Edificio sede de la empresa.	L.depth	Defensa en profundidad
				L.AC	Control de accesos físicos.
				L.A	Aseguramiento de la disponibilidad.

Fuente: Autor.

8. METODOLOGÍA DE INVENTARIO DE ACTIVOS DE INFORMACIÓN PROPUESTA PARA UNITRANSA S.A.

Conocido el inventario de Activos de Información de la empresa, se evidencia que no existe un mecanismo de control de inventario que permita incorporar, dar de baja y/o cambiar de ubicación alguno de ellos. Considerando la información como uno de los activos más importantes para toda organización y los elementos que la soportan, procesan y transmiten como de vital importancia para todos los procesos, es pertinente recomendar se implemente un sistema que facilite llevar a cabo cada una de las tareas antes descritas con relación a los activos de información, donde se guarde los datos relacionados con fecha, tipo de activo, código del activo, departamento al que pertenece, modo de incorporación o de baja, responsable, entre otros, de la modificación del inventario de activos de información de UNITRANSA S.A. en un momento determinado.

La información de la empresa está guardada en papel, sistemas computacionales (Bases de Datos y archivos ofimáticos), imágenes, etc. y tiene además un ciclo de vida que inicia con la creación, pasando por el procesamiento, uso y finaliza con la destrucción. El cuidado que conlleva la gestión de la información depende en gran medida de la criticidad, disponibilidad, autenticidad y confidencialidad.

Los Activos de Información actuando como soporte de todos los procesos llevados a cabo en el funcionamiento de la empresa, requieren de un sistema de gestión sistemático que permita asignar responsabilidades, especificar funciones, ordenar tareas y facilitar el control de incidentes. Por lo anterior se propone un mecanismo de control de inventario de activos de información compuesto por tres procesos:

8.1 PROCESO DE INCORPORACIONES DE ACTIVOS DE INFORMACIÓN.

Correspondiente a la vinculación de Activos de Información al inventario de activos de UNITRANSA S.A. Este proceso se inicia con la adquisición del activo por parte de la empresa, continuando con su valoración, donde se analiza la importancia para los procesos de la organización, las vulnerabilidades existentes y el impacto que significaría la materialización de incidentes de seguridad sobre él, para de esta manera determinar los controles adecuados que mitiguen los riesgos a los que está expuesto.

8.1.1 Valoración de nuevos activos de información. La implementación de controles sobre los nuevos activos de información requiere de un análisis exhaustivo que involucre entre otros los siguientes aspectos:

- **Tipo de información**. Determinar si la información que contendrá el activo será pública o privada.
- **Importancia del activo**. Establecer el grado de relevancia del activo para los procesos de la empresa. Esta puede ser Alta, Media o Baja.

- **Ciclo de vida**. Estipular el ciclo de vida útil del Activo de Información que puede ser de corto plazo (no mayor a un año), mediano plazo (de dos a tres años) o largo plazo (mayor a cinco años).
- **Cuidados requeridos**. Fijar los cuidados necesarios para mantener la integridad, confidencialidad y trazabilidad del Activo de Información. Estos pueden ser: ciclos de mantenimiento, control de acceso, temperatura controlada, monitoreo permanente, entre otros.
- **Tipo de vulnerabilidades**. Acordar las vulnerabilidades que experimenta el activo.
- **Tipo de amenazas**. Estudiar las amenazas a las que se expone el activo de información.

Luego de realizado el análisis del nuevo Activo de Información a vincularse al inventario de activos de UNITRANSA se recomienda el llenado del formato de altas (Anexo A), el cual contiene entre otros los siguientes campos:

- **Fecha de alta.** Corresponde a la fecha en que se vincula el activo al inventario de activos del departamento establecido por parte de la gerencia de la empresa.
- **Departamento**. Departamento al que se vincula el activo.
- **Modo de incorporación**. Se debe marcar con “X” la forma como se vincula el nuevo activo (Tabla22).
- **Responsable**. Nombre y apellidos de la persona responsable del departamento al que se le asigna el nuevo activo.
- **Documento de identificación**. Identificación de la persona que debe responder por el activo de información.
- **Propietario**. Nombre y apellidos de la persona a la cual se asignará el activo de información.
- **Documento de identificación**. Identificación de la persona que oficiará como usuario del activo de información.
- **Descripción del activo**. Texto que identifique brevemente el activo.
- **Código asignado**. Todos los activos deben llevar un código previamente establecido que lo identifique inequívocamente.
- **Suministrador**. Debe colocarse en este campo el nombre de la persona o empresa que lo vendió, cedió, alquiló, contrató o lo produjo (cuando se trata de un producto intelectual).
- **Fecha de adquisición**. Corresponde a la fecha en que UNITRANSA S.A. adquirió el activo, aun sin ser asignado a ningún departamento.

Tabla 21. Tipo de incorporación

CÓDIGO	TIPO DE INCORPORACIÓN
I1	Compra
I2	Alquiler
I3	Cesión
I4	Contratación
I5	Contrato laboral
I6	Producto intelectual

Nota fuente: Enríquez Espinosa, P.R. (2013). Implementación de los controles asignados al dominio "gestión de activos", bajo los lineamientos establecidos por la norma ISO/27001 anexo a, para las empresas municipales de Cali, Emcali e.i.c.e-esp (p.94). Santiago de Cali. Universidad Autónoma de Occidente.

El proceso de Incorporación de Activos de Información finaliza cuando el administrador de activos de UNITRANSA S.A. coloca su firma en el documento Formato de Incorporación, teniendo en cuenta que la fecha de vinculación del nuevo activo debe ser la misma en que se recibe la solicitud mediante el formato debidamente diligenciado.

8.1.2 Proceso de traslado o traspaso de Activos de Información. Corresponde a la acción de cambiar de ubicación y/o de destinación de un Activo de Información sin cambiar de departamento (traslado) y la operación de reasignar un Activo de Información a otro departamento (traspaso). Este procedimiento requiere, cuando el asunto es un traspaso de Activo de Información, el cambio de responsable del activo y el cambio de propietario del mismo. Cuando se trate de un traslado de Activo de Información, solo requerirá de cambio de propietario.

Nota 1. Propietario de Activo de Información. Individuo o entidad que tiene la responsabilidad, designada por la gerencia, de controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos[41].

Nota 2. Responsable del Activo de Información. También conocido como custodio, representa a la persona, cargo o grupo de trabajo dentro de la organización que es responsable de definir los controles, el mantenimiento y el uso aceptable de los activos de Información de dicho sector de la organización.

El proceso de traslado o traspaso de Activos de Información conlleva el diligenciamiento del formato de traslado y traspaso (Anexo C), el cual contiene los siguientes campos:

- **Consecutivo No.** Número de orden de este tipo de procesos realizados.

[41] ICONTEC. NORMA TÉCNICA NTC-ISO/IECCOLOMBIANA 27001 [online]. Disponible en Internet: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

- **Fecha de solicitud**. Fecha en la que se solicita el traslado o traspaso del Activo de Información.
- **Proceso**. Debe marcarse con una “X” la casilla correspondiente al tipo de proceso, ya sea traslado o traspaso.
- **Código anterior del activo**. En este campo se registra el código del activo asignado por la administración de activos de UNITRANSA S.A. cuando lo incorporó al inventario de activos del departamento asignado.
- **Nuevo código del activo**. Registra el código que se le asigna a efectos de su vinculación al nuevo departamento, esto cuando el proceso es un traspaso. Cuando el proceso corresponde a un traslado, se deja el espacio en blanco o se escribe el mismo código en los dos campos (Código anterior del activo y Nuevo código del activo).
- **Descripción del activo**. Breve texto que identifica al Activo de Información.
- **Etiqueta del activo**. Etiqueta que identifica toda la información relacionada con el activo.
- **Código departamento origen**. Código que identifica al departamento al cual pertenece el activo.
- **Código departamento destino**. Código que identifica al departamento al que pertenecerá el activo, cuando el proceso es un traspaso. Cuando el proceso es un traslado se deja este campo en blanco o se escribe el mismo código.
- **Aprobado**. Se debe colocar una “X” en la casilla “SI” cuando la aprobación es aceptada y una “X” en la casilla “NO” cuando la aprobación es denegada.
- **Fecha**. Fecha en la que se acepta o deniega la solicitud.
- **Firma**. Firma del Administrador de Activos de UNITRANSA S.A.
- **Propietario anterior (código).** Código de la persona a la cual está asignado el Activo de Información.
- **Propietario anterior (nombre).** Nombres y apellidos de la persona que tiene asignado el Activo de Información.
- **Responsable anterior (código).** Código de la persona responsable del activo, del departamento al cual pertenece.
- **Responsable anterior (nombre).** Nombres y apellidos de la persona responsable del activo, del departamento al cual pertenece.
- **Propietario actual (código).** Código de la persona a la que se le asigna el Activo de Información.
- **Propietario actual (nombre)**. Nombres y apellidos de la persona a la que se le asigna el Activo de Información.
- **Responsable actual (código).** Código de la persona responsable del activo de Información, del departamento al cual pertenece.
- **Responsable actual (nombre).** Nombre y apellidos de la persona del departamento al cual pertenece el activo y que tiene la responsabilidad de velar por el uso aceptable que se dé al Activo de Información.

El Proceso de Traslado o Traspaso de Activos de Información se concreta cuando el administrador de activos de UNITRANSA S.A. coloca su firma en el documento Formato de Traslado o Traspaso y se hace efectivo a partir de la fecha escrita en el campo fecha del apartado aprobación.

8.1.3 Proceso de bajas de Activos de Información. Corresponde a la desvinculación del inventario de activos de UNITRANSA S.A. de aquellos activos de información que dejarán de intervenir en los diferentes procesos de la empresa.

El administrador de activos de UNITRANSA S.A., junto con el gerente, determinarán, luego de un estudio técnico y administrativo, cuales o cual activo de Información, termina su vida útil para dar paso a otro de mayor tecnología (hardware) y/o mayor robustez (software). La Tabla22 muestra las maneras por las que un Activo de Información sale del Inventario de Activos.

Tabla 22. Tipos de Bajas

CÓDIGO	ARGUMENTO
BJ1	Venta
BJ2	Deterioro
BJ3	Hurto
BJ4	Extravío
BJ5	Término de contrato
BJ6	Fin de vida útil de la información.

Nota Fuente: Enríquez Espinosa, P.R. (2013). Implementación de los controles asignados al dominio "gestión de activos", bajo los lineamientos establecidos por la norma ISO/27001 anexo a, para las empresas municipales de Cali, Emcali e.i.c.e-esp (p.88). Santiago de Cali. Universidad Autónoma de Occidente.

El argumento por el cual se da de baja un activo de información de UNITRANSA S.A. debe estar debidamente sustentado.

- **Argumentación de venta**. Se debe anexar copia del documento de venta y certificado de Borrado Seguro, expedido por el departamento técnico.

Borrado Seguro en Windows. Al borrar un archivo de una computadora o dispositivo móvil, este no se elimina físicamente, lo que hace Windows es sólo borrar los punteros de los datos, es decir las indicaciones de los espacios físicos del disco rígido donde comienza y donde termina el archivo, en conclusión, no elimina el archivo ni su información. A menos que se escriba algo nuevo podría recuperarse los datos.

Esta situación constituye un verdadero riesgo para la seguridad de la información de una empresa, ya que como es habitual vender e incluso regalar los dispositivos viejos cada vez que se adquieren nuevos equipos o traspasar los de los ejecutivos a empleados, sin percatarse de que puedan contener información sensible que en manos equivocadas podrían hacer mucho daño a la organización.

El proceso de borrado seguro puede aplicarse a cualquier dispositivo de almacenamiento, llámese disco duro, pendrive, Smartphone, etc. Existen tres tipos de borrado seguro:

1. **Limpieza**. Consiste en la sobre escritura de datos o wiping. Se fundamenta en escribir nueva información sobre el lugar donde se encontraban los archivos borrados, evitando así su recuperación.
2. **Saneamiento**. Se basa en eliminar los datos de forma tal que no puedan ser recuperados de ninguna forma, como la desmagnetización de dispositivos, que consiste en la utilización de imanes de gran potencia para borrar la información y el encriptado de discos, que utiliza un código para hacer ilegible la información. De este mismo sistema de saneamiento forman parte las aplicaciones software desarrolladas para tal fin como CCleaner y Sdelete, entre otras.
3. **Destrucción controlada de medios.** Es muy segura, se aplica a elementos que terminaron su vida útil y que manejaron información clasificada. Algunos de estos métodos son la trituración, incineración de equipos, aplicación de productos químicos, aplicación de voltajes muy altos, etc.[42]

- **Argumentación de deterioro.** Se debe anexar un documento expedido por el departamento técnico de UNITRANSA S.A. que especifique de manera clara los motivos por los cuales se debe dar de baja el Activo de Información en razón a sus fallas técnicas.
- **Argumentación de hurto.** Debe ir acompañada de una copia de la denuncia interpuesta ante la autoridad competente por el hurto del Activo de Información.
- **Argumentación de extravío.** Debe incorporar el informe del custodio o responsable del Activo de Información, donde explique de manera clara las circunstancias de modo, tiempo y lugar de su extravío.
- **Argumentación del fin de vida útil de la información**. Debe contener el informe de la gerencia de la empresa donde ordena dar de baja el Activo de Información por término de su vida útil.

El proceso de bajas de Activos de Información conlleva el diligenciamiento del formato de bajas (Anexo B), el cual contiene los siguientes campos:

- **Consecutivo No**. Número de orden de procesos de bajas realizados.
- **Fecha.** Fecha en la que se da de baja el Activo de Información.
- **Código del activo**. Código que identifica al activo.

[42]VELAZQUEZ, Andrés. Mattica [26, septiembre, 2011] [online]. Disponible en Internet: http://mattica.com/borrado-seguro-y-destruccion-controlada-de-medios/

- **Tipo de baja.** Marcar con “X” la casilla que corresponda al tipo de baja.
- **Responsable actual.** Nombre y apellidos de la persona responsable del activo.
- **Propietario.** Nombre y apellidos de la persona que figura como usuario del activo.
- **Código del departamento** (dependencia origen). Código asignado al departamento al cual pertenece el activo.
- **Dependencia** (destino). Nombre de la dependencia que almacenará el activo a dar de baja.
- **Nombre y apellido** (soporte técnico). Nombre y apellido del jefe del departamento técnico que avaló el peritaje del activo.
- **Observaciones**. Situaciones que requieren ser plasmadas en el documento.

8.2 ETIQUETADO DE ACTIVOS DE INFORMACIÓN.

Este control se plantea como un complemento a la gestión de activos de la información, buscando fortalecer los mecanismos adoptados para ejercer un control adecuado de las acciones que se realicen sobre ellos, tales como:

- Mantenimiento.
- Control de acceso.
- Uso.
- Controles.
- Importancia para los procesos de la empresa.
- Criticidad de la información que manejan.
- Entre otros.

La Norma ISO/IEC-27001 Anexo A contiene el control **7.2.2 etiquetado y manipulación de la información.** Este control no posee una regulación específica en cuanto a las acciones a tomar por la organización para su implementación, en tal sentido, se considera de libre albedrío la presentación de las soluciones que contribuyan con la seguridad de la información desde la perspectiva de este control.

Luego de un análisis generalizado de la información de la empresa UNITRANSA S.A. y de los equipos considerados de mayor criticidad por albergar información clasificada, siendo estos, el equipo de Gerencia, Secretaría de Gerencia y Departamento Jurídico, planteamos el Etiquetado de Equipos Informáticos como instrumento contributivo a la organización, mantenimiento y seguridad, fundamentado en la base de que los equipos hospedan los programas y los datos sobre los cuales se ejecutan todos los procesos operativos y administrativos de la organización.

8.2.1Objetivo del etiquetado de Activos Informáticos. El objetivo que se persigue con la colocación de una etiqueta de marcado sobre cada uno de los Activos de Información de UNITRANSA S.A. es facilitar su apropiada identificación,

permitiendo la realización de un inventario físico en menor tiempo con una gran exactitud y facilitando las acciones de mantenimiento y seguridad de la información guardada en los equipos de cómputo.

8.2.2 Estructura de la etiqueta de Activos de Información. La etiqueta de Activos de Información consta de los siguientes campos (Figura 15):

- **Nombre en la red**. Corresponde al nombre con el que se identifica el equipo en la red, sea este un pc, una impresora o un router.
- **Código del departamento.** Caracteres que identifican a un departamento. (Tabla23).
- **Criticidad.** Muestra el grado de importancia del Activo de Información para los procesos de UNITRANSA S.A.
- **Propiedades**. Características del Activo de Información relacionadas con uso del equipo y los cuidados que se deben tener con él (Tabla 24). Cuando el activo tiene más de una propiedad, deben anotarse estas en forma seguida, sin dejar espacio entre ellas, ej. P1P3P4.
- **Código del activo**. Número asignado por el Administrador de Inventario de UNITRANSA para identificar inequívocamente al Activo de Información.
- **Código de barras**. Conjunto de líneas paralelas de distinto grosor y espaciado que permiten reconocer un activo de forma única, y así poder consultar sus características asociadas.

Toda la información relacionada con los Activos de Información debe ir relacionada en una Base de Datos, la cual contendrá, entre otros, aspectos como marca, modelo, sistema operativo, aplicaciones, proveedor, fecha de adquisición, fecha de fin de la garantía, departamento al cual pertenece, propietario, custodio, cuidados o recomendaciones de seguridad, etc. Esta información puede ser obtenida a través de un lector de código de barras.

Figura 15. Estructura de la etiqueta

Fuente: Autor.

Figura 16. Ejemplo de etiqueta de marcado

Fuente: Autor.

Tabla 23. Relación Departamento.

DEPARTAMENTO	RELACIÓN
Personal	DPP
Sistemas	DPS
Transito	DPT
Jurídico	DPJ
Médico	DPM
Contabilidad	DPC
Estaciones de servicio	DPE
Mantenimiento	DPM

Fuente: Autor.

Tabla 24. Propiedades de Activos.

PROPIEDAD	CÓDIGO
Propiedad que indica que el Activo requiere protección	P1
Propiedad que revela que el Activo tiene un limitado número de usuarios.	P2
Propiedad que demuestra que el Activo es crítico para los procesos de UNITRANSA S.A.	P3
Propiedad que señala que el Activo es muy crítico para los procesos de la organización.	P4

Fuente: Autor.

8.3 ESTRATEGIA DE SENSIBILIZACIÓN A LOS USUARIOS DEL SISTEMA DE UNITRANSA S.A. RESPECTO A LA PROTECCIÓN DE LA INFORMACIÓN Y LOS ACTIVOS.

La mayoría de los usuarios de un sistema de información de una empresa, desconocen el término “seguridad de la información”, especialmente la gravedad del tema. Si se realizara un cuestionario a los funcionarios de una organización y se formularan preguntas como: ¿Qué es un IDS?, ¿Qué es un análisis de riesgos?, ¿Qué es una IPS?, ¿Cuál es la diferencia entre hacker y cracker?, ¿Qué es un Firewall?, ¿Qué objetivo tiene el malware?, ¿Qué es spam?, ¿Qué es spyware?, ¿Qué es un exploit?, ¿Qué es un servidor proxy?, ¿Qué es un activo de información?, ¿Qué tipos de activos de información hay en una empresa?, ¿Qué significa SGSI?, ¿Qué es criptografía?; las respuestas obtenidas no siempre son las más acertadas.

Se estima que más del 80% de los ataques a un sistema de información se origina desde el interior de la organización, por diferentes razones, tales como empleados descontentos, falta de sentido de pertenencia, negligencia, desconocimiento normativo, motivación económica, falta de capacitación, ingeniería social, etc. En muchas ocasiones es más fácil descubrir la contraseña de usuario de la red interna recorriendo los equipos y observando los papeles pegados en el monitor, que tratando de vulnerar el sistema para descubrirla y descifrarla.

El aseguramiento de los Activos de Información planteado a la empresa UNITRANSA S.A. no alcanzaría los objetivos trazados si no se diseña, ejecuta y supervisa un plan de sensibilización a los usuarios del sistema, teniendo en cuenta que en la larga cadena de elementos que intervienen en la seguridad de la información, siempre se considera a los usuarios como el eslabón más débil, pues son ellos quienes interactúan con el mismo y explotan las vulnerabilidades existentes. Identificar la criticidad de los activos para los procesos de la empresa a partir de la etiqueta de marcado, conocer y aplicar la Política de Seguridad de la Información (PSI), desempeñar adecuadamente el rol asignado y asumir un verdadero sentido de pertenencia, son los pilares fundamentales para lograr la seguridad de los Activos de Información y por ende de la información contenida en ellos.

El plan de sensibilización de empleados de UNITRANSA S.A. debe contener, entre otros, los siguientes aspectos:

- **Objetivo general.** Concientizar e involucrar a funcionarios de UNITRANSA S.A. de la importancia de asumir la seguridad de la información como un compromiso personal con el fortalecimiento y posicionamiento de la empresa dentro del sector transporte en el departamento de Santander.
- **Objetivos específicos**. Contribuyen al logro del objetivo general:
    - Brindar capacitación técnica sobre seguridad de la información.

    - Promover cambios en la cultura de los usuarios del sistema, relacionados con la seguridad de la información.
    - Asignar roles de seguridad de la información.
    - Estimular la incorporación de aptitudes que permitan disminuir la ocurrencia de incidentes de seguridad.
    - Fomentar la conciencia crítica de las amenazas, vulnerabilidades y consecuencias de la no aplicación de controles pertinentes para la gestión de la información.
- **Alcance del plan de sensibilización**. Determina a quienes está dirigido el plan de sensibilización. Se considera necesario incluir a todo el personal de la empresa, incluyendo usuarios del sistema, personal administrativo y no usuarios del sistema.
- **Temas a tratar**. Comprende la temática contenida en el plan de sensibilización para lograr que los usuarios del sistema fortalezcan las competencias relacionadas con la protección de los activos de información de la organización.
- **Metodología.** Establece las alternativas utilizadas para adelantar el plan de sensibilización. Estas pueden ser:
    - Capacitaciones.
    - Catálogos.
    - Carteles.
    - Mensajes en salvapantallas.
    - Material BTL.[43]
    - Uso de la tecnología**.**
- **Diseño del logotipo**. El plan de sensibilización debe incluir una imagen que lo identifique. Esta debe tener una relación con el tema, ser llamativa, instructiva e incluir un mensaje de texto claro, corto y preciso (Figura17).
- **Duración y costos**. Estimación del tiempo utilizado para adelantar el plan de sensibilización y consideración económica de la inversión. El proceso de sensibilización se inicia con la planificación de todas y cada una de las actividades que se llevaran a cabo, lo que incluye un cronograma de actividades y costos debidamente justificado y aprobado por la dirección de la organización.
- **Auditoria y evaluación**. Comprende la verificación de la ejecución del plan de sensibilización y la evaluación de los contenidos. Es importante que se establezca un mecanismo de control para evitar que las personas a las que está dirigido el proyecto no participen en las capacitaciones, talleres y herramientas de sensibilización ejecutadas. Esto se logra a través de planillas de asistencia y aplicación de sanciones disciplinarias a quienes incumplan sin justa causa con las tareas asignadas, considerando esta

[43]Below The Line (debajo de la línea). Se basa en el empleo de formas de comunicación no masivas dirigidas a un grupo específico **(**target) utilizando como herramienta primordial la creatividad, la sorpresa o el sentido de oportunidad.

situación como falta de compromiso con la seguridad de la información de la empresa.

La etapa final del proceso de sensibilización es la evaluación de las capacidades adquiridas por parte de los usuarios del sistema de UNITRANSA S.A. y la aplicabilidad que de ello se esté dando en la seguridad de los activos de información de la empresa. Ejecutar una encuesta donde se aprecie el grado de sensibilización de la seguridad de la información y los activos, realizar test de evaluación a una muestra poblacional de los asistentes a las diferentes actividades y realizar un análisis comparativo de incidentes de seguridad ocurridos antes y después de finalizado el proceso de sensibilización, constituyen el principal mecanismo de seguimiento a la efectividad del mismo.

Figura 17. Logotipos plan sensibilización

Fuente: Autor.

8.3.1 Herramientas de sensibilización. Para lograr la sensibilización de los empleados de UNTRANSA S.A. hacia la seguridad de la información y los activos, debe incluirse además de la capacitación propiamente dicha, herramientas que los ayuden a apoderarse de los conceptos propios del tema. Estos instrumentos pueden ser:

- **Afiches.** Estrategia muy utilizada porque permite llegar a un gran número de personas a quienes está dirigido el plan de sensibilización, con una mínima inversión económica y por el tiempo que estime conveniente el director del proyecto. Consiste en ubicar carteles en los lugares por donde circulan los empleados de la empresa, con mensajes alusivos a la seguridad de la información y la importancia de mantener la integridad de los activos de información.

  Otro aspecto importante de esta herramienta es que incluso personal que no es usuario del sistema, puede adquirir conocimientos básicos relacionados con la seguridad de la información y contribuir de alguna manera a preservar la integridad de la información. Lo ideal es que se cambien con determinada frecuencia los enunciados para lograr que las personas amplíen sus conocimientos y mantengan el interés por conocer las principales incertidumbres, peligros y elementos relacionados con la seguridad de la información.

  Algunos ejemplos de afiches propuestos para la campaña de sensibilización:

Figura 18. Afiche de cierre de sesión.

Fuente: Autor.

Este afiche recuerda a los usuarios del sistema que deben cerrar sesión de su PC cuando abandonen su puesto de trabajo. Evita que se realicen acciones peligrosas en el sistema.

Figura 19. Afiche bloqueo de terminal

Fuente: Autor.

Este cartel nos enseña que debes activar el protector de pantalla con contraseña de ingreso. Evita que alguien ingrese a su sistema sin su consentimiento.

.

Figura 20. Afiche contraseña de archivos

Fuente: Autor.

Este afiche recuerda que la información privado debe estar guardada con contraseña. No le hagamos facil el trabajo a los intrusos.

Figura 21. Afiche contraseñas seguras

Fuente: Autor.

Este cartel enseña que se debe utilizar contraseñas robustas y cambiarlas con frecuencia.

- **Catálogos.** Este instrumento de sensibilización consiste en la distribución de cuadernillos con información detallada de los aspectos más importantes sobre la seguridad de los activos e información de UNITRANSA S.A. Contiene recomendaciones sobre el buen uso de los activos de información, tips de seguridad, herramientas software y hardware utilizadas actualmente, incidentes más comunes y consecuencias de la materialización de las amenazas.

  Los catálogos de seguridad son una excelente herramienta para dar a conocer la Política de Seguridad de la Información (PSI) y lograr que los usuarios del sistema tomen conciencia de su importancia.

  Se recomienda que el primer catálogo sea distribuido al mismo tiempo que se coloquen los primeros carteles, esto con el fin de aumentar su impacto y conseguir una conectividad entre las dos actividades.

- **Mensajes en salvapantalla**. Los funcionarios de la empresa representan el principal objetivo de la campaña de sensibilización. El computador como mecanismo por excelencia para el desempeño de sus funciones diarias también puede ser utilizado como medio de sensibilización de la seguridad de la información a través de la incorporación de salvapantallas con mensajes alusivos a las amenazas informática, vulnerabilidades de los sistemas operativos, concejos prácticos, conceptos básicos y cualquier tipo de ayuda que contribuya a la concienciación de asumir estos temas con la mayor responsabilidad.

- **Medio BTL.** Consiste en la utilización de elementos de uso cotidiano de los empleados de UNITRANSA. S.A. con contenidos que despierten el interés por los temas relacionados con la seguridad de los Activos de Información y la información propiamente dicha. Estos objetos deben ser puestos al servicio de los usuarios de manera simultánea con la distribución de los cuadernillos para lograr un significativo impacto.

  Como ejemplos de este medio se podría citar la utilización de vasos con mensajes e imágenes llamativas sobre seguridad informática, crucigramas, sopas de letras y juegos de mesa, etc.

9. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE UNITRANSA S.A.

9.1 OBJETIVO

Brindar los criterios necesarios para el mantenimiento de la integridad, disponibilidad, confidencialidad y trazabilidad de los activos de información de UNITRANSA S.A.

9.2 ALCANCE.

Las políticas de seguridad están dirigidas a todos los usuarios del sistema, practicantes, contratistas, socios, proveedores, asesores, personal de oficios varios y visitantes de las instalaciones de UNITRANSA S.A.

9.3 POLÍTICAS GENERALES

- Las herramientas y recursos entregados a los funcionarios de UNITRANSA S.A. son utilizados exclusivamente para el desarrollo de actividades propias de la empresa.
- Los activos informáticos de UNITRANSA S.A. solo pueden ser utilizados para alcanzar los objetivos propios de la empresa.
- La información catalogada como crítica por parte de UNITRANSA S.A., debe contar con mecanismos pertinentes que faciliten su recuperación en caso de materializarse un incidente de seguridad.
- Restringirse al acceso al centro de cómputo, dada la importancia que representan los equipos para el almacenamiento y proceso de la información.
- Disponer de mecanismos de monitoreo y control que permitan registrar el acceso, las acciones y el tiempo de permanencia en el centro de cómputo de las personas que ingresen a dicho lugar.
- Solo personal autorizado mediante mecanismos de autenticación, podrá acceder a las estaciones de trabajo y los sistemas de información.
- Todos los equipos que pertenecen a UNITRANSA S.A. deben tener instalada la versión actualizada del antivirus de uso corporativo.
- La utilización inadecuada de los recursos y los activos de información de UNITRANSA S.A. son considerados como falta a la Política de Seguridad de la Información. Las siguientes acciones son calificadas inapropiadas para el mantenimiento de la seguridad de los activos de información:
  - ✓ Proporcionar información confidencial a personas o entidades diferentes a la empresa.
  - ✓ Utilizar la información de la empresa para conseguir lucro personal o de terceros.

- ✓ Alterar la información para ocultar algún incidente.
- ✓ Difundir información sin la autorización debida.
- ✓ Hurtar activos de información hardware y/o software.
- ✓ Realizar copias de documentos y software sin la autorización requerida.
- ✓ Extorsionar, amenazar e intimidar a cualquier funcionario con el objeto de obtener algún tipo de información.
- ✓ Utilizar indebidamente el usuario administrador.
- ✓ Instalar en los equipos de cómputo de UNITRANSA S.A. software sin autorización debida.
- ✓ Instalar en los equipos de la empresa, software malicioso (Adware, Spyware, keylogger, virus, gusanos, troyanos, bombas lógicas, etc.).
- ✓ Reubicar equipos de cómputo y otros elementos del departamento sin autorización.
- ✓ Vulnerar los mecanismos de seguridad para acceder a lugares restringidos o zonas Wifi.
- ✓ Interceptar la red LAN de la empresa para capturar las tramas de información que circulan.
- ✓ Enviar mensajes fraudulentos a través del correo electrónico a nombre de UNITRANSA S.A.
- ✓ Violar la propiedad intelectual de los compañeros de la empresa a través del robo o plagio de información.
- ✓ Publicar en internet información confidencial de UNITRANSA S.A.

9.4 POLÍTICAS ESPECÍFICAS.

Establecen los aspectos más importantes de seguridad de los activos de información de UNITRANSA S.A. ajustados a la labor que desempeñan todos y cada uno de los empleados de la empresa, en aras del buen uso que de ellos se haga.

Las políticas específicas reglamentan detalladamente la forma como se deben usar los activos de información, los recursos que facilitan el trabajo y comunicación dentro de la empresa.

Los aspectos más relevantes de las políticas específicas contemplan:

- Uso correcto del correo electrónico.
- Uso de estaciones de trabajo.
- Uso de cuentas de usuario y contraseñas.
- Disponibilidad de la Información.

9.4.1 Políticas Para el Uso Adecuado del Correo Electrónico.

9.4.1.1 Objetivo. Instaurar las normas que deben seguir los empleados, practicantes, contratistas, proveedores, directivos, socios a los cuales se les haya asignado una cuenta de correo electrónico empresarial para el desarrollo de sus actividades.

9.4.1.2 Alcance. Ésta política se hace extensiva a toda persona o entidad que tenga a su cargo una cuenta de correo electrónico empresarial de UNITRANSA S.A. y puede hacer uso de ella dentro y fuera de la empresa sin distingo de horario o día.

Políticas:

- Las solicitudes de cuentas de correo electrónico empresarial por parte de los empleados de UNITRANSA S.A. deben hacerse de forma escrita al ingeniero jefe del Departamento de Sistemas.
- Esta cuenta de correo electrónico no debe usarse para difundir todo tipo de información, su uso es estrictamente laboral.
- Las cuentas de correo electrónico de UNITRANSA S.A. son de carácter personal e intransferible y su estructura corresponde a las iniciales del primer nombre, su primer apellido (en caso de homónimos se debe utilizar la combinación de letras que identifiquen inequívocamente al solicitante) seguido del dominio de la empresa (@unitransa.com).
- Luego de establecida una cuenta de correo electrónico al solicitante, este deberá cambiar la contraseña asignada por el Departamento de Sistemas y repetir la misma acción cada tres meses o antes, según criterio del usuario de la cuenta.
- El propietario de la cuenta de correo electrónico empresarial de UNITRANSA S.A. es el único responsable de las operaciones que realice utilizando este medio, la empresa solo podrá tomar acciones disciplinarias por la falta cometida.
- Las cuentas de correo electrónico empresarial no deben usarse para enviar información sensible.
- Evitar el envío de mensajes que puedan causar un efecto de cadena entre usuarios del sistema.
- La cuenta de correo electrónico empresarial debe utilizarse como una herramienta de trabajo y no como fuente de distracción.
- El usuario y la contraseña de la cuenta de correo electrónico deben ser guardados por sus propietarios de forma confidencial.
- Prescindir del envío de material pornográfico o que hiera susceptibilidades de las personas utilizando el correo electrónico empresarial.
- Procurar no dejar la cuenta de correo electrónico abierta cuando se ausente de la estación de trabajo.

- El usuario de la cuenta de correo electrónico deberá crear una carpeta en su equipo de cómputo donde almacenará sus correos y de esta manera liberar espacio en el servidor.
- Los empleados de UNITRANSA S.A. deberán hacer una clasificación de los correos considerando los de mayor importancia y guardarlos en sitios de almacenamiento externo como Pendrives, CDs o VDs y posteriormente eliminarlos de la cuenta.
- Cuando los empleados envíen un correo electrónico desde su cuenta empresarial deberán incluir su nombre, su cargo y el número de extensión de su despacho.
- Procurar no utilizar la opción respuesta de envío de recepción exitosa y confirmación de lectura, a menos que sea estrictamente necesario, esto con el fin de descongestionar la red.

9.4.2 Políticas para el uso de estaciones de trabajo.

9.4.2.1 1Objetivo. Dictar las normas de procedimientos que deben cumplir los empleados, practicantes, contratistas, proveedores, etc. de UNITRANSA S.A. cuando utilizan las computadoras de la empresa para el ejercicio de sus labores cotidianas buscando mantener la confidencialidad, integridad, disponibilidad y trazabilidad de los activos de información.

9.4.2.2 alcance. Ésta política se hace extensiva a todos los empleados y personas ajenas a la empresa que hacen uso de los equipos de cómputo y demás recursos del sistema de UNITRANSA S.A.

Políticas:

- Las estaciones de trabajo de UNITRANSA S.A. estarán dotadas de un sistema de usuario y contraseña para permitir el acceso a los recursos del sistema solamente al propietario del equipo de cómputo.
- Se deberá bloquear la pantalla del equipo de cómputo cuando el usuario del sistema deba abandonar su sitio de trabajo.
- Todos los empleados deberán revisar el entorno de sus equipos al inicio de su jornada laboral para descubrir elementos extraños conectados a las estaciones de trabajo.
- Al término de su jornada laboral, los usuarios del sistema cerrarán su sección.
- Cada Departamento dispondrá de espacios seguros para el almacenamiento de información guardada en medio físico como papel.
- Utilizar elementos dotados de cerraduras con llave para guardar en ellos documentación importante para UNITRANSA S.A. que no se maneja de forma cotidiana, además de la información generada durante la jornada laboral.

- Crear un formato de registro para solicitudes de información guardada en los espacios seguros. Este formato debe incluir fecha de la solicitud, nombres y apellidos del empleado que solicita la información, tipo de información requerida, justificación del requerimiento, hora de inicio y fin del procedimiento.
- Asignar mecanismos de usuario y contraseña a las impresoras y scanner de documentos para evitar el uso irresponsable de estos activos.
- Los equipos de cómputo de UNITRANSA S.A. deberán mantener su escritorio libre de documentos o carpetas de usuario; estos serán guardados en las particiones asignadas por el Departamento de Sistemas, con el objetivo de no dejar la información demasiado visible a potenciales intrusos.
- No es permitido instalar software en los equipos de la empresa sin la debida autorización del jefe del Departamento de Sistemas.
- Es responsabilidad de cada empleado proteger la infraestructura que está siendo usada para sus labores.

9.4.3 Políticas para el uso de cuentas de usuario y contraseñas

9.4.3.1 Objetivo. Establecer las estrategias diseñadas por UNITRANSA S.A. para el manejo de cuentas de usuario y contraseñas de acceso a los recursos del sistema, utilizados por los empleados de la empresa.

9.4.3.2 Alcance. Esta política se hace extensiva a todos los empleados y personal ajeno a UNITRANSA S.A. que cuentan con un usuario y contraseña asignado por la empresa para el ingreso a las estaciones de trabajo y/o los recursos del sistema de información.

Políticas:

- La persona a la cual UNITRANSA S.A. le asigne un usuario y contraseña es responsable absoluto del uso que de ellos haga.
- La cuenta de usuario y contraseñas asignadas son de carácter personal e intransferible.
- Los empleados, contratistas, practicantes, etc. a los cuales se les asigne una cuenta de usuario y contraseña deben evitar escribirlas en lugares visibles y guardarlas en sitios accedidos exclusivamente por el titular de la cuenta.
- Utilizar contraseñas seguras, esto es que tengan una longitud mínima de ocho caracteres entre los que se cuenten letras mayúsculas y minúsculas, números y de ser posible caracteres especiales.
- Las contraseñas no deben contener nombres, apellidos, secuencias numéricas, fechas de cumpleaños o cualquier tipo de información asociada con el titular de la cuenta.

- Una buena práctica es asignar contraseñas diferentes para acceder a cada recurso del sistema, ejemplo correo electrónico, estación de trabajo, etc.
- UNITRANSA ha determina un periodo de tres meses para el cambio de contraseñas.
- Para el acceso a un determinado sistema de información, el Departamento de Sistemas le asignará al empleado una contraseña, la cual será entregada por el jefe de Sistemas de manera personal con el fin de evitar que queden registros en los correos con esta información.
- Diferenciar entre los privilegios de una cuenta de usuario normal y una cuenta de usuario administrador, de igual manera determinar que usuario utilizará la cuenta administrador.
- Acudir al jefe del Departamento de Sistemas cuando el usuario haya olvidado su contraseña para su restablecimiento.
- Dar a conocer a los empleados, practicantes y todo persona natural o jurídica que tenga cuentas de usuario asignadas por UNITRANSA S.A. los criterios de contraseñas seguras y aplicar un sistema que permita su validación en el momento de su creación.

Los criterios para la construcción de contraseñas seguras son:

- ✓ Debe tener una longitud mínima de 8 caracteres.
- ✓ Debe contener letras mayúsculas y minúsculas.
- ✓ Debe contener valores numéricos.
- ✓ Se sugiere que contenga caracteres especiales como &, %, #, etc.
- ✓ No emplear palabras completas.

Un ejemplo de contraseña segura sería utilizando una frase fácil de recordar como “mi hijo nació el 18 de marzo de 1994”. Con esta frase formar la contraseña “Mhne18m/94”.

9.4.4 Políticas para la disponibilidad de la Información.

9.4.4.1 Objetivo. Crear las pautas a seguir por los empleados de UNITRANSA S.A. para el fortalecimiento de la disponibilidad de la información como pilar fundamental de la seguridad informática que estipula que esta debe estar disponible a ser usada en el momento en que la requieran los usuarios debidamente autorizados.

9.4.4.2 Alcance. Esta política se hace extensiva al jefe del Departamento de Sistemas sobre quien recae el compromiso de diseñar, poner en marcha y velar por el buen funcionamiento de los mecanismos adoptados para garantizar la disponibilidad de la información, los directivos de UNITRANSA S.A. responsables

de asignar los recursos necesarios para la implementación y los usuarios del sistema encargados del buen uso de los activos de información de la empresa.

Políticas:

- La información debe estar disponible en el momento en que el usuario debidamente autorizado la requiera.
- Adoptar mecanismos que proporcionen una fuente de energía con tensión estable y continua como una UPS (Uninterruptible Power Supply) para que continúe alimentado las estaciones de trabajo y los servidores por un corto tiempo cuando se presenten cortes del fluido eléctrico.
- Adquirir una planta eléctrica que supla el suministro de energía mientras se reestablece el servicio.
- Implementar mecanismos de Backup de datos en línea como OneDrive que permiten respaldar la información en caso de incidentes de seguridad.
- Guardar copias de seguridad de la información en sitios diferentes a los de la empresa UNITRANSA S.A.

9.4.5 Política de control de acceso y protección de la información

9.4.5.1 Objetivo. Establecer las directrices de UNITRANSA S.A. para restringir los accesos no autorizados al centro de cómputo y de esta manera proteger la información ante posibles eventos de seguridad.

9.4.5.2 Alcance. Esta política está dirigida a los empleados, practicantes, proveedores, contratistas, y visitantes de UNITRANSA S.A.

Políticas:

- Cada empleado es responsable de la información almacenada localmente en su equipo de trabajo.
- El centro de cómputo debe permanecer cerrado y solo personal responsable del proceso debe acceder a él.
- Todo empleado debe portar el carné en lugar visible dentro de las instalaciones de UNITRANSA S.A.
- Todos los empleadores y proveedores que tengan acceso a la información del negocio y sus servicios, deben tener acuerdos formales de confidencialidad de la información.

9.4.6 Política de control de dispositivos móviles.

9.4.6.1 Objetivo. Proporcionará las condiciones de uso de los dispositivos móviles (Tablets, Smartphone y portátiles, entre otros) empresariales y de uso personal que utilicen los servicios de la empresa. De igual manera vigilar porque los empleados, practicantes, socios y proveedores de servicios utilicen de modo responsable los servicios y equipos proporcionados por la organización.

9.4.6.2 Alcance. Esta política está dirigida a los empleados, practicantes, proveedores, contratistas, y visitantes de UNITRANSA S.A.

Políticas:

- Es deber del Departamento de Sistemas indagar y aplicar las opciones de protección y seguridad de dispositivos móviles tanto empresariales como personales utilizados en el desarrollo de los procesos de la empresa.
- El Departamento de Sistemas debe establecer las configuraciones de seguridad necesarias para los dispositivos móviles empresariales y personales que utilicen los servicios de UNITRANSA S.A.
- Adoptar por parte del Departamento de Sistemas un método de bloqueo (contraseñas, sistema biométrico, reconocimiento de voz, etc.) a los dispositivos móviles empresariales que fueren asignados a los empleados, socios o practicantes. Este procedimiento se activará luego de cierto tiempo de inactividad y para su reactivación requerirá el sistema de desbloqueo adoptado.
- El Departamento de Sistemas debe adoptar un mecanismo de cifrado de datos almacenados en dispositivos móviles empresariales con el fin de evitar la copia o extracción de información sin el conocimiento del sistema de descifrado.
- Es deber del Departamento de Sistemas implementar un mecanismo de copias de seguridad de la información contenida en los dispositivos móviles de propiedad de UNITRANSA S.A.
- Instalar por parte del Departamento de Sistemas software antivirus en los dispositivos móviles empresariales y personales que utilicen los recursos de la empresa.
- El Departamento de Sistemas debe activar los códigos de seguridad de las tarjetas SIM de los dispositivos móviles con anterioridad a su asignación y guardar estos códigos en un lugar seguro.
- Es deber de los usuarios de dispositivos móviles de propiedad de la empresa evitar la modificación de configuración de seguridad, la desinstalación de software provisto por la empresa y la descarga e instalación de programas desde fuentes desconocidas.

- Es deber de los usuarios de dispositivos móviles de propiedad de la empresa, evitar la conexión vía USB a computadoras públicas, hoteles, centros comerciales, etc.
- Está prohibido las conexiones WIFI a través de la Wireless Password del punto de acceso de la empresa UNITRANSA S.A. para dispositivos de carácter personal. Los equipos móviles de carácter empresarial o personal que requieran una conexión inalámbrica deberán solicitarla por escrito al Departamento de Sistemas y esta se hará solo por medio de su MAC address.

9.5 FALTAS Y SANCIONES.

La empresa UNITRANSA S.A. en el reglamento interno de trabajo contempla sanciones para aquellas conductas que conllevan el incumplimiento del contrato de trabajo, entre las cuales se encuentran las políticas de seguridad de la información.

El departamento de recurso humano de la empresa UNITRANSA S.A. tipifica las faltas al incumplimiento de las políticas de seguridad de la información, de responsabilidad del gerente de la compañía, con carácter disciplinario y se clasifican en:

- **Leves:** se trata de conductas de los empleados que por su carácter implican falta de disciplina sin poner en riesgo la información de la empresa, por lo que se sanciona esta clase de conductas con un llamado de atención formal, por escrito.
- **Graves:** se trata de conductas de los empleados que por su carácter ponen en riesgo la información de la empresa, por lo que se sanciona de acuerdo con la gravedad, con suspensión en el ejercicio del cargo.
- **Gravísimas:** se trata de conductas de los empleados que por su carácter implican poner en riesgo no solo la información sino la estabilidad de la empresa (Ley 1273 del 2009 "**de la protección de la información y de los datos**"), por lo que se sanciona con la terminación del contrato de trabajo. Así mismo deberá compulsar copias a la entidad competente como la fiscalía general de la nación para la respectiva investigación penal de la conducta para que se establezca si se trata de un delito y la respectiva indemnización a que hubiere lugar.

Las sanciones disciplinarias deberán imponerse dentro de un proceso disciplinario en el cual se garantice los principios de celeridad y debido proceso y no podrá exceder de seis meses siguientes a la fecha en que se tuvo conocimiento de la conducta.

10. CONCLUSIONES

Con base en las visitas realizadas a la empresa UNITRANSA S.A. se obtuvo datos importantes de los Activos de Información, de los funcionarios, los procesos y el entorno laboral. Realizado el análisis de riesgos y vulnerabilidades existentes, se pudo establecer que existen serias falencias en la gestión de activos que ponen al descubierto situaciones que de ser aprovechadas por intrusos podrían afectar seriamente la confidencialidad, la integridad y la disponibilidad de uno de sus activos más importantes, como lo es su información.

Las conclusiones a las que se pudo llegar con la realización del presente trabajo son las siguientes:

- La realización del Análisis de Riesgos de los activos de información pudo establecer que existen dos Activos de Información (Sistema Operativo Windows XP y Red Local de UNITRANSA S.A.) en alto grado de nivel riesgo de probabilidad de ocurrencia de algún tipo de incidentes. El proyecto de Diseñar un Sistema de Gestión de la Seguridad de la Información se constituye en una herramienta muy valiosa para la empresa UNITRANSA S.A. ya que contiene las pautas necesarias para ejecutar la gestión de activos de información que permite un conteo rápido de los activos de la empresa, facilidad a la hora de ejecutar las acciones de mantenimiento de los equipos y disminución del riesgo de incidentes de seguridad sobre los activos, gracias a su clasificación de importancia para los procesos de la organización, entre otros aspectos.
- La Política de Seguridad de la Información (PSI) es la herramienta básica con la que debe contar toda organización para alcanzar los niveles óptimos de seguridad, partiendo de la premisa de que, en la larga cadena de factores de seguridad, el eslabón más débil lo representan las personas. Esta debe involucrar a todos los que laboran en la empresa y los que realizan servicios contratados a terceros. En este sentido, es importante la implementación, verificación y monitoreo de acuerdos, a fin de lograr que se cumplan los requerimientos de seguridad pactados. Sin embargo, es importante señalar que la creación y aplicación de la Política de Seguridad de la Información y la implementación del sistema de Gestión de Activos que estipula el Dominio A.8 de la Norma ISO/IEC 27001, no garantiza el 100% de la seguridad de la información de la empresa, pero si determina una reducción significativa de las eventualidades de seguridad sobre los activos y la información.

- El sistema de gestión de inventario de activos de información no es lo suficientemente eficiente para ejercer un control sobre los equipos en aspectos como pertenencia a un departamento, propietario, nivel de criticidad, procesos que maneja, controles, entre otros. Esta situación se percibe en la falta de etiquetas de marcado que suministren información básica del equipo.
- La incorporación de un plan de sensibilización es primordial para alcanzar los objetivos trazados en el diseño del proyecto de seguridad de la información. Debe incluir no solamente el desarrollo de cursos de capacitación en el tema, sino también ejecutar acciones paralelas como carteles alusivos a la seguridad, suvenires, salvapantallas, etc. para lograr que los usuarios del sistema incluyan la seguridad de la información en todas y cada una de las actividades que realicen.

11. RECOMENDACIONES

Finalmente se presentó a la gerencia de UNITRANSA S.A. algunas recomendaciones que permitirán alcanzar un alto grado de seguridad de la información y con ello hacer de la empresa una organización más confiable, más rentable y sostenible.

- Adelantar un programa de sensibilización en política de seguridad de la información que permita generar la cultura del uso responsable de los recursos informáticos que involucre a todos los empleados de la empresa, socios, proveedores y contratistas.
- Sustituir los equipos de cómputo obsoletos conectados a la red de la empresa, con sistemas operativos que no cuentan con el respaldo necesario para actualizaciones que contrarresten las vulnerabilidades que ponen en peligro la seguridad de la información, por equipos de última generación con prestaciones que satisfagan las necesidades de la empresa, sin caer en el error de gastos excesivos en dispositivos subutilizados.
- Instalar en los equipos de la empresa UNITRANSA S.A. Windows 10 por las siguientes razones:
    - Windows 10 presenta un incremento tanto en la velocidad de arranque del equipo como en la velocidad de carga inicial de sus aplicaciones, de igual forma a la hora de ejecutar programas.
    - Los requerimientos mínimos son similares a los de Windows 8.1, 8 e incluso Windows 7, por lo que migrar al nuevo sistema operativo no resulta ser traumático. La Tabla 26 muestra los requisitos mínimos de Windows 10.

Tabla 25. Requerimientos Windows 10

Procesador	3GHz con soporte para PAE, NX y SSE2
Memoria RAM	4GB para 32 bits y 8GB para 64 bits.
Espacio en disco	16GB para 32 bits o 20 GB para 64 bits.
Tarjeta Gráfica	Compatible con DirectX9 y WDDM.

Fuente: http://www.meristation.com/pc/reportaje/diez-razones-para-cambiarse-a-windows-10/2076190/58

    - La interfaz, que en anteriores versiones generó mucha crítica, esta vez presenta un escritorio clásico pero elegante, permitiendo un acceso rápido a los programas más utilizados, a los menús de configuración y al botón de encendido y apagado del sistema, entre otras particularidades.
    - El nuevo navegador web Microsoft Edge, que reemplaza a Internet Explorer, posee velocidades comparables a las de los clásicos Mozilla y Chrome. Aunque debe mejorar en algunos aspectos, tiene

herramientas para pintar, comentar y capturar partes de una página web fácilmente, incluye además la posibilidad de eliminar la publicidad y otros complementos para leer su contenido sin distracción.
    - Windows 10 incluye el centro de actividades, por medio del cual es posible gestionar muchos procesos del computador, muestra notificaciones como presencia de virus, actualizaciones de Windows, etc.
    - Tecnología de seguridad Hello, SmartScreen, controles parentales nuevos, entre otros, son algunas de las características de Windows 10 que lo hacen muy robusto de cara al malvare y los espías.

- Adquirir un software de gestión de mantenimiento de equipos que disponga de un cronograma de acciones preventivas, incluyendo lector de código de barras que permita al departamento técnico obtener fácilmente la información más relevante del equipo y los procesos que maneja. Esta información está dispuesta en la etiqueta de marcado de activos de información adherida a los equipos.
- Obtener herramientas software para el mantenimiento preventivo y correctivo de los equipos de cómputo de la empresa. Algunas aplicaciones recomendadas son:
    - **Eudora:** herramienta gratuita de limpieza y optimización del disco duro.
    - **Norton Utilities**. Entre sus beneficios está mantener la privacidad digital, recupera archivos borrados o corruptos, acelerar el equipo, reparar errores más comunes y mejorar el rendimiento de la máquina.
    - **Advanced SystemCare**. Poderosa herramienta que además de limpiar de archivos basura para liberar espacio en disco, desfragmenta el registro y elimina las aplicaciones inútiles, haciendo su equipo más limpio y rápido. Ayuda a mantener la privacidad y confidencialidad mediante detección y eliminación de spyware, adware y otros malware.
- Instalar un firewall o cortafuegos que permita a la empresa UNITRANSA S.A. gestionar y filtrar la totalidad de trafico entrante y saliente entre la red local e Internet. Preferiblemente un dispositivo de tipo hardware firewall o router que dispongan de esta función.
- Colocar un sistema de cámaras de seguridad en los puntos estratégicos de la empresa para controlar el acceso de personal no autorizado principalmente en horas no laborales.
- Contratar un servicio de Cloud Computing para guardar la información más relevante de la empresa y de esta manera obtener la continuidad del negocio en la eventualidad de que ocurra algún desastre. Algunas de las alternativas para el almacenamiento de archivos en la nube son:

- **Dropbox.** Permite el alojamiento de archivos multiplataforma en la nube y admite el intercambio de archivos y/o carpetas con otros usuarios. Tiene una versión gratuita y otra de pago.
- **Google Drive**. Otorga 15 GB de espacio gratuito para guardar archivos y puede ser ampliado según condiciones de pago. Facilita la edición de documento y hojas de cálculo.
- **iCloud.** Plataforma de Apple que ofrece servicio de Cloud Computing a usuarios de Mac e iOS. Permite realizar copias de seguridad de los equipos.
- **Onedrive**. Este servicio de almacenamiento en la nube que ofrece Microsoft, además de permitir guardar y compartir cualquier tipo de archivos, es compatible con Microsoft Windows, Mac, iOs, Android y Windows Phone.
- **Dataprius**. Servicio que imita un escritorio de Windows. Se diferencia de los anteriores en que no actúa como disco virtual de archivos, funciona como servidor virtual.[44]

[44] WIKIPEDIA. Almacenamiento en nube [11, abril, 2017] [online]. Disponible en Internet: https://es.wikipedia.org/wiki/Almacenamiento_en_nube

BIBLIOGRAFÍA

Acosta, J. M. "*Políticas de Seguridad*" [online]. [Julio de 2012]. Disponible en Internet: http://es.slideshare.net/jmacostarendon/politicas-deseguridad

Alcaldía Municipal de Ibagué." Política de seguridad de la información" [online] (sf). Disponible en Internet: http://www.alcaldiadeibague.gov.co/portal/admin/archivos/publicaciones/2015/11918-DOC-20151001.pdf

Buitrago Estrada, J. B. "*Diseño de una metodología para la implementación del sistema de gestión de seguridad de la información - SGSI, en el sector de laboratorios de análisis microbiológicos, basado en ISO 27001*" [online]. [2012]. Disponible en Internet: http://repository.ean.edu.co/bitstream/handle/10882/2692/MurilloCarol2012.pdf;jsessioni%09d=F222F0CE793E0428069FA54CE3BDECE4?sequence=1%5d

Cisco "*Cisco ASA 5500 Series Firewall Solution Overview*", (sf). [online] [2016]. Disponible en Internet: http://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/prod_brochure0900aecd8048dba8.html

COLOMBIA.CONGRESO DE LA REPUBLICA. Ley 527(5, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos". Diario Oficial. Bogotá. D.C.,2009, no.47223.

COLOMBIA.CONGRESO DE LA REPUBLICA. Ley 1341(29, julio, 2009). Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones. Diario Oficial. Bogotá. D.C., 2009, no.4742.

COLOMBIA.CONGRESO DE LA REPUBLICA. Ley 1266(31, diciembre, 2008). Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales. Diario Oficial. Bogotá. D.C., 2009, no.47219

COLOMBIA.CONGRESO DE LA REPUBLICA. Ley 527(18, agosto, 1999). por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales. Diario Oficial. Bogotá. D.C.,18, agosto, 1999, no.43673.

Coraje, P. "*La tecnología como factor clave del crecimiento económico"* [online] [2013]. Disponible en Internet: http://www.pablocoraje.es/2013/02/la-tecnologia-como-factor-clave-del.html

Enríquez Espinosa, R. "*Implementación de los controles asignados al dominio gestión de activos, bajo los lineamientos establecidos por la norma ISO/27001 anexo A, para las empresas municipales de Cali, EMCALI E.I.C.E.-ESP".* [online] [2013]. Disponible en Internet: http://bdigital.uao.edu.co/handle/10614/53274

Erb, M. (s.f.). "*Gestión de Riesgo en la Seguridad Informática*" [online] [2016] Disponible en Internet: https://protejete.wordpress.com/about/

González, S. "*Diez razones para cambiarse a Windows 10*". [online] [2015] Disponible en Internet: http://www.meristation.com/pc/reportaje/diez-razones-para-cambiarse-a-windows-10/2076190/58

Instituto Colombiano de Normas Técnicas y Certificación INCONTEC. "*NTC 1486*" [online] [2008] Disponible en Internet: http://datateca.unad.edu.co/contenidos/356025/NTC1486.pdf

Instituto Colombiano de Normas Técnicas y Certificación INCONTEC "*NTC 4490*" [online] [2008] Disponible en Internet: http://www.politecnicojic.edu.co/images/downloads/biblioteca/guias/NTC4490.pdf

Instituto Colombiano de Normas Técnicas y Certificación INCONTEC "*NTC*-ISO/IEC 27001" [online] [2006] Disponible en Internet: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

Instituto Nacional de Ciberseguridad Incibe. "*Kid de concienciación*" [online] (sf). Disponible en Internet: https://www.incibe.es/protege-tu-empresa/kit-concienciacion

ISACA. "*La integridad de los datos: el aspecto más relegado de la seguridad de la información*" [online] [2016]. Disponible en Internet: http://www.isaca.org/Journal/archives/2011/Volume-6/Pages/Data-Integrity-Information-Securitys-Poor-Relation-spanish.aspx?

ISO, "*ISO/IEC 27001:2013*" [online] [2013] Disponible en Internet: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54534

Kosutic, D. "¿Qué es norma ISO 27001?" [online] [2015] Disponible en Internet: http://www.iso27001standard.com/es/que-es-iso-27001/

Microsoft, "*Windows Server 2012 R2*" [online] [2014] Disponible en Internet: http://www.microsoft.com/es-es/server-cloud/products/windows-server-2012-r2/

Ministerio de Hacienda y Administraciones Públicas de España. "*MAGERIT v.3*" [online] [2012]. Disponible en Internet: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Mageri t.html#.Vu4AgI-cE2w

MINTIC, "*En TIC Confió*" [online] [2015]. Disponible en Internet: http://www.enticconfio.gov.co/index.php/enticconfio/item/234-ley-1341-de-2009.htm

PCEL. "Switch 3Com Office Connect de 16 Puertos 10/100Mbps" [online] [2016] Disponible en Internet: http://pcel.com/3Com-JD858AABA-73227

Revista ALIDE, "*¿Cómo gestionar activos de información?*" [online] [2015] Disponible en Internet: http://www.alide.org.pe/download/Financ_Sectorial/fn13_fin_rev1_activos.pdf

Secretaría general de la alcaldía mayor de Bogotá, "*Inventario de activos de Información*" [online]. [2015]. Disponible en Internet: http://secretariageneralalcaldiamayor.gov.co/sites/default/files/lineamiento_11_inventario_de_activos_de_informacion.pdf

Tabares Rendón J. D., "*Implementación de un sistema de gestión de seguridad informática en la confederación de cámaras de comercio -CONFECÁMARAS*" {En Línea} {2015} Disponible en: http://hdl.handle.net/10596/3653

UNAD, "*SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACIÓN SGSI*. Pilares de la seguridad Informática" [online] [2016] Disponible en Internet:

http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/11_leccin_1_pilares_de_la_seguridad_informtica.html

Wikipedia, "*Análisis de riesgo informático*" [online] [2016] Disponible en Internet: https://es.wikipedia.org/wiki/An%C3%A1lisis_de_riesgo_inform%C3%A1tico

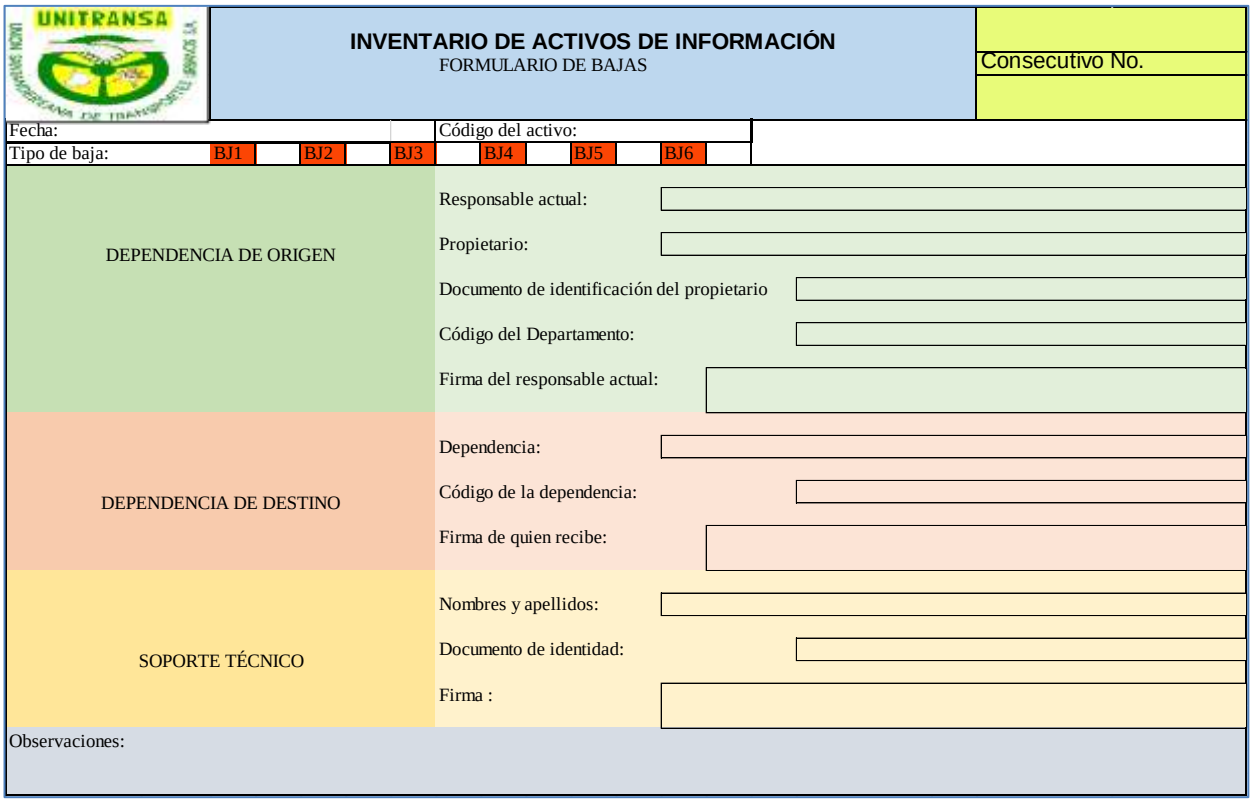
ANEXOS

Anexo A. Formulario de Incorporaciones

UNITRANSA	**INVENTARIO DE ACTIVOS DE INFORMACIÓN** FORMULARIO DE INCORPORACIONES		Consecutivo No.
Fecha de incorporación:	Departamento:	Modo de incorporación:	I1 I2 I3 I4 I5 I6
Responsable:		Documento de identificación:	
Propietario:		Documento de identificación:	
Descripción del activo:		Código asignado:	
Fabricante:	Marca:	Modelo:	No de Serie:
Suministrador:	Fecha de adquisición:	Fecha fin de la garantía:	
Observaciones:			
Firma de aprobación:			

Fuente: Autor.

Anexo B. Formulario de bajas



UNITRANSA	INVENTARIO DE ACTIVOS DE INFORMACIÓN FORMULARIO DE BAJAS	Consecutivo No.

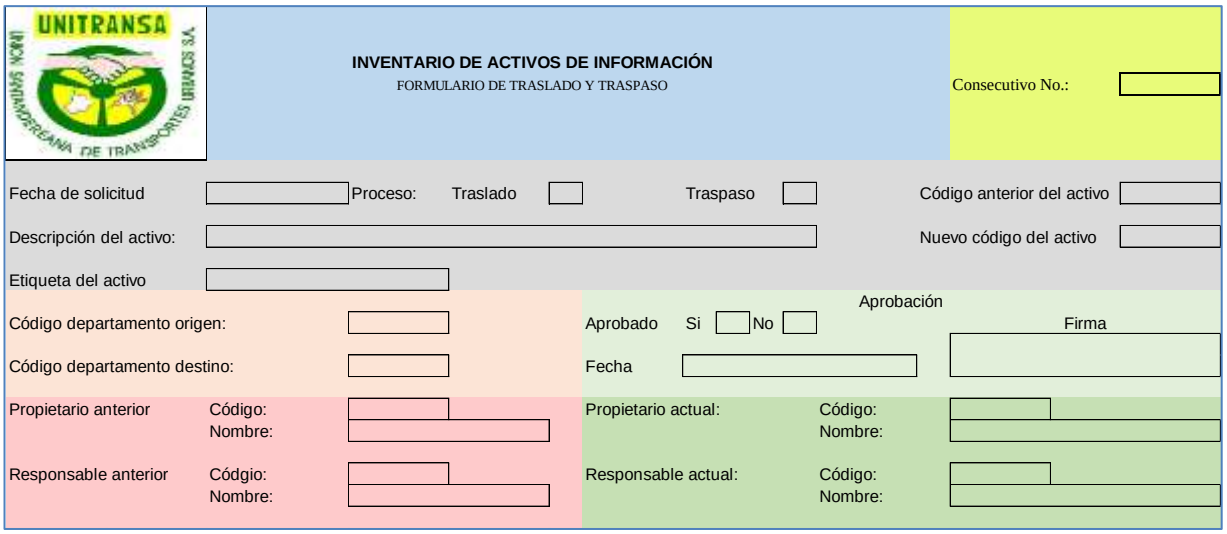
Fecha:						Código del activo:					
Tipo de baja:	BJ1		BJ2		BJ3		BJ4		BJ5		BJ6

DEPENDENCIA DE ORIGEN	Responsable actual:	
	Propietario:	
	Documento de identificación del propietario	
	Código del Departamento:	
	Firma del responsable actual:	
DEPENDENCIA DE DESTINO	Dependencia:	
	Código de la dependencia:	
	Firma de quien recibe:	
SOPORTE TÉCNICO	Nombres y apellidos:	
	Documento de identidad:	
	Firma :	

Observaciones:

Fuente: Autor.

Anexo C. Formulario de traslado y traspaso



UNITRANSA	**INVENTARIO DE ACTIVOS DE INFORMACIÓN** FORMULARIO DE TRASLADO Y TRASPASO					Consecutivo No.:	
Fecha de solicitud		Proceso:	Traslado		Traspaso	Código anterior del activo	
Descripción del activo:						Nuevo código del activo	
Etiqueta del activo							
				Aprobación			
Código departamento origen:				Aprobado	Si / No	Firma	
Código departamento destino:				Fecha			
Propietario anterior	Código: Nombre:			Propietario actual:	Código: Nombre:		
Responsable anterior	Códgio: Nombre:			Responsable actual:	Código: Nombre:		

Fuente: Autor.

Anexo D. Checklist sobre componentes de seguridad

Tabla 26. Checklist

PREGUNTA	SI	NO
¿La empresa posee una Política de Seguridad de la Información?		
¿Existe una persona encargada de gestionar y vigilar por la seguridad de la información?		
¿Hay algún guarda de seguridad física en la empresa las 24 horas?		
¿Las oficinas tienen algún mecanismo de seguridad para su ingreso?		
¿Poseen extintores de incendios en cada una de las plantas del edificio?		
¿El personal de las oficinas tiene conocimiento del funcionamiento de los extintores?		
¿Se revisan periódicamente los extintores para verificar su fecha de caducidad?		
¿Si los hay, poseen algún mecanismo que los active de forma automática?		
¿Hay un plan de evacuación en caso de una emergencia?		
¿Se realizan simulacros de evacuación?		
¿Existen sensores de humo en las instalaciones de la empresa?		
¿Las salidas de emergencia están debidamente señaladas?		
¿Se ha asignado a una persona por planta como líder en caso de una evacuación?		
¿Existe un cronograma de mantenimiento preventivo de equipos?		
¿Hay alguna persona de la empresa que realiza el mantenimiento de los equipos?		
¿Existe un sistema de backup de la información en la empresa?		
¿Las copias de los archivos y programas se guardan fuera de la empresa?		
¿La empresa cuenta con algún programa de backup en línea?		
¿Maneja el concepto de contraseñas seguras?		
¿Se cambian con frecuencia las contraseñas?		
¿Los equipos de cómputo poseen sistema de bloqueo automático cuando se abandona el puesto de trabajo?		
¿Posee la empresa un programa de antivirus actualizado?		
¿Se realizan auditorias de sistemas de información?		
¿Posee cuenta de correo empresarial?		

Tabla 26. (Continuación)

PREGUNTA	SI	NO
¿Existe un reglamento para el manejo de la cuenta empresarial?		
¿Los equipos de cómputo están alejados de los ventanales?		
¿Existe un mecanismo de Sistema de Alimentación Ininterrumpida (UPS) conectado a su equipo?		
¿El acceso al servidor está restringido?		
¿Se revisan maletines, bolsos y otros elementos por parte del guarda al salir del edificio?		
¿se solicita autorización para retirar algún elemento de computo de las instalaciones?		

Fuente: Autor.

Anexo E. Encuesta de satisfacción de servicio

ENCUESTA DE SATISFACCIÓN DE SERVICIOS INFORMÁTICOS

Tabla 27. Encuesta de satisfacción

Marque con una X		
Pregunta	Si	No
1. ¿El lugar donde está ubicado el centro de cómputo está seguro de inundaciones, robo o cualquier otra situación que pueda poner en riesgo los equipos?		
2. ¿El centro de cómputo da hacia el exterior?		
3. ¿Dentro del centro de cómputo existen materiales que pueden ser inflamables o que causen algún daño a los equipos?		
4. ¿Existe lugar suficiente para los equipos?		
5. ¿Se cuenta con una salida de emergencia?		
6. ¿Hay señalamientos que las hagan visibles?		
7. ¿Es adecuada la iluminación de su oficina?		
8. ¿Su oficina cuenta con servicio de aire acondicionado?		
9. ¿El aire acondicionado emite algún tipo de ruido?		
10. ¿Los equipos de cómputo cuentan con un regulador?		
11. ¿Su equipo cuenta con sistema de alimentación ininterrumpida?		
12. ¿Los cables están dentro de paneles y canales eléctricos?		
13. ¿Se cuenta con alarma contra incendios?		
14. ¿Existen extintores?		
15. ¿Cuentan con algún tipo de control de entrada o salida física a la oficina?		
16. ¿El usuario respeta ese control?		
17. ¿Cuentan con manuales para los programas que se manejan?		
18. ¿Existe un reglamento de buen uso de equipos informáticos?		
19. ¿Si existe, se encuentra a la vista del usuario?		

Tabla 27. (Continuación).

Marque con una X		
Pregunta	Si	No
20. ¿Se realiza mantenimiento preventivo a los equipos?		
21. ¿Se realiza mantenimiento correctivo a los equipos?		
22. ¿Los usuarios tienen suficiente confianza como para presentar quejas sobre fallas en los equipos?		
23. ¿Se tienen copias de los archivos en lugar diferente al de la computadora?		
24. ¿Se tiene definido procedimiento alguno para actualización de estas copias?		
25. ¿Se ha definido qué información puede ser accedida y por quién?		
26. ¿Se han instalado equipos que protejan los dispositivos y la información en caso de cambios bruscos de voltaje tales como reguladores de voltajes, supresores de picos, ups o generadores de energía?		
27. ¿Su equipo cuenta con antivirus actualizado?		
28. ¿Se hacen revisiones periódicas y sorpresivas del contenido del disco duro para verificar la instalación de aplicaciones no relacionadas con la gestión de UNITRANSA S.A.?		
29. ¿El encargado del área de sistemas te brinda atención cuando la requieres?		
30. ¿Su equipo está protegido con contraseña?		
31. ¿Maneja el concepto de contraseña segura?		

Fuente: Autor

Tabla 28. Pregunta abierta.

Pregunta abierta	
Pregunta	Respuesta
1. ¿Está su empresa protegida a nivel informático?	
2. ¿Qué es la política de seguridad de la información?	
3. ¿Qué es un IDS?	
4. ¿Qué es un firewall?	
5. ¿Qué es un análisis de riesgos?	
6. ¿Qué es un hacker?	
7. ¿Qué significa el termino spam?	

Tabla 28. (Continuación).

Pregunta abierta	
Pregunta	Respuesta
1. ¿Qué significa SGSI?	
2. ¿Qué entiende por criptografía?	
3. ¿Qué es una IDS?	
4. ¿Qué es un exploit?	
5. ¿Conoce las leyes colombianas sobre la protección de los datos?	

Fuente: Autor.

Anexo F. Ejemplo resumido de un catálogo de seguridad de la información

¿Qué es la Política de Seguridad de la Información?

Definir la Política de Seguridad de la Información no es describir técnicamente los elementos de seguridad de una organización, tampoco es un enunciado legal que incluya sanciones a conductas de los empleados. Podríamos decir más bien, que es una descripción detallada de lo que se quiere proteger, las razones por las que se hace y los mecanismos utilizados para ello. Todo PSI es un instrumento de guía y vigilancia a los usuarios del sistema para el uso adecuado de los recursos y servicios informáticos de la empresa. Es un conjunto de normas especificadas por el encargado de la seguridad de un sistema informático, básicamente lo que está permitido y lo que no lo está. [45]

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE UNITRANSA S.A.

Algunos de los mecanismos de seguridad de la información que deben conocer los usuarios del sistema de la empresa son:

INVENTARIOS DE ACTIVOS DE INFORMACIÓN

- ✓ Todos los activos de la empresa UNITRANSA S.A. se encuentran identificados y verificados para constatar el uso apropiado, para la recuperación ante desastres.
- ✓ La empresa UNITRANSA S.A. cuenta con una base de datos del inventario de activos de información, como hardware, software, servicios de tecnología, discriminados por dependencias.

SERVICIO DE DATOS "INTERNET"

El servicio de Datos e Internet de la empresa UNITRANSA S.A. es un mecanismo de apoyo a los usuarios en el desarrollo de los procesos de la organización. Este servicio debe

[45] Acosta Rendón, J. Manuel. Políticas de Seguridad Informática [marzo, 2010], Disponible en Internet: http://es.slideshare.net/jmacostarendon/politicas-deseguridad

cumplir una serie de normas para su utilización, como se mencionan a continuación.

- ✓ El servicio de Datos e Internet está estrictamente designado para propósitos laborales.
- ✓ Los usuarios tienen prohibido usar el canal de datos para navegar por páginas Web no autorizadas, enviar/descargar contenidos obscenos o violenten.
- ✓ Los usuarios no tienen permitido enviar/descargar software de procedencia desconocida, esto con el fin de evitar propagación de virus.
- ✓ UNITRANSA S.A. se reserva el derecho de monitorear el acceso al servicio de datos e Internet de los usuarios.

SERVICIO CORREO ELECTRÓNICO

Para el uso del servicio de correo electrónico se establece las siguientes Normas

- ✓ El servicio de correo electrónico de la empresa UNITRANSA S.A. es de carácter empresarial y no se debe usar para uso personal o comercial.
- ✓ Los usuarios tienen prohibido el uso del correo empresarial para enviar correos masivos, como cadenas.
- ✓ Los mensajes SPAM deben ser reportados al Ingeniero de Sistemas de la empresa y proceder a eliminarlo inmediatamente, porque pueden contener virus cifrados en extensiones .exe, .bat,. prg, .bak, o .pif. El mecanismo más utilizado es el envío de mensajes con contenidos eróticos o personajes famosos.
- ✓ Las cuentas de correo empresarial de UNITRANSA S.A. son supervisadas para garantizar que se le esté dando el manejo correspondiente a lo estipulado en la política. El mal uso de este servicio puede llevarlo a una investigación disciplinaria o penal.

RECURSOS TECNOLÓGICOS

La empresa UNITRANSA S.A. les proporciona a sus colaboradores los recursos tecnológicos como elementos de soporte para que realicen sus labores sujetándolos a las siguientes normas:

- ✓ Los empleados de UNITRANSA S.A. son los responsables del buen uso de los recursos tecnológicos asignados. Estos no pueden ser utilizados para fines personales o por terceros no autorizados.
- ✓ En los equipos asignados a los usuarios, está prohibido almacenar archivos de video, música y fotos que no sean de propiedad de la empresa UNITRANSA S.A.
- ✓ Está prohibido ingerir alimentos, bebidas o fumar en las estaciones de trabajo donde se encuentran los recursos tecnológicos.

- ✓ No está autorizado realizar derivaciones eléctricas por los funcionarios.
- ✓ La empresa UNITRANSA S.A. cuenta con un empleado autorizado para realizar modificaciones, actualizaciones, retirar, revisar y reparar los recursos tecnológicos
- ✓ Todos los computadores de la empresa poseen programas antivirus licenciados. Como regla general se debe verificar las unidades de almacenamiento externo como CDs, DVDs, Memorias USB o Discos Duros antes de realizar cualquier operación.
- ✓ Los equipos de cómputo que no pertenezcan a la empresa UNITRANSA S.A. deberá tener autorización del ingeniero sistemas para acceder a la red local.

TALENTO HUMANO

- ✓ Los usuarios del sistema de información de la empresa UNITRANSA S.A. son responsable de los registros y/o modificaciones de la información que se haga con su cuenta de usuario, así como (alteración, destrucción y/o uso inadecuado de la información),
- ✓ Las cuentas de usuario (Usuario y Contraseña) de acceso a la red de la empresa UNITRANSA S.A. son de carácter estrictamente personal e intransferible.
- ✓ Cuando un empleado de la empresa UNITRANSA S.A. deja de laborar, el jefe inmediato del departamento donde ejecutaba sus funciones será el encargado de custodiar la información.

Fuente: Autor.

RESUMEN ANALITICO ESPECIALIZADO RAE

TITULO:	DISEÑAR UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) A LA EMPRESA UNITRANSA S.A. UBICADA EN LA CIUDAD DE BUCARAMANGA.
FUENTES BIBLIOGRÁFICAS:	23 fuentes bibliográficas**.**
AUTOR:	Castro Angarita, Jaime Alfonso y García Ramírez, Germán.
FECHA:	19 de abril de 2017
PALABRAS CLAVE:	SGSI, ISO/IEC 27001, confidencialidad, integridad, malware, disponibilidad, vulnerabilidad, amenaza, ingeniería social, activo de información.
CONTENIDOS:	INTRODUCCIÓN, I PLANTEAMIENTO DEL PROBLEMA, II JUSTIFICACIÓN, III OBJETIVOS DEL PROECTO, IV MARCO REFERENCIAL, V MARCO METODOLÓGICO, VI DESARROLLO DEL PROYECTO, VII ESTIMACIÓN DEL ESTADO DE RIESGO DEL SISTEMA, VIII METODOLOGÍA DE INVENTARIO DE ACTIVOS DE INFORMACIÓNPROPUESTA PARA UNITRANSA S.A., IV POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE UNITRANSA S.A, X CONCLUSIONES, XI RECOMENDACIONES.
DESCRIPCIÓN DE INVESTIGACIÓN:	El documento contiene 11capítulos que inicia con el planteamiento del problema hasta llegar a las conclusiones y recomendaciones del diseño de un SGSI para mejorar la seguridad de la información y los activos de información de la empresa UNITRANSA S.A.

RESUMEN:

El trabajo inicia con la Introducción, que plantea la importancia de incorporar en las organizaciones mecanismos tecnológicos que agilicen sus procesos y permitan almacenar cantidades considerables de información en dispositivos muy pequeños, así como la incorporación de redes de datos que logran un ahorro importante de recursos con una mayor organización y eficiencia a la hora de tomar las decisiones.

Se aborda la metodología MAGERIT versión 3 para realizar el análisis y evaluación de los riesgos y las vulnerabilidades a las que están expuestos los activos de información de UNITRANSA S.A., una empresa de transporte urbano de pasajeros en la ciudad de Bucaramanga y su área metropolitana.

El estándar internacional ISO/IEC 27001 establece los requisitos para establecer, monitorear y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI). Este documento está hecho bajo las ordenanzas de esta norma.

Mantener la seguridad de la información y sus activos requiere como primera medida la adopción de una Política de Seguridad de la Información (PSI) robusta, documentada, conocida por todos, aprobada por la administración y revisada periódicamente, sin desconocer la aplicación de la legislación penal colombiana en materia de Seguridad Informática. Este manuscrito contiene de manera clara y sucinta las reglas de uso aceptado de los Activos de Información y la Información misma, al igual que las leyes colombianas aprobadas por el congreso para combatir los delitos informáticos.

La gestión de Activos de Información requiere la adopción de un mecanismo de control adecuado que permita algunas acciones como: control de acceso, uso, controles, importancia para los procesos de la empresa, criticidad de la información que manejan, entre otros. Estos mecanismos se logran con la utilización de un sistema de etiquetado de Activos de Información que UNITRANSA S.A. incorporó para mejorar la seguridad de su información.

Se considera que en la seguridad de la información los usuarios son el eslabón más débil, pues son ellos quienes interactúan con el mismo y explotan las vulnerabilidades existentes. En este orden de ideas, fomentar un sentido de pertenencia por la organización necesita la puesta en marcha de un programa de sensibilización de los usuarios del sistema en temas relacionados con la Seguridad de la Información y los activos; situación que se analiza detalladamente y se sugieren las pautas necesarias para adoptarla como parte de las tareas diarias.

El trabajo finaliza con una serie de conclusiones donde se expone las situaciones más relevantes que afectan la seguridad de la información y los activos,

clausurando con una serie de recomendaciones que de aplicarse de una manera sistemática y responsable se obtienen uno niveles altos de Seguridad de la Información que harán de UNITRANSA S.A. una empresa rentable y sostenible.

OBJETIVO GENERAL

Diseñar un Sistema de Gestión de Seguridad de la Información (SGSI) bajo la norma ISO 27001 en la empresa UNITRANSA S.A. para alcanzar unos niveles óptimos de la seguridad de la información.

OBJETIVOS ESPECIFICOS

- Plantear una técnica para gestionar el inventario de activos de información de UNITRANSA S.A. que admita incorporar, dar de baja y cambiar ubicación de los activos de información.
- Diseñar una metodología para el manejo de etiquetado de los activos de información de la organización.
- Proponer un mecanismo para concienciar a los empleados de UNITRANSA S.A. de la importancia de asumir la seguridad de la información como parte fundamental de sus funciones diarias.
- Diseñar las Políticas de Seguridad de la Información (PSI) para la empresa UNITRANSA S.A. usando la norma ISO 27001.

METODOLOGIA

Investigación aplicada a la empresa UNITRANSA S.A. debido a la carencia de un SGSI que administre la seguridad de la información y los activos de información. Se parte del modelo PHVA (Planear – Hacer – Verificar – Actuar) para su diseño y se siguen los preceptos de la metodología MAGERIT V3 para el análisis y evaluación de riesgos. El SGSI está enmarcado dentro del estándar ISO/IEC 27001.

CONCLUSIONES

- La realización del Análisis de Riesgos de los activos de información pudo establecer que existen dos Activos de Información (Sistema Operativo Windows XP y Red Local de UNITRANSA S.A.) en alto grado de nivel riesgo de probabilidad de ocurrencia de algún tipo de incidentes.
- La Política de Seguridad de la Información (PSI) es la herramienta básica con la que debe contar toda organización para alcanzar los niveles óptimos de seguridad, partiendo de la premisa de que, en la larga cadena de factores de seguridad, el eslabón más débil lo representan las personas.

- El sistema de gestión de inventario de activos de información no es lo suficientemente eficiente para ejercer un control sobre los equipos en aspectos como pertenencia a un departamento, propietario, nivel de criticidad, procesos que maneja, controles, entre otros.
- La incorporación de un plan de sensibilización es primordial para alcanzar los objetivos trazados en el diseño del proyecto de seguridad de la información.