DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

TESIS PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS E INFORMÁTICA

AUTOR: MONCAYO SALAS ERIKA PATRICIA

TEMA: DESARROLLO DE UN SISTEMA DE GESTIÓN EN CONTROL Y SEGURIDAD BASADO EN LA NORMA BASC PARA LA EMPRESA TRANSPORTES Y SERVICIOS ASOCIADOS SYTSA CÍA. LTDA.

DIRECTOR: ING. MAURICIO CAMPAÑA

CODIRECTOR: ING. FERNANDO SOLÍS

SANGOLQUÍ, SEPTIEMBRE 2014

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por la Sra. ERIKA PATRICIA MONCAYO SALAS como requerimiento parcial a la obtención del título de INGENIERO EN SISTEMAS E INFORMÁTICA.

Sangolquí, SEPTIEMBRE del 2014

_____	_____
ING. MAURICIO CAMPAÑA	ING. FERNANDO SOLÍS
DIRECTOR DE TESIS	CODIRECTOR DE TESIS

AUTORÍA DE RESPONSABILIDAD

Yo, Erika Patricia Moncayo Salas declaro que el presente trabajo es de nuestra autoría; que no ha sido previamente presentado para ningún grado o calificación personal y que hemos consultado las referencias bibliográficas que se incluyen en el documento.

La Universidad de las Fuerzas Armadas ESPE puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley de Propiedad Intelectual por su reglamento y por la normativa institucional vigente

Sangolquí, SEPTIEMBRE del 2014

_____

Erika Patricia Moncayo Salas

AUTORIZACIÓN

Yo, **ERIKA PATRICIA MONCAYO SALAS**, autorizo a la Universidad de las Fuerzas Armadas ESPE la publicación en el repositorio digital de la biblioteca Alejandro Segovia el presente proyecto denominado **"DISEÑO DE UN SISTEMA DE GESTIÓN EN CONTROL Y SEGURIDAD BASADO EN LA NORMAS BASC PARA LA EMPRESA TRANSPORTES Y SERVICIOS ASOCIADOS SYTSA CÍA. LTDA.**, así como también los materiales y documentos relacionados a la misma.

Sangolquí, SEPTIEMBRE de 2014

_____

Erika Patricia Moncayo Salas

DEDICATORIA

A mi madre que siempre mantuvo su fe en mí, que siempre estuvo a mi lado con una palabra de aliento, de apoyo en todo sentido, con su amor, con su cariño incondicional y con una sonrisa en su rostro para alegrar mis días.

A mi padre, que siempre busco la forma de sacar a sus hijos adelante sin importar todos los obstáculos que se atravesaron a los largo de todos estos años. Por todos los valores que me enseñó y que están arraigados en mi mente y corazón.

A mi esposo, que ha sido durante todos estos años juntos mi piedra angular, mi amigo, mi cómplice a quien admiro y amo por su fortaleza, por buscar siempre ser alguien mejor, por su paciencia, comprensión y su tiempo.

A mis hijas que son la razón más importante para cada día salir adelante, son mi alegría, mi fuerza para continuar y que con su inocencia me demuestran lo que significa el amor incondicional, me inspiran a ser mejor.

Y por último con todo mi cariño y amor a aquellas personas importantes en mi vida que no dudaron en brindarme toda su ayuda a lo largo de esta etapa de mi vida.

ERIKA MONCAYO

AGRADECIMIENTOS

Agradezco a Dios en primer lugar por permitirme una oportunidad más para estar junto a mi familia. A mostrarme que día a día con humildad, paciencia y constancia todo es posible.

Agradezco a mis padres, por la formación que me dieron, por todo su esfuerzo y dedicación para que hoy culmine con un gran objetivo.

A mi esposo que siempre me dio su apoyo incondicional, que no dudo en brindarme su tiempo, su conocimiento y sobre todo su amor.

A mis hermanos, familiares y amigos que siempre estuvieron pendientes y fueron de mucho apoyo durante todo este proceso.

A mis Directores de Tesis Ing. Mauricio Campaña e Ing. Fernando Solís que gracias a sus conocimientos y enseñanzas me encaminaron por la senda correcta.

ERIKA MONCAYO

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El presente proyecto constituye la elaboración de un Sistema de Gestión en Control y Seguridad para la Empresa Transportes y Servicios Asociados Sytsa, con la finalidad de generar una cultura de seguridad en la organización como requerimiento de sus clientes en vista de las constantes irregularidades que existen en el área del comercio y segundo porque requieren de establecer políticas y procedimientos aplicados a los Sistemas de Información que permitan la obtención de la Certificación Basc en una de sus áreas de auditoría. Este proceso iniciará con una evaluación de la situación actual de la empresa mediante la recopilación de información a través de encuestas, entrevistas, formularios, etc. Posteriormente se elabora el Análisis de Riesgos donde se establecen los activos, las amenazas y las salvaguardas. Para este proceso se utilizó la metodología MAGERIT, procedimiento para realizar Análisis de Riesgos, donde se obtiene como resultado el Impacto y los Riesgos que recae sobre los recursos informáticos de la empresa. Como producto final de este análisis se propone un Sistema de Gestión y Control mediante la generación de políticas y procedimientos según lo que recomienda la ISO 27001 para que posteriormente sean implementadas en la empresa y puedan cumplir con los requisitos de obtención de la certificación.

Palabras Clave: **SISTEMA DE GESTIÓN, TRANSPORTE TERRESTRE, NORMA BASC, POLÍTICAS, SEGURIDAD.**

ABSTRACT

This project is the development of a Management Sistema Control and Security for Transportes y Servicios Asociados Sytsa Organization, in order to create a safety culture as clients requirements in view of the irregularities that exist in the trade area and second because they require to stablish policies and procedures applied to the Information System that allow obtaining the Certification Basc in one of their areas to audit. This process starts with an assessment of the current situation of the company by collecting information through surveys, interviews, forms and others. Later Risk Analysis where assets are set, the threats and safeguards is made. MAGERIT methodology procedure was used to perform risk analysis which is obtained as a result the Impact and Risks borne by the computing resources of the company for this process. The final product of this Analysis is proposed a Management and Control System through the development of policies and procedures as recommended by the ISO 27001 to be subsequently implemented in the company and can meet the requirements for obtaining certification.

***Key Words*: MANGEMENT SYSTEM, GROUND TRANSPORTATION, NORMA BASC, SECURITY, POLICIES.**

CAPÍTULO 1

GENERALIDADES

1.1 INTRODUCCIÓN

La seguridad de la información comprende diversos aspectos entre ellos la disponibilidad, comunicación, identificación de problemas, análisis de riesgos, la integridad, confidencialidad, recuperación de los riesgos. (Fernández, 1988)

La seguridad de la información comprende diversos aspectos entre ellos la disponibilidad, comunicación, identificación de problemas, análisis de riesgos, la integridad, confidencialidad, recuperación de los riesgos. (Fernández, 1988)

La correcta Gestión de la Seguridad de la Información busca establecer y mantener programas, controles y políticas, que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información, si alguna de estas características falla no se está ante nada seguro. Es preciso anotar, además, que la seguridad no es ningún hito, es más bien un proceso continuo que hay que gestionar conociendo siempre las vulnerabilidades y las amenazas que se ciñen sobre cualquier información, teniendo siempre en cuenta las causas de riesgo y la probabilidad de que ocurran, así como el impacto que puede tener. (Fernández, 1988)

La Seguridad Tecnológica en una empresa se define como un conjunto de reglas, planes y acciones que permiten asegurar la información contenida en uno o varios sistemas de la empresa. Pero para garantizar esta seguridad no es suficiente

con un conjunto de software avanzado capaz de proteger nuestra red, sino que la labor principal reside en la persona física que administra el sistema, la cual debe ser capaz de analizar situaciones futuras y tomar decisiones, para prevenir de esta forma posibles ataques, porque la mejor forma de combatir al enemigo es anticipándose a sus movimientos**.** (INTECO, 2013)

Este documento pretende diseñar un Sistema de Gestión en Control y Seguridad basado en la Norma BASC para la empresa Transportes y Servicios Asociados SYTSA Cía. Ltda. Empresa dedicada al Transporte de Mercancía a Nivel Internacional que permita cumplir y por ende poner en práctica lineamientos que a futuro fomenten una cultura de seguridad hacia los recursos informáticos de la empresa.

1.2 ANTECEDENTES

La Empresa Transportes y Servicios Asociados SYTSA es una empresa con una amplia experiencia en el área de transporte, coordinación, bodegaje, movimiento y asesoramiento de todo tipo de embarques refrigerados o secos dentro del país así como también fuera (Colombia, Perú, Venezuela). Por tal razón es de suma importancia que la empresa cuente con Certificaciones que garanticen un servicio de Logística y Coordinación excelente desde que se embarca hasta que se llega a destino final es decir al Cliente. Se torna importante el manejo de la información que se genera tanto interna como externamente de la empresa.

MISIÓN

Proporcionar soluciones logísticas y aduaneras con: tecnología, seguridad y eficiencia; al servicio de clientes corporativos en el ámbito local, nacional e internacional.

VISIÓN

Consolidarnos como la mejor opción logística y aduanera garantizando seguridad con eficiencia, utilizando herramientas de gestión adecuadas para el beneficio de clientes, socios, empleados y proveedores.

Para llevar adelante sus actividades, SYTSA tiene su Oficina Matriz en la ciudad de Quito, desde donde se desarrollan los procesos administrativos, financieros, contables, de operaciones y abastecimientos. Adicionalmente, cuenta con tres oficinas ubicadas en las ciudades de Guayaquil, Tulcán y Huaquillas que sirven de soporte a las operaciones y un taller, plenamente equipado, ubicado en Quito, para el mantenimiento preventivo y correctivo los equipos de la empresa. Se mantiene un representante en Colombia, en la ciudad de Ipiales y un representante en Perú con quienes se respalda su funcionamiento fuera del País.

SYTSA presta servicios de transporte de carga por carretera a nivel nacional e internacional (se ejecutan operaciones en Colombia y Perú). Las operaciones que desarrolla la empresa se apoyan en una importante flota de vehículos debidamente acondicionados, en las modalidades de productos congelados, refrigerados, líquidos y maquinaria.

Para mantener la cadena de seguridad y disminuir el riesgo de una posible contaminación de sus servicios por el Narcotráfico y el Terrorismo, los Accionistas de la empresa han tomado la decisión de afiliar la empresa al BASC con la finalidad de fortalecer sus procedimientos de seguridad y obtener su certificación.

La Coalición Empresarial Anticontrabando BASC (Business Anti Smuggling Coalition), se ha consolidado como modelo mundial de los programas de cooperación, gracias a la asociación exitosa entre el sector empresarial, aduanas, gobiernos y organismos internacionales que lograron fomentar procesos y controles seguros.

La cooperación se fundamenta principalmente en un intercambio permanente de experiencias, información y capacitación, lo cual ha permitido a las partes incrementar sus conocimientos y perfeccionar sus prácticas en un esfuerzo por mantener las compañías libres de cualquier actividad ilícita y a la vez facilitar los procesos aduaneros de las mismas.

Las empresas que forman parte del BASC son auditadas periódicamente y ofrecen la garantía de que sus productos y servicios son sometidos a una estricta vigilancia en todas las áreas mediante diversos sistemas y procesos.

La iniciativa BASC refleja el compromiso de las empresas por mejorar las condiciones de su entorno, y a su vez, contribuye a desalentar fenómenos que perjudiquen los intereses económicos, fiscales y comerciales del país.

1.3 JUSTIFICACIÓN E IMPORTANCIA

El mundo de hoy se caracteriza por un aumento cada vez más extraordinario de las actividades mercantiles y de intercambio de bienes y servicios. A la par de este intercambio incesante de elementos de comercio, aparecen también problemas fundamentales como el contrabando, la evasión de normas de calidad, la piratería y la competencia desleal entre las diferentes empresas que existen en nuestro mundo capitalista.

La seguridad no depende del azar. Las organizaciones deben dar la misma o mayor importancia al logro de altos estándares de Gestión en Control y Seguridad, que dan a otros aspectos de sus actividades empresariales. Esto exige adoptar una propuesta estructurada para la identificación de los peligros, la evaluación y control de los riesgos relacionados con las actividades de comercio internacional que las empresas realizan.

La Empresa SYTSA, es una empresa dedicada al Transporte Pesado, que busca la certificación BASC, por lo tanto necesita del Diseño de un Sistema de Gestión en Control y Seguridad.

Es importante que la empresa determine la vulnerabilidad de la organización a problemas de seguridad actuales y a futuro, determinar las alternativas disponibles para ser utilizadas por la empresa para cubrir las necesidades. Los Elementos que cubren la norma BASC. Son esenciales para un sistema eficaz de Gestión de Control y Seguridad en el Comercio Internacional.

Mediante la elaboración de este SGSI se desea conseguir que la empresa minimice considerablemente el riesgo de su productividad debido a la ocurrencia de un evento que comprometa la confidencialidad, disponibilidad e integridad de sus activos.

Los recursos informáticos tales como como equipos informáticos, aplicaciones, servicios, redes de comunicación o la misma información deben estar disponibles para servir de apoyo a las labores que la empresa lleve a cabo. La no disponibilidad de alguno dilataría los tiempos lo que incidiría negativamente en la imagen de la empresa frente a sus clientes.

1.4 OBJETIVOS

1.4.1 Objetivo General

Diseñar un Sistema de Gestión en Control y Seguridad basado en la Norma BASC para la Empresa Transportes y Servicios Asociados SYTSA Cía. Ltda.

1.4.2 Objetivo Específico

- Desarrollar un Sistema de Gestión de Seguridad de Información (SGSI) que permita una correcta gestión de los riesgos para precautelar las características de la información: confidencialidad, integridad y disponibilidad.
- Realizar el Análisis de Gestión de Riesgos donde se determinarán y clasificarán los activos informáticos que posee la empresa, el establecimiento de amenazas y salvaguardas.

- Establecer el Impacto y los Riesgos obtenidos como resultado del análisis de gestión de riesgos a realizar.

- Evaluar las políticas y directrices para proteger los recursos informáticos de eventos que puedan afectar la disponibilidad.

- Definir los controles necesarios para asegurar el uso aceptable de los recursos informáticos por parte de los funcionarios.

1.5 ALCANCE

La Empresa Transportes y Servicios Asociados SYTSA, es una empresa dedicada al Transporte de Mercancía tanto nacional como internacional que está aplicando a la Certificación BASC. El desarrollo de este proyecto esta basado en esta Norma, con el afán de mejorar en varios aspectos tecnológicos de la empresa, mediante el desarrollo de un Sistema de Gestión en Control y Seguridad, donde se permitirá identificar y visualizar:

- Una restructuración y creación de nuevas políticas de seguridad informática.

- Evaluar del estado actual de la Empresa.

- Identificar los riesgos y amenazas a los que están expuestos los recursos informáticos (software, equipos, redes, comunicaciones, información, etc.).

- Identificar las salvaguardas existentes, los impactos de los riesgos a los que están expuestos los recursos informáticos.

- Emitir el informe para realizar las correcciones en base a las falencias encontradas.

- Establecer recomendaciones en base al análisis de riesgo a realizar, con el objetivo de que se implemente en lo posterior las políticas a obtenerse del Plan de Seguridad.

- Generar controles sobre las amenazas encontradas hacia los activos informáticos que posee la empresa; con el fin de que la Gerencia realice una adecuada toma de decisiones.

- Este proyecto no contempla la implementación del Plan de Seguridad, solamente incluye la definición de políticas y directrices para que este plan pueda ser elaborado posteriormente.

CAPÍTULO 2

MARCO TEÓRICO

2.1 LA INFORMACIÓN

Durante el proceso de evolución del uso de la tecnología como soporte a las operaciones en las organizaciones siempre ha existido la preocupación por evitar incidentes que comprometan la seguridad.

La seguridad de la información consiste en combinar de manera coherente las herramientas técnicas de seguridad y a la vez gestionar el comportamiento del factor humano tratando de reducir en lo posible las vulnerabilidades o posibles atentados contra la seguridad de la información y sistemas. (27000)

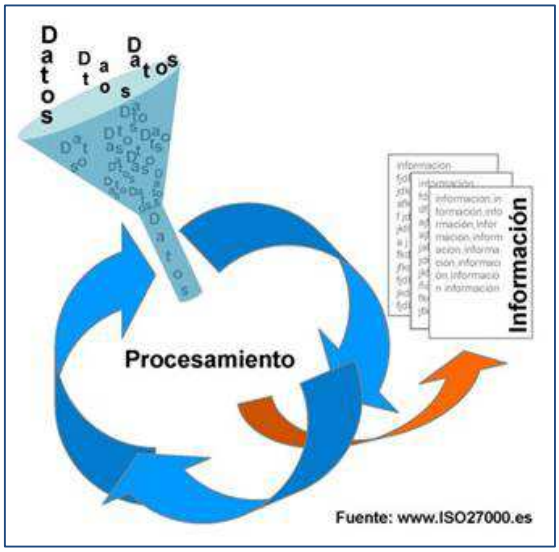


Figura 1 Procesamiento de la información. Fuente *www.iso27000.es*

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información: (27000)

2.1.1 Confidencialidad de Datos. Cuando el usuario o el empleado garantice que la información que se está ingresando no sea divulgada a personas externas y ajenas a la empresa. (27000)

2.1.2 Disponibilidad de los datos. Es el acceso a la información cuando esta se la requiera para que los usuarios puedan realizar las diferentes actividades de actualización, respaldos, etc. (27000)

2.1.3 Integridad de datos. Se refiere a la seguridad de que la información no ha sido alterada, borrada, reordenada, copiada, etc. Sea durante el proceso de transmisión o en su origen. (27000)

Existen otros atributos de la información como son:

2.1.4 Autenticación. La garantía de que quien firme un mensaje es realmente quien dice ser. (27000)

2.1.5 No Repudio. Garantía de que ninguna de las partes involucradas pueda negar en el futuro una operación realizada. (27000)

Generalmente la seguridad se concentrar en garantizar el derecho de acceder a los datos y recursos del sistema configurando los mecanismos de autenticación y control que aseguran que los usuarios de estos recursos solo posean los derechos que se les han otorgado. (ISO 27000)

Uno de los primeros pasos que debe dar una compañía es definir una política de seguridad que se pueda implementar en función a:

- Identificar las necesidades de seguridad y los riesgos informáticos que enfrenta la compañía así como las posibles consecuencias. (ISO 27000)

- Proporcionar una perspectiva general de las reglas y los procedimientos que deben implementarse para afrontar los riesgos identificados en los diferentes departamentos de la organización. (ISO 27000)

- Controlar y detectar las vulnerabilidades del sistema de información y mantenerse informado acerca de las falencias en las aplicaciones y en los materiales que se usan. (ISO 27000)

- Definir las acciones a realizar y las personas a contactar en caso de detectar una amenaza. (ISO 27000)

La política de seguridad comprende todas las reglas de seguridad que sigue una organización. Por lo tanto la administración de la organización debe encargarse de definirla ya que afecta a todos los usuarios del sistema.

La seguridad informática de una compañía depende de que los empleados aprendan las reglas a través de sesiones de capacitación y de concientización.

2.2 NORMA BASC V4

World BASC Organization, Inc. es una entidad sin ánimo de lucro liderada por el sector empresarial y con apoyo de Aduanas y Organismos Internacionales, cuya misión es facilitar y agilizar el Comercio Internacional mediante el establecimiento y administración de estándares y procedimientos globales de seguridad aplicados a la cadena logística del Comercio Internacional. (BASC, 2011)

La creación de BASC se remonta a 1996 cuando una empresa Norteamericana decidió presentar la propuesta antes el Comisionado del Servicio de Aduana de los Estados Unidos en San Diego California, con el propósito de implementar mecanismos y procedimientos que ayudaran a evitar ser utilizados por organizaciones ilícitas para el transporte de narcóticos y buscar poner fin a una larga lista de experiencia con robos y cargamentos contaminados de empresas de todos los sectores y como una forma de complementar y fortalecer los programas. (BASC, 2011)

BASC se ha consolidado como modelo mundial de los programas de cooperación, gracias a la asociación exitosa entre el sector empresarial, aduanas, gobiernos y organismos internacionales que lograron fomentar procesos y controles seguros. (BASC, 2011)

La seguridad no depende del azar. Las organizaciones deben dar la misma o mayor importancia al logro de altos estándares de Gestión en Control y Seguridad,

que dan a otros aspectos de sus actividades empresariales. Esto exige adoptar una propuesta estructurada para la identificación de los peligros y la evaluación y control de los riesgos relacionados con el las actividades de Comercio Internacional que realizan. (BASC, 2011)

Esta norma está destinada a ayudar a las organizaciones en el desarrollo de una propuesta de Gestión en Control y Seguridad en el Comercio Internacional, que proteja a las empresas, a sus empleados y otras personas cuya seguridad puedan verse afectadas por sus actividades. Muchas de las características de una administración efectiva no se pueden distinguir de las prácticas propuestas de administración de calidad y excelencia empresarial. (BASC, 2011)

La Norma BASC está diseñada de tal forma que su contenido sea totalmente comprensible, permitiendo que el Sistema de Gestión sea aplicable a las organizaciones que hoy día participan en actividades de Comercio Internacional, buscando demostrar conformidad con todos y cada uno de los requisitos que se determinan tanto en la norma como en los Estándares BASC y en otro tipo de programas de Seguridad que hoy día han sido establecidos por diferentes entidades internacionales tales como el Marco de Estándares de la Organización Mundial de Aduanas (Framework of Standards), el Código de Protección de buques e instalaciones portuarias emitido por la Organización Marítima Internacional, etc. Esta norma constituye un marco general para la implementación del Sistema de Gestión en Control y Seguridad BASC, con la cual las organizaciones utilizando una metodología de procesos, planearán, implementarán, verificarán y tomarán las acciones necesarias en procura de mejorar su Sistema de Gestión en Control y Seguridad de una manera eficaz. (BASC, 2011).

Referencias Informativas

Esta Norma hace referencia a otras publicaciones que dan información u orientación tales como:

- WCO SAFE Framework of Standard – World Customs Organization
- Standards CTPATC Trade Partnership Against Terrorism.
- Coding ISPS/PBIP – Ship
- Safe Port Act
- ISO EC 27001/2007
- ISO PAS 17712/2010
- ISO 9001:2000, 14000
- OSHAS 18001:2007
- ANZ4360 NTC 5254
- ISO 14001:2004
- ISO 28000:2007

2.3. GENERALIDADES

2.3. 1 Consideraciones para preparar un programa de seguridad.

(BASC, 2011)

- Los requerimientos de seguridad de la organización.
- El potencial de la organización para cumplir los requisitos.
- La vulnerabilidad de la organización a problemas de seguridad actuales y futuros.
- Las alternativas disponibles para ser utilizadas por la organización para cubrir las necesidades.

2.3.2 Aspectos importantes que se deben incluir en un Plan de Seguridad.

(BASC, 2011)

- Definición clara de los métodos de seguridad.
- Procedimientos escritos para notificación interna/externa
- Mecanismos para responsabilizar en caso de robo o hurto
- Manejo de documentos y archivos
- Procedimientos para cierre de instalaciones (puertas, portones, ventanas, etc.).
- Sistemas de seguridad para registrar las entradas y salidas de personas y/o vehículos.
- Definición de políticas para el monitoreo externo
- Control y manejo de llaves con inventarios periódicos.
- Políticas y procedimientos para la contratación de personal
- Políticas que se aplicarán en la verificación de antecedentes
- Procedimientos para obtener fotografías y huellas digitales de todos los empleados.
- Asignación de responsabilidad para la seguridad contratada.

2.4 SISTEMAS DE GESTIÓN DE CALIDAD

En un documento llamado Buenas Prácticas de seguridad, tercera Edición 2009, elaborado por la organización BASC, el Sistema de Gestión se conceptúa así:

> *"El SGCS es una serie de elementos que interactúan o que están interrelacionados, para establecer y cumplir con una política y objetivos, con el fin de dirigir y controlar una organización con respecto a la seguridad"*.
>
> (EUMED, 2008)

Un Sistema de Gestión de Calidad es un sistema de gestión o administración de la calidad basada en una filosofía, con principios y métodos donde el ser humano es el factor más importante para obtener los objetivos de calidad. Este enfoque apareció en Japón a inicios de los años 50 del siglo pasado y sus principios son:

- No son los inspectores ni las personas del área de producción los responsables de garantizar la calidad si no toda la empresa con cada una de sus personas.

- La calidad empieza con la planeación no solo de los productos y servicios si no de los procedimientos y procesos que intervienen en su creación. (EUMED, 2008)

- La calidad demanda planificación estratégica avanzada, orientada al cliente, donde intervienen también los proveedores de la compañía con quienes se debe compartir la filosofía de la calidad. (EUMED, 2008)

- La calidad incluye mediciones constantes y metódicas de cada una de las áreas de la organización. Que constantes, suficientes datos e indicadores para tomar la decisión a tiempo y correctamente. (EUMED, 2008)

- El desarrollo de sistemas de gestión en control y seguridad.
- La interrelación con otras normas, códigos sobre sistemas de administración y gestión empresarial. (EUMED, 2008)

En consecuencia la gestión de calidad hoy es una necesidad, es una herramienta sin que ninguna organización pueda competir. (EUMED, 2008)

La norma está diseñada para ser utilizada por organizaciones de todos los tamaños, independientemente de la naturaleza de sus actividades. (EUMED, 2008)

2.5. DEFINICIONES

2.5.1 Análisis de Riesgo. Uso sistemático de la información disponible, para determinar la frecuencia con la cual pueden ocurrir eventos especificados y la magnitud de sus consecuencias. (BASC, 2011)

2.5.2 Auditoría del Sistema de Control y Seguridad. Examen sistemático e independiente para determinar si las actividades y resultados relacionados con la gestión en control y seguridad, cumplen las disposiciones preestablecidas y si estas se aplican en forma efectiva y son aptas para alcanzar los objetivos. (BASC, 2011)

2.5.3 Competencia. Idoneidad para conocer o solucionar un asunto derivado de la formación, entrenamiento y experiencia de cada individuo. Capacidad productiva de un individuo que se define y mide en términos de desempeño en un determinado contexto laboral y reflejan los conocimientos de habilidades, destrezas y actitudes para la realización de un trabajo efectivo y de calidad. (BASC, 2011)

2.5.4 Control. Actividad de monitorear los procesos y tomar medidas preventivas, correctivas y de mejora, para evitar eventos indeseables en el futuro. (BASC, 2011)

2.5.5 Evaluación de Riesgo. Proceso usado para determinar las prioridades de gestión mediante la Comparación del nivel de riesgo contra normas predeterminadas, niveles de riesgo objeto y otros criterios. (BASC, 2011)

2.5.6 Estándares BASC. Conjunto de requerimientos específicos aplicables, complementarios a esta norma y de obligatorio cumplimiento en función al alcance del SGCS, en las empresas que implementan un Sistema de Gestión en Control y Seguridad BASC. (BASC, 2011)

2.5.7 Mejora Continua. El objetivo de la mejora continua del Sistema de Gestión BASC es el de incrementar el desarrollo y ejecución de actividades de control y seguridad dentro de los procesos productivos y administrativos al interior de la Organización tendientes a asegurar los diferentes actores de la cadena del comercio internacional. (BASC, 2011)

2.6 ADMINISTRACIÓN DE RIESGOS

Riesgo:

"Combinación de la probabilidad de que se produzca un evento y sus consecuencias negativas" (UNISDR, Terminología sobre Reducción de Riesgos y Desastres 2009 para los conceptos de Amenaza, vulnerabilidad y riesgo).

"Es la proximidad voluntaria o inconsciente a una situación de peligro, Es la exposición al peligro o a circunstancias que nos puedan generar daños o consecuencias" (Normas Basc, 2012)

Según los conceptos de ORM (Operacional Risk Management) los riesgos han sido definidos como el proceso de tomar decisiones que puedan minimizar los efectos de pérdidas que genera la materialización de estos, Por eso es importante manejar, medir y calcular sus consecuencias para que ayude a tomar decisiones para prevenirlo de manera que el futuro de la empresa dependa de su elección y no de la elección de otros. Un manejo adecuado del riesgo permite que se generen menos pérdidas que sea menos severo, menos frecuentes y sea más predecible.

2.6.1 ¿CÓMO SE REALIZA UN SGSI?

Un Sistema de Gestión de Seguridad de la Información tomando como base la Norma ISO 27001, se pone en consideración el Ciclo Continuo PDCA. (27000)

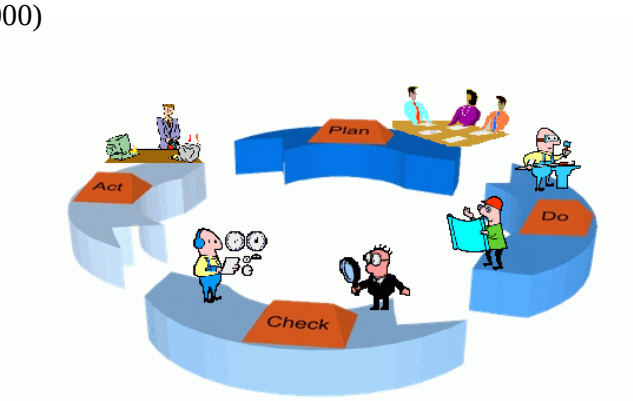


Figura 2 Ciclo continuo PDCA. Fuente ISO 27000

- **Plan. (Planificar)** Establece el SGSI
-

Definir el alcance del SGSI en términos del negocio, la organización, su localización, activos y tecnología, incluyendo detalles y justificación de cualquier exclusión (ISO 27000).

Definir una política de seguridad que:

- Incluir el marco general y los objetivos de seguridad de la información de la organización.

- Considerar requerimientos legales o contractuales relativos a la seguridad de la información;

- Estar alineados con el contexto estratégico de gestión de riesgos de la organización en el que se establecerá y mantendrá el SGSI;

- Establecer los criterios con los que se va a evaluar el riesgo;

- Estar aprobado por la dirección.

Definir una metodología de evaluación del riesgo apropiada para el SGSI y los requerimientos del negocio, además de establecer los criterios de aceptación del riesgo y especificar los niveles de riesgo aceptable. Lo importante de esta metodología es que los resultados obtenidos sean comparables y repetibles existen numerosas metodologías estandarizadas para la evaluación de riesgos, aunque es perfectamente aceptable definir una propia. En este caso se utilizará la herramienta PILAR para la realización del análisis de riesgo. (ISO 27000)

- **Identificar los riesgos:**

(ISO 27000)

- Identificar los activos que están dentro del alcance del SGSI y a sus responsables directos, denominados propietarios;

- Identificar las amenazas en relación a los activos;

- Identificar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas;

- Identificar los impactos en la confidencialidad, integridad y disponibilidad de los activos.

- **Analizar y evaluar los riesgos:**

- Evaluar el impacto en el negocio de un fallo de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información;

- Evaluar de forma realista la probabilidad de ocurrencia de un fallo de seguridad en relación a las amenazas, vulnerabilidades, impactos en los activos y los controles que ya estén implementados;

- Estimar los niveles de riesgo;

- Determinar, según los criterios de aceptación de riesgo previamente establecidos, si el riesgo es aceptable o necesita ser tratado. (ISO 27000)

2.6.2. Tratamiento de Riesgos

- Identificar y evaluar las distintas opciones de tratamiento de los riesgos.

- Aplicar controles adecuados;

- Aceptar el riesgo, siempre y cuando se siga cumpliendo con las políticas y criterios establecidos para la aceptación de los riesgos;

- Evitar el riesgo, por ejemplo, mediante el cese de las actividades que lo originan; transferir el riesgo a terceros, por ejemplo, a compañías aseguradoras o proveedores de outsourcing.

Figura 3 Gestión de Riesgos Fuente ISO 27000

2.6.3. Objetivos de Control y Controles

(ISO 27000)

- Seleccionar los objetivos de control y los controles que propone la ISO 27001 para el tratamiento del riesgo que cumplan con los requerimientos identificados en el proceso de evaluación del riesgo.

- Aprobar por parte de la dirección tanto los riesgos residuales como la implantación y uso del SGSI.

- Definir una declaración de aplicabilidad que incluya:

- Los objetivos de control y controles seleccionados y los motivos para su elección.

- Los objetivos de control y controles que actualmente ya están implantados.

- Los objetivos de control y controles del Anexo A excluidos y los motivos para su exclusión; este es un mecanismo que permite, además, detectar posibles omisiones involuntarias. (ISO 27000)

- **Do. (Hacer)** Implementar y utilizar el SGSI

  - Definir un plan de tratamiento de riesgos que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.

  - Implantar el plan de tratamiento de riesgos, con el fin de alcanzar los objetivos de control identificados, incluyendo la asignación de recursos, responsabilidades y prioridades.

  - Implementar los controles anteriormente seleccionados que lleven a los objetivos de control.

  - Definir un sistema de métricas que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles o grupos de controles.

  - Procurar programas de formación y concienciación en relación a la seguridad de la información a todo el personal.

  - Gestionar las operaciones del SGSI.

  - Gestionar los recursos necesarios asignados al SGSI para el mantenimiento de la seguridad de la información.

  - Implantar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad. (ISO 27000)

• **Check (Verificar)** Monitorizar y revisar el SGSI

La organización deberá:

- Ejecutar procedimientos de monitorización y revisión para:
    - Detectar a tiempo los errores en los resultados generados por el procesamiento de la información;
    - Identificar brechas e incidentes de seguridad;
    - Ayudar a la dirección a determinar si las actividades desarrolladas por las personas y dispositivos tecnológicos para garantizar la seguridad de la información se desarrollan en relación a lo previsto;
    - Detectar y prevenir eventos e incidentes de seguridad mediante el uso de indicadores;
    - Determinar si las acciones realizadas para resolver brechas de seguridad fueron efectivas.
- Revisar regularmente la efectividad del SGSI, atendiendo al cumplimiento de la política y objetivos del SGSI, los resultados de auditorías de seguridad, incidentes, resultados de las mediciones de eficacia, sugerencias y observaciones de todas las partes implicadas.
- Medir la efectividad de los controles para verificar que se cumple con los requisitos de seguridad.
- Revisar regularmente en intervalos planificados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables, teniendo en cuenta los posibles cambios que hayan podido producirse en la organización, la tecnología, los objetivos y procesos de negocio, las amenazas

identificadas, la efectividad de los controles implementados y el entorno exterior -requerimientos legales, obligaciones contractuales, etc.-.

- Realizar periódicamente auditorías internas del SGSI en intervalos planificados.
- Revisar el SGSI por parte de la dirección periódicamente para garantizar que el alcance definido sigue siendo el adecuado y que las mejoras en el proceso del SGSI son evidentes.
- Actualizar los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitorización y revisión.
- Registrar acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del SGSI. (ISO 27000)
-

- **Act (Actuar)** Mantener y mejorar el SGSI

La organización deberá regularmente:

- Implantar en el SGSI las mejoras identificadas.
- Realizar las acciones preventivas y correctivas adecuadas en relación a la cláusula que menciona la ISO 27001 y a las lecciones aprendidas de las experiencias propias y de otras organizaciones.
- Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder.
- Asegurarse que las mejoras introducidas alcanzan los objetivos previstos.

PDCA es un ciclo de vida continuo, lo cual quiere decir que la fase de Act lleva de nuevo a la fase de Plan para iniciar un nuevo ciclo de las cuatro fases. Téngase en

cuenta que no tiene que haber una secuencia estricta de las fases, sino que, por ejemplo, puede haber actividades de implantación que ya se lleven a cabo cuando otras de planificación aún no han finalizado; o que se monitoricen controles que aún no están implantados en su totalidad. (ISO 27000)

En esta tesis se realizará el Sistema de Gestión de Seguridad Informática más no la Implementación de la misma.

2.7 NORMAS ISO 27000

2.7.1 HISTORIA.

Durante más de un siglo, el Instituto Británico de Normas Técnicas (BSI) y la Organización Internacional de Normas Técnicas (ISO) han brindado parámetros globales a [1] las normas técnicas de operación, fabricación y desempeño. Solo faltaba que BSI e ISO propusieran una norma técnica para la Seguridad de la Información. (ISO 27000)

En 1995, el BSI publicó la primera norma técnica de seguridad; la BS 7799, la cual fue redactada con el fin de abarcar los asuntos de seguridad relacionados con el e – commerce. La Norma se consideraba inflexible y no tuvo gran acogida. No se presentó la norma técnica en un momento oportuno y los problemas de seguridad no despertaron mucho interés en ese entonces. (ISO 27000)

En Mayo de 1999, el BSI intentó de nuevo publicar su segunda versión de la Norma BS 7799, la que fue una revisión más amplia de la primera publicación. En Diciembre del 2000, La ISO adoptó y publicó la primera parte de su norma BS 7799 bajo el nombre de ISO 17799. (ISO 27000)

[1] **Tomado de http://www-iso27000.es/sgsi .html**

En Septiembre del 2002 se publicó BS 7799 – 2; en esta revisión se adoptó el "Modelo de Proceso" con el fin de alinearla con ISO 9001 e ISO 14001. (ISO 27000)

El 15 de Octubre del 2005 se aprueba la Norma ISO 27001:2005 y en 2006 existen más de 2030 compañías certificadas a nivel mundial. (ISO 27000)

2.7.2 DEFINICIÓN DE LAS NORMAS ISO 27000

La serie ISO 27000 es una Familia de Estándares internacionales para Sistemas de Gestión de Seguridad de la Información (SGSI), que propone requerimientos de sistemas de gestión de seguridad de la información, gestión de riesgo, métricas y medidas, guías de implantación, vocabulario y mejora continua. (ISO 27000)

- **ISO 27000**

  En fase de desarrollo. Contendrá términos y definiciones que se emplean en toda la serie 27000. La aplicación de cualquier estándar necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión. (ISO 27000)

- **ISO 27001**

  Es la norma principal de requerimientos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual serán certificados por auditores externos los SGSI de las organizaciones. Fue publicada el 15 de Octubre de 2005 y sustituye a la BS7799-2, habiéndose establecido unas condiciones de transición para aquellas empresas certificadas en esta

última. Se lista en forma de resumen los objetivos de control y controles que desarrolla la ISO17799:2005 (futura ISO27002), para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en esta última, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados. (ISO 27000)

- **ISO 27002 (ISO 17799)**

Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. (ISO 27000)

- **ISO 27003**

Se centra en los aspectos críticos necesarios para la implementación de un SGSI, describiendo los procesos de especificación del SGSI y el diseño desde la elaboración de planes hasta la ejecución. (ISO 27000)

- **ISO 27004**

Especifica las métricas y las técnicas de medida aplicables para determinar la eficiencia y efectividad de la implantación de un SGSI y de los controles relacionados. Estas métricas se usan fundamentalmente para la medición de los componentes de la fase “Do” (Implementar y Utilizar) del ciclo PDCA. (ISO 27000)

- **ISO 27005**

Consiste en una guía para la gestión del riesgo de la seguridad de la información y sirve por tanto, de apoyo a la ISO27001 y a la implantación de un SGSI. Se basa en la BS7799-3 (publicada en Marzo de 2006) y probablemente, en ISO 13335. (27000)

- **ISO 27006**

Especifica el proceso de acreditación de entidades de certificación y el registro de SGSI. (27000)

- **ISO 27001 /2013**

Cuando su publicación se haga oficial va a tener gran impacto en las empresas que se encuentra certificadas, las organizaciones tendrán un período de tiempo para efectuar la transición a la nueva versión de la Norma. La transición se la puede realizar mediante la realización de una auditoría. (27000)

2.8 MAGERIT

Para la realización de estas tesis se utilizará la Metodología MAGERIT, este fue creado por el Consejo Superior de Administración Electrónica de España, en respuesta al crecimiento de la Tecnología de Información y el uso del que está siendo objeto las organizaciones, con el fin de concientizar a todos aquellos responsables de la existencia de riesgos y de la necesidad de amenorarlos a tiempo. Ofrece un método sistemático para analizar los riesgos. Ayuda a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control y prepara a

la organización para procesos de evaluación, auditoría, certificación o acreditación según sea el caso. (PILAR, 2012).

Mediante este método se puede conocer el nivel de riesgo actual de los activos y con la aplicación de nuevas salvaguardas o mejorando las que están implementadas permitiendo que el riesgo se minimice. (PILAR, 2012)

MAGERIT, tiene las siguientes fases:

2.8.1 Planificación de Proyectos

(PILAR, 2012)

Establece el marco general de referencia para todo el proyecto. En este paso se debe realizar:

- Establecer las condiciones para la realización del proyecto
- Investigar la oportunidad de realizarlo
- Define objetivos y dominio que abarcará
- Planifica los medios materiales y humanos para la realización
- Lanzamiento del proyecto

2.8.2. Análisis de Riesgos

(PILAR, 2012)

- Identificar los activos, las relaciones y su valoración
- Identificar Amenazas significativas sobre los activos evaluándolos en términos de ocurrencia y degradación
- Identificar Salvaguardas, valorando la eficacia de su implantación
- Interpretación del impacto y el riesgo.

2.8.3 Gestión de Riesgos

(PILAR, 2012)

- Elegir una estrategia para la mitigación del impacto y el riesgo.
- Determinar las salvaguardas oportunas para lo tratado en el punto anterior.
- Determinar la calidad necesaria para las salvaguardas propuestas.
- Diseñar un Plan de Seguridad (Plan de Acción o Plan al Director) para llevar el impacto y el riesgo a niveles aceptables.
- Ejecutar el Plan de Seguridad.

2.9 PILAR

Pilar, acrónimo de "Procedimiento Informático-Lógico para el Análisis de Riesgos" es una aplicación informática desarrollada bajo especificación del Centro Criptológico Nacional-Centro Nacional de Inteligencia (CCN-CNI) para soportar el análisis de riesgos de sistemas de información siguiendo la metodología MAGERIT, la herramienta comercial está ampliamente utilizada en la Administración Pública y en la actualidad también en organismos no gubernamentales. Tiene por objetivo realizar el análisis según la Metodología MAGERIT y diseñar el Plan de Mejora de la Seguridad. (EAR PILAR, 2014)

Ofrece un conjunto de herramientas que permiten: (Méndez, Andrés, Mañas, José Antonio, 2010, MANUAL DE USUARIO PILAR BASIC Versión, 4.4)

(EAR PILAR, 2014)

- " Un análisis general, estudiando las diferentes dimensiones de seguridad (Confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad)

- Un análisis de continuidad centrándose en la disponibilidad del Sistema de Información para detener interrupciones de servicio ante incidentes o desastres. “

Pilar permite realizar un seguimiento continuo del Sistema de la Empresa con el fin de que el sistema enfrente riesgos actuales y futuros así tener mayor confianza del sistema que posee. (EAR PILAR, 2014)

CAPÍTULO 3

ANÁLISIS DE GESTIÓN DE RIESGOS

Tomando como base la Metodología MAGERIT a continuación se detalla los pasos a seguir.

3.1 PLANIFICACIÓN DEL PLAN DE SEGURIDAD

3.1.1 Objetivo

- Motivar y concienciar a la Gerencia de la Organización, sobre la importancia de realizar un Análisis de Gestión de Riesgos.
- Establecer una cultura de seguridad sobre los recursos informáticos.
- Minimizar los riesgos hacia los activos informáticos de la empresa.

Para un trabajo eficiente es necesario contar con la colaboración y participación de todo el personal involucrado con los Sistemas de Información.

A continuación se presenta las siguientes actividades y tareas

- Estudio de Oportunidad.
- Determinación del Alcance del Proyecto
- Planificación del Proyecto
- Lanzamiento del Proyecto.

3.1.2 Estudio de Oportunidad

Mediante este procedimiento lo que se trata es de identificar el interés de la Alta Gerencia sobre la realización de un Análisis de Gestión de Riesgos.

SYTSA es una empresa dedicada al Transporte de Mercancía Nacional e Internacional. Por tanto debe cumplir con Normas y Estándares que permita que todos los procesos que intervienen para que el embarque y desembarque de la carga sea cien por ciento seguro, en este caso nos enfocamos en la normas solicitadas por el BASC, certificado que la Empresa está obteniendo.

Por tanto la aplicación de recursos tecnológicos para la seguridad de todos los procedimientos que incluya a la Seguridad de la Información se ha tornado un tema muy importante dentro de la Empresa. Al realizar este análisis se emitirá un informe con medidas concretas que mitiguen o eliminen el riesgo a los Sistemas de Información y a la Empresa en conjunto mismo, como por ejemplo: incidentes, cambios de tecnología, la no existencia de evaluación de las necesidades para alcanzar un nivel de seguridad aceptable, etc.

En la sección de anexos se realizó la recopilación a detalle del hardware, software, medios de comunicación, bases de datos, medios humanos, técnicos etc. con los que la empresa consta actualmente, con la ayuda de la Alta Gerencia, responsable del Área de Sistemas y responsable del Departamento de Calidad y Seguridad en general. También se obtuvo información sobre antecedentes sobre la Seguridad de los Sistemas de Información, con todos estos datos y con el afán de aplicar a la Certificación BASC se determinó la necesidad de realizar un Análisis de Gestión de Riesgos.

3.1.3 Determinación del Alcance del Proyecto

Una vez que se ha determinado la necesidad de realizar un Análisis de Gestión de Riesgos, se procede a definir los objetivos que debe cumplir el proyecto, definir su dominio y límites.

El dominio del proyecto se centra en el Departamento Informático de la empresa Transportes y Servicios Asociados SYTSA, ubicada en la ciudad de Quito, su oficina principal.

El personal involucrado actualmente en la realización de este proyecto son:

Ingeniero Pablo Pesantez – Responsable del Área de Sistemas e Informática

Ingeniero Roberto Pesantes – Soporte en Redes y Cableado Estructurado

Ingeniero Freddy Constante – Administrador de la Base de Datos

Ingeniero Freddy Constante – Programador y Desarrollador

Sr. Lauro Sánchez – Responsable del Departamento de Seguridad y Calidad

Sr. Roberto Pesantes – Soporte a Usuarios y otros

Sr. Edgar Toalombo – Monitoreo y Soporte del Sistema de Rastreo

La restricción estipulada por SYTSA es: en el Sistema solo se permite realizar consultas tanto para auditores y personal externo con la respectiva autorización del Departamento Contable.

Con respecto al manejo de la información de cada usuario se puede visualizar todos los recursos compartidos debido a que no existe la debida estructura del manejo de datos en cuanto a las políticas de seguridad que se debe mantener por departamento.

3.1.4 Planificación del Proyecto

Esta etapa se define como la etapa donde se estima los elementos del proyecto es decir las cargas de trabajo, el grupo de usuarios, los participantes, su intervención y el plan de trabajo a realizarse.

Para la recopilación de datos se contó con la ayuda del responsable del Área de Sistemas y del responsable del Área de Calidad y Seguridad, mediante entrevistas y visitas a las oficinas matrices y sucursales.

En base a esto se puede decir que el equipo está constituido de la siguiente forma:

Equipo de Estudio: Director y Subdirector de la Tesis y Egresada de la ESPE.

Grupos de Usuarios: formado por el personal que utiliza los Sistemas de Información.

3.1.5 Lanzamiento del Plan

En esta etapa, seleccionaremos los cuestionarios para la recopilación de datos, especificación de técnicas que se van a emplear para el Análisis y Gestión, asignación de recursos necesarios para la elaboración del proyecto.

Se utilizó como base la Metodología MAGERIT, y lo mencionado en el Catálogo de Elementos sobre los cuestionarios con el fin de identificar correctamente los elementos de trabajo como son los activos, amenazas, vulnerabilidades, salvaguardas, impactos, restricciones generales, etc.

Actualmente en la empresa SYTSA se ha realizado una serie de procedimientos de seguridad para reducir los riesgos en las diferentes áreas incluyendo el área de Sistemas sin embargo no han sido analizados de forma sistémica. No hay eventos que hay ocasionado un daño de relevancia, sin embargo la falta de análisis no ha permitido priorizar los procedimientos adquiridos. Con este proyecto se pretende mejorar las medidas actuales e incluir otras nuevas.

SYTSA dispone de los recursos necesarios para el desarrollo del proyecto, en cuanto a equipo, tiempos, documentación, traslados, etc.

Inicialmente se conversó con el Gerente General El Sr. Arturo Chávez informando sobre el proyecto, objetivos y parámetros, quien autorizó a los responsables del Área de Sistemas y Área de Calidad y Seguridad a que nos brinden el apoyo necesario para la elaboración del proyecto.

Con lo anterior expuesto se procede a la ejecución del Análisis de Gestión en Control y Seguridad para la empresa SYTSA.

3.2 ANÁLISIS DE RIESGO

En esta etapa se procederá a realizar los siguientes procedimientos.

- Identificación de Activos
- Identificación de Amenazas
- Identificación de Salvaguardas
- Identificación de Impactos

Esto se realizará mediante la aplicación de la Metodología MAGERIT, constituye la parte medular del Análisis de Riesgo.

3.2.1 IDENTIFICACIÓN DE ACTIVOS

Los activos corresponden a los recursos en este caso de los Sistemas de Información o que tenga relación que permite que la empresa funcione correctamente. El activo más importante es la información que maneja el sistema, es decir los datos. Partiendo de esto se determina otros activos que forman parte de los Sistemas de Información.[2]

- Servicios, que son los que permiten gestionar los datos.
- Aplicaciones Informáticas: se refiere al software que permite el manejo de los datos.

[2] LOPEZ, Francisco, AMUTO, Miguel, Javier 2006, MAGERIT-versión 2, Metodología de Análisis de Gestión de Riesgos de los Sistemas de Información II-Catálogo de Elementos, Ministerio de Administraciones Públicas, p17

- Equipos Informáticos: el hardware donde se encuentran los datos, aplicaciones y servicios.
- Redes de Comunicaciones: para el intercambio de los datos.
- Soportes de Información: el lugar donde de almacenamiento de los datos.
- Equipamiento Auxiliar: como complemento del material informático.
- Las Instalaciones: donde se ubican los equipos informáticos y comunicaciones.
- El personal: aquellos quienes utilizan los elementos anteriormente descritos.

Identificando los activos se puede valorar y así mismo identificar las amenazas.

A continuación el detalle de los activos clasificados de acuerdo a las entrevistas y encuestas realizadas.

a. [S] Servicios

Estos activos corresponden a los servicios finales prestados por la organización a terceros, servicios donde los usuarios y los medios son propios o servicios contratados.[3]

Los servicios que la empresa presta para los USUARIOS INTERNOS son:

- Portal Web
- Servidor de Correo Electrónico Zimbra

[3] LOPEZ, Francisco, AMUTO, Miguel, Javier 2006, MAGERIT-versión 2, Metodología de Análisis de Gestión de Riesgos de los Sistemas de Información II-Catálogo de Elementos, Ministerio de Administraciones Públicas, p17

- Telefonía IP
- Servicio de copias de respaldo (Backup)

Los servicios que la empresa presta para los USUARIOS EXTERNOS son:

- Transporte de Carga de Mercancía Refrigerada/Seca
- Alquiler de Contenedores
- Servicio de Montaje y Desmontaje

b. [D] Datos/Información

Estos activos constituyen uno de los más importantes dentro de una organización. Entre ellos constan a continuación:

- Información Logística
- Información por cada Departamento
- Información de Registro de Ingresos sobre los Servidores
- Información Personal de cada usuario

c. [SW] Aplicaciones de Software

Corresponde a los programas, aplicaciones, desarrollos, etc. Son tareas que han sido automatizadas para su desarrollo por un equipo informático permitiendo gestionar, analizar y transformar los datos para la prestación de un servicio.[4]

[4] LOPEZ, Francisco, AMUTO, Miguel, Javier 2006, MAGERIT-versión 2, Metodología de Análisis de Gestión de Riesgos de los Sistemas de Información II-Catálogo de Elementos, Ministerio de Administraciones Públicas, p8

Los activos de Software encontrados son:

- Sistema Financiero NIGISU
- Ofimática
- Antivirus
- Otros Software
- Internet

d. [HW] Equipos Informáticos

Estos activos corresponden a los bienes físicos que soportan directa o indirectamente a los servicios que presta la empresa, son depósitos permanentes o temporales de los datos y son soporte de ejecución de las aplicaciones informáticas.[5]

En este grupo según el análisis realizado se encontró lo siguiente.

- Servidor de Datos
- Firewall
- Computadoras de Escritorio
- Computadoras Portátiles
- Scanner
- Impresoras Matriciales

[5] LOPEZ, Francisco, AMUTO, Miguel, Javier 2006, MAGERIT-versión 2, Metodología de Análisis de Gestión de Riesgos de los Sistemas de Información II-Catálogo de Elementos, Ministerio de Administraciones Públicas, p9

- Switch
- Router
- Gateway
- Punto de Acceso Wirelles
- Central Telefónica

e. [COM] Redes de Comunicaciones

Corresponde tanto las instalaciones dedicada como servicios de comunicación contratados a terceros, constituyen medios de transporte de los datos.[6]

A continuación los activos encontrados.

- Red Telefónica
- WIFI
- Red LAN
- Red WAN

f. [SI] Soportes de Información

Este tipo de activos corresponde a los dispositivos físicos que permiten el almacenamiento de la información de forma permanente o por largos períodos de tiempo.[7]

[6] LOPEZ, Francisco, AMUTO, Miguel, Javier 2006, MAGERIT-versión 2, Metodología de Análisis de Gestión de Riesgos de los Sistemas de Información II-Catálogo de Elementos, Ministerio de Administraciones Públicas, p10

Los dispositivos encontrados son:

- Discos
- Disco Externo

g. [AUX] Equipamiento Auxiliar

Son considerados aquellos equipos que sirven de soporte a los sistemas de información si estar directamente relacionados con datos.[8]

La empresa cuenta con los siguientes equipos auxiliares.

- Sistema de Alimentación Ininterrumpida
- Circuito Cerrado de Televisión.
- Sistema de Rastreo

h. [SS] Servicios Subcontratados

La Empresa SYTSA cuenta con servicios Subcontratados para mejor las necesidades de sus clientes.

- Internet PUNTONET
- NIC EC

---

[7] p,10

[8] LOPEZ, Francisco, AMUTO, Miguel, Javier 2006, MAGERIT-versión 2, Metodología de Análisis de Gestión de Riesgos de los Sistemas de Información II-Catálogo de Elementos, Ministerio de Administraciones Públicas, p10

- Telefonía Móvil

i. [L] Instalaciones

Corresponde a los lugares donde se hospedan los sistemas de información y comunicaciones.

La infraestructura de los Sistemas de Información y comunicación se localiza en las oficinas centrales, Quito, Carcelén Diego Vásquez N77-670, en un cuarto compartido actualmente con el Departamento de Calidad y Seguridad.

j. [P] Personal

Corresponde a las personas relacionadas con los sistemas de información.[9]

En este grupo se encuentran:

- Ingeniero Pablo Pesantez – Responsable del Área de Sistemas e Informática
- Ingeniero Roberto Pesantes – Soporte en Redes y Cableado Estructurado y Soporte a Usuarios y otros.
- Ingeniero Freddy Constante – Administrador de la Base de Datos

  Programador y Desarrollador
- Sr. Lauro Sánchez – Responsable del Departamento de Seguridad y Calidad

[9] [9] LOPEZ, Francisco, AMUTO, Miguel, Javier 2006, MAGERIT-versión 2, Metodología de Análisis de Gestión de Riesgos de los Sistemas de Información II-Catálogo de Elementos, Ministerio de Administraciones Públicas, p11

- Sr. Edgar Toalombo – Monitoreo y Soporte del Sistema de Rastreo

El detalle de cada activo se puede observar en el Modelo de Valor ANEXO III.

3.2.2 DEPENDENCIA DE ACTIVOS

Después de identificado los activos se procede a valorar el grado de dependencia que tiene uno con otros. Con esto se puede determinar que la dependencia de un activo con otro puede provocar que los riesgos que posee un activo sean mucho más de lo que inicialmente se había determinado. Es decir se realiza la dependencia de activos para conocer la medida en que un activo de orden superior se puede ver perjudicado por una amenaza materializada sobre un activo de orden inferior.

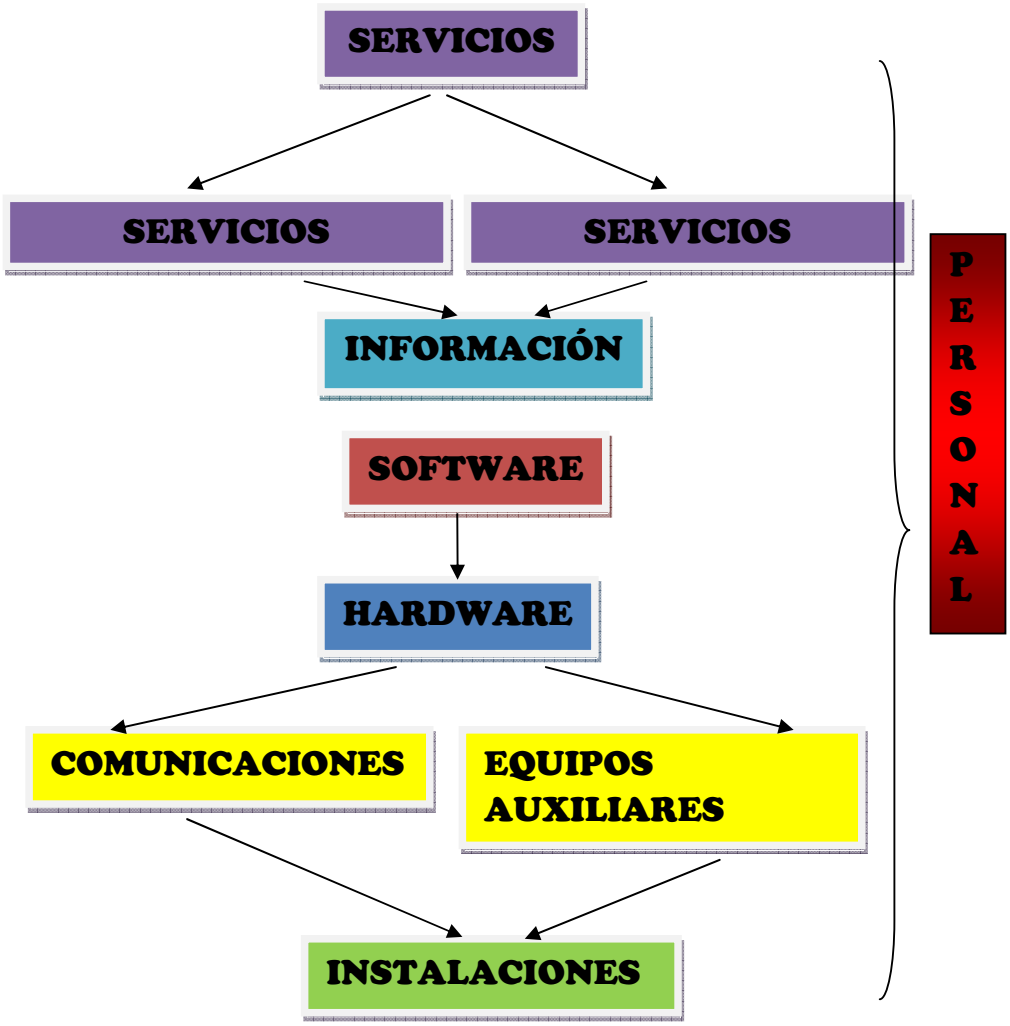


Figura 4 Dependencia de Activos en forma general

El gráfico anterior muestra a manera general la dependencia entre activos. Los servicios dados por el sistema de información se puede notar que dependen de forma directa de los Datos/Información y de forma indirecta del restante de activos.

Se han realizado entrevistas a fin de obtener las dependencias de activos detalladas, que a continuación se pone a consideración.

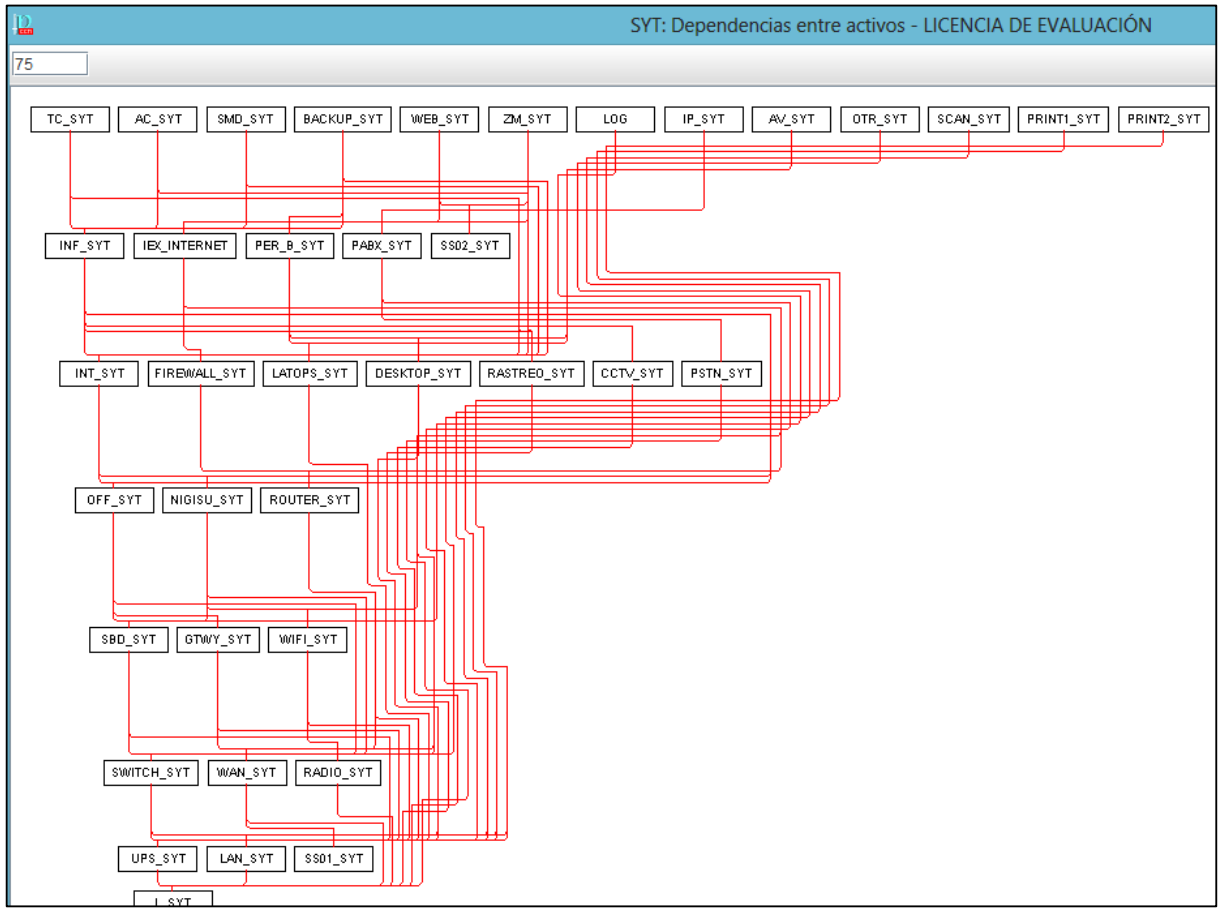


Figura 5 Dependencia de Activos detallada

3.2.3 VALORACIÓN DE ACTIVOS

En esta etapa lo que se realiza es en que dimensión es valioso cada activo descrito anteriormente, tomado en cuenta lo que supondría el coste para la empresa en caso de existiere la destrucción del activo. Obteniendo de esta manera el Modelo de Valor con lo que se conocerá la importancia de un activo, sus dependencias, sus dimensiones y la estimación de su valor en cada dimensión.

El criterio bajo el cual se realizó esta valoración es de valoración cualitativa. Se realiza mediante la ayuda de una escala, donde se busca que los activos del análisis sean homogéneos y comparables.

Cada activo en cada dimensión recibe un valor en la escala. Las dimensiones a valorarse son: Disponibilidad, Integridad y Confidencialidad.

La escala de valor que se va a emplear es la siguiente:

Tabla 1 Escala de Valor de Activos

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

El MODELO DE VALOR para los activos de la Empresa SYTSA se encuentro en el ANEXO III, donde se detalla todos los aspectos referentes a los activos. A continuación se presenta la tabla de Valoración de cada activo:

Tabla 2

Cuadro de Valoración de cada Activo

ACTIVO	D	I	C
[S] SERVICIOS			
[TC] TRANSPORTE DE MERCADERÍA REFRIGERADA	[9]		
[AC] ALQUILER DE CONTENEDORES	[6]		
[SMD] SERVICIO DE MONTAJE Y DESMONTAJE	[4]		
[WEB] PORTAL WEB	[1]		
[ZM] SERVIDOR DE CORREO ELECTRÓNICO ZIMBRA	[10]	[10]	
[IP] TELEFONÍA IP	[7]	[7]	[7]
[BACKUP] SERVICIO DE COPIAS DE RESPALDO	[3]	[3]	[3]
[I] INFORMACIÓN			
[COM] INFORMACIÓN DE LOGÍSTICA	[10]	[10]	[10]
[INT] INFORMACIÓN POR CADA DEPARTAMENTO	[7]	[7]	[7]
[LOG] INFORMACIÓN DE REGISTROS DE ING/SAL	[9]	[9]	[9]
[PER_B] INFORMACIÓN PERSONAL DE USUARIOS			
[SW] APLICACIONES/SOFTWARE			
[NIGISU] SISTEMA FINANCIERO NIGISU	6	6	6
[OFF] OFIMÁTICA	1		
[AV] ANTIVIRUS			[7]
[OTROS SOFTWARE] OTROS	[1]		
[IEX] INTERNET	2		

Continúa

ACTIVO	D	I	C
[HW] EQUIPOS			
[SBD] SERVIDOR DE DATOS	10	10	
[FIREWALL] FIREWALL	10		
[DESKTOP] COMPUTADORAS DE ESCRITORIO	3		10
[LAPTOPS] COMPUTADORAS PORTÁTILES	3		
[SCANNER] SCANNER			
[PRINT1] IMPRESORAS MATRICIALES	[1]		
[PRINT2] IMPRESORA LASER	[1]		
[SWITCH] SWITCH	10		
[ROUTER] ROUTER	1		
[GTWY] GATEWAY	1		
[WIFI] PUNTO DE ACCESO WIRELESS	1		
[PABX] CENTRAL TELEFÓNICA	7		
[C] COMUNICACIONES			
[PSTN] RED TELEFÓNICA	7		
[RADIO] RED INHALÁMBRICA	1		
[LAN] RED LAN	10		
[WAN] RED WAN	2		
[SI] SOPORTES DE INFORMACIÓN			
[DISK] DISCOS	[3]		
[USB] DISPOSITIVO USB	[3]		
[AUX] ELEMENTOS AUXILIARES			
[UPS] SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA	[4]		
[CCTV] CIRCUITO CERRADO DE TELEVISIÓN	[4]		
[SIST_RASTREO] SISTEMA DE RASTREO	[4]		

Continúa

ACTIVO	D	I	C
[SS] SERVICIO SUBCONTRATADOS			
[SS01] PUNTO NET	2		
[SS02] NIC EC	10		
[SS03]TELEFONÍA MÓVIL	9		
[L] INSTALACIONES			
[L] UNIDAD DE SISTEMA DE REDES Y COMUNICACIONES	10		
[P] PERSONAL			
[GER] RESPONSABLE DEL ÁREA DE SISTEMAS	[7]		[10]
[UI] SOPORTE DE USUARIOS	[2]		
[ITL] INFRAESTRUCTURA Y TELECOMUNICACIONES	[2]		
[DBA] ADMINISTRADOR DE LA BASE DE DATOS	[2]		
[SEG] SEGURIDAD Y CALIDAD	[1]		
[RASTREO] MONITOREO Y SOPORTE DE RASTREO	[1]		

En este cuadro se muestra solamente la valoración de los activos de Datos/Información y Servicio y aquellos activos que no dependen de estos.

El detalle del porque se obtienen estos valores para cada activo puede observarse en el Modelo de Valor ANEXO III.

Valoración Acumulada. En el siguiente cuadro se muestra el valor perteneciente a cada activo más el valor de los activos que dependen de él. Los elementos que se encuentran marcados de color celeste corresponden a la valoración acumulada.

Tabla 3

Cuadro de Valoración de cada Activo Acumulado

ACTIVO	D	I	C
[S] SERVICIOS			
[TC] TRANSPORTE DE MERCADERÍA REFRIGERADA	[9]		
[AC] ALQUILER DE CONTENEDORES	[6]		
[SMD] SERVICIO DE MONTAJE Y DESMONTAJE	[6]		
[WEB] PORTAL WEB	[1]		
[ZM] SERVIDOR DE CORREO ELECTRÓNICO ZIMBRA	[10]	[10]	
[IP] TELEFONÍA IP	[7]	[7]	
[BACKUP] SERVICIO DE COPIAS DE RESPALDO	[3]	[3]	[3]
[I] INFORMACIÓN			
[COM] INFORMACIÓN DE LOGÍSTICA	[10]	[10]	[10]
[INT] INFORMACIÓN POR CADA DEPARTAMENTO	[10]	[10]	
[LOG] INFORMACIÓN DE REGISTROS DE ING/SAL	[9]	[9]	[9]
[PER_B] INFORMACIÓN PERSONAL DE USUARIOS	[3]	[3]	[3]
[SW] APLICACIONES/SOFTWARE			
[NIGISU] SISTEMA FINANCIERO NIGISU	[10]	[10]	[10]
[OFF] OFIMÁTICA	[10]	[10]	[10]
[AV] ANTIVIRUS			[7]
[OTROS SOFTWARE] OTROS	[1]		
[IEX] INTERNET	[10]	[10]	

Continúa

ACTIVO	D	I	C
[HW] EQUIPOS			
[SBD] SERVIDOR DE DATOS	[10]	[10]	[10]
[FIREWALL] FIREWALL	[10]	[10]	
[DESKTOP] COMPUTADORAS DE ESCRITORIO	[3]	[3]	[7]
[LAPTOPS] COMPUTADORAS PORTÁTILES	[3]	[3]	[7]
[SCANNER] SCANNER	[0]		
[PRINT1] IMPRESORAS MATRICIALES	[1]		
[PRINT2] IMPRESORA LASER	[1]		
[SWITCH] SWITCH	[10]	[10]	[10]
[ROUTER] ROUTER	[10]	[10]	
[GTWY] GATEWAY	[10]	[10]	[10]
[WIFI] PUNTO DE ACCESO WIRELESS	[10]	[10]	[10]
[PABX] CENTRAL TELEFÓNICA	[7]	[7]	
[C] COMUNICACIONES			
[PSTN] RED TELEFÓNICA	[7]	[7]	
[RADIO] RED INHALÁMBRICA	[10]	{10]	[10]
[LAN] RED LAN	[10]	[10]	[10]
[WAN] RED WAN	[10]	[10]	[10]
[SI] SOPORTES DE INFORMACIÓN			
[DISK] DISCOS			
[USB] DISPOSITIVO USB			
[AUX] ELEMENTOS AUXILIARES			
[UPS] SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA	[10]		
[CCTV] CIRCUITO CERRADO DE TELEVISIÓN	[10]	[10]	[10]
[SIST_RASTREO] SISTEMA DE RASTREO	[10]	[10]	[10]

Continúa

ACTIVO	D	I	C
[SS] SERVICIO SUBCONTRATADOS			
[SS01] PUNTO NET	[10]	[10]	[10]
[SS02] NIC EC	[10]	[10]	
[SS03]TELEFONÍA MOVIL	[9]		
[L] INSTALACIONES			
[L] UNIDAD DE SISTEMA DE REDES Y COMUNICACIONES	[10]	[10]	[10]
[P] PERSONAL			
[GER] RESPONSABLE DEL ÁREA DE SISTEMAS	[7]		[10]
[UI] SOPORTE DE USUARIOS	[2]		
[ITL] INFRAESTRUCTURA Y TELECOMUNICACIONES	[2]		
[DBA] ADMINISTRADOR DE LA BASE DE DATOS	[2]		
[SEG] SEGURIDAD Y CALIDAD	[1]		
[RASTREO] MONITOREO Y SOPORTE DE RASTREO	[1]		

Los elementos marcados son aquellos cuyos valores provienen de sus dependencias con otros activos. Es decir los valores acumulados

3.2.4 IDENTIFICACIÓN DE AMENAZAS

En esta etapa se procede a la identificación de las amenazas que pueden afectar a un activo. Una amenaza es un evento que puede desencadenar un incidente a una organización produciendo como resultado pérdidas tanto materiales como inmateriales.

Las amenazas han sido tomadas en cuenta en base a las encuestas realizadas al personal responsable de los sistemas de información, según el catálogo que se presenta en la Metodología MAGERIT. La frecuencia y degradación de las amenazas se la realizó manualmente y se lo elaboró por capas.

La degradación mide el daño causado por un incidente si este llegará a ocurrir. Estos valores posteriormente se extienden debido a la dependencia entre activos obteniendo el Impacto y el Riesgo tanto acumulado como repercutido. En la siguiente tabla se muestra el esquema bajo el cual se lo ha medido.

Tabla 4

Escala de Degradación

NIVELES	DEGRADACIÓN
25%	POCO
50%	MEDIO
75%	ALTO
100%	MUY ALTO

La frecuencia es como se materializa la amenaza se modela como una tasa anual de ocurrencia, siendo los valores que normalmente se utilizan los siguientes:

Tabla 5

Escala de Frecuencia

PERIODICIDAD	FRECUENCIA
360	A DIARIO
12	MENSUALMENTE
4	CUATRO VECES AL AÑO
2	DOS VECES AL AÑO
1	UNA VEZ AL AÑO
1/12	CADA VARIOS AÑOS

Las amenazas ha sido categorizadas según:

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

En el Anexo 4 MAPA DE RIESGOS se detalla las amenazas existentes para la empresa, en primer lugar se muestra el cuadro de Amenazas existentes por cada Activo de la organización, lo cual resulta la relación Amenaza-Activo de forma directa.

El segundo cuadro muestra los Activos de la empresa por cada Amenaza existente

3.2.5 IDENTIFICACIÓN DE SALVAGUARDAS

Las salvaguardas dentro de un Análisis de Gestión de riesgos juegan el papel de hacer frente a las amenazas. Las salvaguardas pueden actuar desde el punto de vista de: procedimientos, políticas de personal y soluciones técnicas.

Los procedimientos son necesarios tanto para una operación de salvaguardas preventivas como para la gestión de incidencias. Los procedimientos deben cubrir aspectos diversos como son el desarrollo de sistemas, la configuración del equipamiento o la formalización del sistema. Las políticas son necesarias cuando se

consideran sistemas atendidos por el personal. Las soluciones técnicas aplicadas a los activos de aplicación, hardware, comunicaciones y la seguridad física.

Es decir que las salvaguardas pueden ser clasificadas en los siguientes grupos:

- Marco de Gestión
- Relaciones con terceros
- Datos/Información
- Aplicaciones informáticas (SW)
- Equipos Informáticos (HW)
- Comunicaciones
- Elementos auxiliares
- Seguridad Física
- Personal

La eficacia de las salvaguardas se pueden observar en el ANEXO 5 Evaluación de Salvaguardas. A continuación se muestra un cuadro de las Salvaguardas a manera general tomando en cuenta los grupos en los cuales se dividió.

Tabla 6

Resumen de la eficacia de las salvaguardas agrupadas por tipos

SALVAGUARDAS	PRESENTE
Marco de Gestión	20%
Relaciones con terceros	47%
Servicios	41%
Datos/información	28%
Aplicaciones Informáticas (SW)	27%
Equipos Informáticos (HW)	39%
Comunicaciones	34%
Elementos Auxiliares	50%
Seguridad Física	15%
Personal	48%

La forma en que se calculan los porcentajes de eficiencia depende de ciertos criterios que se valoran en forma ponderada. Cada grupo de salvaguardas a la vez está formado por subgrupos. En el cuadro anterior se los ha mostrado a manera general el cuadro detallado se encuentra en el Anexo de Evaluación de salvaguardas.

En la Tabla 7 podemos observar que el aspecto más crítico es el relacionado con la Seguridad física, el lugar donde actualmente se encuentran las instalaciones no es el adecuado puesto que se comparte con el departamento de calidad y seguridad, como resultado de esto no existe un control en el acceso, las condiciones del sitio no cumplen con los parámetros establecidos, no existe normativas de conductas (prohibición fumar, beber, comer, etc.) bien establecidas y que sean cumplidas. No existe procedimientos que permitan realizar inspecciones y aprobaciones periódicas un plan de seguridad, un plan de emergencia, el procedimiento para el acceso del personal no es cumplido en su totalidad, no existe registro del mismo. No existe una

protección frente a desastres a pesar de haber la salvaguarda del Sistema de antincendios.

Tabla 7

Salvaguarda. Seguridad Física

SEGURIDAD FÍSICA	15%	56%
SALVAGUARDA	**HOY**	**SOLUC**
Inventario de instalaciones	40%	80%
Normativa	20%	60%
Procedimientos	10%	50%
Diseño	0%	40%
Control de los accesos físicos	10%	50%
Protección del perímetro	10%	50%
Vigilancia	30%	100%
Iluminación de seguridad	10%	40%
Protección frente a desastres	5%	30%

En la Tabla 8 el segundo parámetro que tiene un grado crítico muy alto es el del Marco de Gestión, existen algunos procedimientos que se ha escrito y difundido, existe un formato de incidentes que debe ser llenado y enviado por la persona responsable sin embargo esto no siempre ocurre bajo el tiempo establecido y de ocurrir se realiza el análisis sin embargo el porcentaje de cumplimiento del plan de acción del incidente no es cubierto o ejecutado en su totalidad.

Existen algunos procedimientos que han sido escritos, que si analizamos más a fondo se puede comprobar que no existe una metodología de actuación formal en la organización en relación a los sistemas de información. No existe un documento de

análisis de riesgo ni un plan de seguridad escrito, ni procedimientos de emergencia en caso de que ocurran este tipo de incidencias.

Tabla 8

Marco de Gestión. Salvaguarda

MARCO DE GESTIÓN	20%	82%
SALVAGUARDA	**HOY**	**SOLUC**
Organización	9%	48%
Normativa de seguridad	21%	75%
Identificación y autenticación	40%	100%
Control de acceso lógico	34%	91%
Gestión de incidencias	10%	80%
Revisión de la seguridad de los sistemas de información	10%	80%
Continuidad del negocio (contingencia)	13%	100%

En la Tabla 9 se observa que existe una falta de documentación que viene arrastrándose por el mismo tema del Marco de Gestión; el almacenamiento de copias de seguridad aún se encuentra implantado en un porcentaje bajo.

No se verifica periódicamente que los equipos estén actualizados porque los equipos se actualizan automáticamente, tomando en cuenta que algunas de estas actualizaciones perjudican para el uso diario de los recursos de la empresa como por ejemplo hay algunas aplicaciones Web que el cliente utiliza con versiones posteriores de navegadores.

Tabla 9

Salvaguarda. Aplicaciones Informáticas.

APLICACIONES INFORMÁTICAS (SW)	27%	78%
SALVAGUARDA	**HOY**	**SOLUC**
Inventario de aplicaciones	10%	80%
Copias de seguridad	40%	100%
Adquisición	20%	60%
Desarrollo	20%	60%
Aplicación de perfiles de seguridad	20%	60%
Explotación	36%	96%
Cambios (actualizaciones y mantenimiento)	40%	90%

Los datos/información activo más importante de la organización tiene un valor similar al de Aplicaciones Informáticas. Respecto al inventario el nivel de criticidad es muy alto no existe una revisión periódica de la información y el usuario responsable.

Respecto a escribir procedimiento para escribir un documento de seguridad, no está realizado en su totalidad, este se debe hacer en base a las medidas de seguridad adoptadas por la Empresa para el tratamiento de archivos, donde debe incluirse recomendaciones, normas y procedimientos. Ver Tabla 10

Tabla 10

Salvaguarda. Datos/Información

DATOS/INFORMACIÓN	28%	88%
SALVAGUARDA	**HOY**	**SOLUC**
Inventario de activos de información	10%	100%
Clasificación de la información	20%	100%
Disponibilidad	40%	50%
Integridad	40%	100%

Actualmente no existe una documentación donde se establezca normas para la salida de la información, es importante generar políticas en pro de mejorar normas claras sobre el uso y privilegio de la información.

Tabla 11

Salvaguarda. Relaciones con Terceros

RELACIONES CON TERCEROS	47%	100%
SALVAGUARDA	**HOY**	**SOLUC**
Seguridad en los accesos de terceras partes	50%	100%
Establecimiento de acuerdos para intercambio de información y software	20%	100%
Inclusión de cláusulas de confidencialidad en los contratos con otras empresas	70%	100%

Un punto muy importante respecto a las Comunicaciones y que se torna crítico es el hecho de solo tener un proveedor de servicio de internet, lo que hace que se dependa

de forma directa de este elemento para garantizar el servicio a través de internet. Ver Tabla 11

Se necesita una reestructuración del cableado, cambios de políticas sobre todo en la parte de la Red Inhalámbrica, Red Lan. Respecto a la Red Wan una reestructuración del Data Center.

Tabla 12

Salvaguardas. Comunicaciones

COMUNICACIONES	34%	64%
SALVAGUARDA	**HOY**	**SOLUC**
Inventario de servicios de comunicación	50%	80%
Adquisición o contratación	35%	80%
Instalación	50%	80%
Aplicación de perfiles de seguridad	10%	10%
Operación	43%	73%
Cambios (actualizaciones y mantenimiento)	18%	60%

Respecto a los Equipos Informáticos, se tiene un inventario de los equipos existentes pero no se realiza con la periodicidad del caso la revisión del mismo. No se ha contemplado el impacto que produciría el cambio de equipos por diferentes modelos en caso de tener que hacerse en forma inmediata. No existen planes de contingencia.

Se debe establecer mejora en las políticas sobre el control de inventarios, procedimientos para el control de entradas y salidas. Ver Tabla 13

También se determina la necesidad de una reestructuración del Data Center.

Tabla 13

Salvaguardas. Equipos Informáticos

EQUIPOS INFORMÁTICOS (HW)	39%	81%
SALVAGUARDA	**HOY**	**SOLUC**
Inventario de equipos	60%	100%
Adquisición de HW	40%	80%
Desarrollo de HW	40%	80%
Instalación	40%	80%
Operación	26%	75%
Cambios (actualizaciones y mantenimiento)	30%	70%

En la Tabla 14, se puede observar que el evento de los Servicios se necesita equipos que tengan mayor capacidad, se necesita un mayor control en los sobre todos los sucesos y diagnósticos diarios, mejorando las políticas de seguridad que se encuentran implantadas hasta el momento.

También se sugiere la reestructuración del Data Center y que existe un mayor control y supervisión a nivel administrativo.

Tabla 14

Salvaguardas. Servicios

SERVICIOS	41%	81%
SALVAGUARDA	**HOY**	**SOLUC**
Inventario de servicios	60%	100%
Disponibilidad	50%	100%
Desarrollo	40%	60%
Despliegue	35%	65%
Aplicación de perfiles de seguridad	20%	80%
Explotación	43%	80%
Gestión de servicios externos	40%	80%

Reestructuración del contrato para la disponibilidad del personal al cien por ciento. Ver Tabla 15

Tabla 15

Salvaguardas. Personal

PERSONAL	48%	92%
SALVAGUARDA	**HOY**	**SOLUC**
Relación de personal	60%	80%
Puestos de trabajo	60%	80%
Formación	40%	100%
Política del puesto de trabajo despejado y bloqueo de pantalla	40%	100%
Evaluación y revisión del plan de formación	40%	100%

Los elementos auxiliares que se tienen tendrían un mejor funcionamiento y uso si es que se realiza una reestructuración del Data Center como se lo ha mencionado en otras ocasiones. Ver Tabla 16

Existen procedimientos de emergencia que no han sido establecidos totalmente, se debe realizar una revisión y modificación de los mismos

Tabla 16

Salvaguardas. Elementos Auxiliares

ELEMENTOS AUXILIARES	50%	83%
SALVAGUARDA	**HOY**	**SOLUC**
Inventario de equipamiento auxiliar	50%	100%
Disponibilidad	50%	80%
Instalaciones	50%	80%
Suministro eléctrico	50%	80%
Climatización	50%	80%
Protección del cableado	50%	80%
Otros suministros	50%	80%

3.2.6 ESTADO DE RIESGO

a. ESTIMACIÓN DEL IMPACTO

En esta etapa del Análisis se va a determinar el Impacto y el Riesgo potencial/residual al que está sometido el sistema.

El impacto constituye el daño sobre el activo al materializarse alguna amenaza. Esto puede realizar al conocer el valor de cada activo y las amenazas.

Se obtiene dos tipos de impacto: Potencial y Residual.

El Impacto Potencial es aquél al que está expuesto el sistema tomando en cuenta el valor de los activos y la valoración de las amenazas como se mencionó anteriormente, sin las salvaguardas.

El Impacto Residual es aquél que está expuesto al sistema pero tomando en cuenta el valor de los activos y la valoración de las amenazas incluyendo también la eficacia de las salvaguardas que se tienen actualmente.

Hay amenazas que provocan mayor impacto que otras sobre el mismo activo. En las tablas que se presentan a continuación según el mayor impacto que puedan sufrir. Para ver los impactos según amenazas se lo puede visualizar en el Anexo de Impacto/Riesgos. A continuación se lo clasifica por dimensiones entonces se tiene lo siguientes:

a.1 IMPACTO POTENCIAL

IMPACTO MUY ALTO (10-7)

Tabla 17

Impacto Muy Alto por cada Activo

DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD
[INF_SYT] INFORMACIÓN LOGÍSTICA	[INF_SYT] INFORMACIÓN LOGÍSTICA	[INF_SYT] INFORMACIÓN LOGÍSTICA
INT_SYT] INFORMACIÓN X DEPTO	INT_SYT] INFORMACIÓN X DEPTO	INT_SYT] INFORMACIÓN X DEPTO
[LOG_SYT] INFORMACIÓN DE REGISTROS DE INGRESOS SOBRE SERVIDORES	[LOG_SYT] INFORMACIÓN DE REGISTROS DE INGRESOS SOBRE SERVIDORES	[LOG_SYT] INFORMACIÓN DE REGISTROS DE INGRESOS SOBRE SERVIDORES
[TC_SYT] TRANSPORTE DE CARGA		
[ZM_SYT] SERVIDOR DE CORREO ZIMBRA	[ZM_SYT] SERVIDOR DE CORREO ZIMBRA	
[NIGISU_SYT] SISTEMA FINANCIERO CONTABLE	[NIGISU_SYT] SISTEMA FINANCIERO CONTABLE	[NIGISU_SYT] SISTEMA FINANCIERO CONTABLE
[OFF_SYT] OFIMÁTICA	[OFF_SYT] OFIMÁTICA	[OFF_SYT] OFIMÁTICA
[IEX_SYT] INTERNET	[IEX_SYT] INTERNET	
[SBD_SYT] SERVIDOR DE BASE DE DATOS	[SBD_SYT] SERVIDOR DE BASE DE DATOS	[SBD_SYT] SERVIDOR DE BASE DE DATOS

Continúa

DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD
[FIREWALL_SYT] FIREWALL	[FIREWALL_SYT] FIREWALL	
	[PRINT2_SYT] IMPRESORA LASER	[PRINT2_SYT] IMPRESORA LASER
[SWITCH_SYT] SWITCH		
[ROUTER_SYT] ROUTER	[ROUTER_SYT] ROUTER	
[GTWY_SYT] GATEWAY	[GTWY_SYT] GATEWAY	[GTWY_SYT] GATEWAY
[WIFI_SYT] WIFI	[WIFI_SYT] WIFI	[WIFI_SYT] WIFI
[RADIO_SYT] RED INHALÁMBRICA	[RADIO_SYT] RED INHALÁMBRICA	[RADIO_SYT] RED INHALÁMBRICA
[LAN_SYT] RED LAN	[LAN_SYT] RED LAN	[LAN_SYT] RED LAN
[WAN_SYT] RED WAN	[WAN_SYT] RED WAN	[WAN_SYT] RED WAN
[UPS_SYT] SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA		[L_SYT] UNIDAD DE SISTEMA DE REDES Y COMUNICACIONES
[CCTV_SYT] CIRCUITO CERRADO DE TELEVISIÓN		
[RASTREO_SYT] SISTEMA DE RASTREO		
[L_SYT] UNIDAD DE SISTEMA DE REDES Y COMUNICACIONES		
[GER_SYT] RESPONSABLE EL ÁREA DE SISTEMAS		

IMPACTO ALTO (7-5)

Tabla 18

Impacto por cada Activo

DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD
[AC_SYT] ALQUILER DE CONTENEDORES	[PABX_SYT] CENTRAL TELEFÓNICA	[AV_SYT] ANTIVIRUS
[SMD_SYT] SERVICIO DE MONTAJE Y DESMONTAJE	[PSTN_SYT] RED TELEFÓNICA	[DESKTOP_SYT] COMPUTADORAS DE ESCRITORIO
[IP_SYT] TELEFONÍA IP	[L_SYT] UNIDAD DE SISTEMA DE REDES Y COMUNICACIONES	[LAPTOPS_SYT] COMPUTADORAS PORTÁTILES
[PABX_SYT] CENTRAL TELEFÓNICA		
[PSTN_SYT] RED TELEFÓNICA		

IMPACTO MEDIO O BAJO (4-3) MEDIO, (2-1) BAJO

Tabla 19

Impacto medio o bajo por cada Activo

DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD
[PER_B_SYT] INFORMACIÓN DE CADA USUARIO	[PER_B_SYT] INFORMACIÓN DE CADA USUARIO	[PER_B_SYT] INFORMACIÓN DE CADA USUARIO
[BACKUP_SYT] SERVICIO DE COPIAS DE RESPALDO	[BACKUP_SYT] SERVICIO DE COPIAS DE RESPALDO	[BACKUP_SYT] SERVICIO DE COPIAS DE RESPALDO

Continúa

DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD
[OTR_SYT] OTROS SOFTWARE	[DESKTOP_SYT] COMPUTADORAS DE ESCRITORIO	
[DESKTOP_SYT] COMPUTADORAS DE ESCRITORIO	[LAPTOPS_SYT] COMPUTADORAS PORTÁTILES	
[LAPTOPS_SYT] COMPUTADORAS PORTÁTILES	[CCTV_SYT] CIRCUITO CERRADO DE TELEVISIÓN	
[PRINT1_SYT] IMPRESORA MATRICIAL	[RASTREO_SYT] SISTEMA DE RASTREO	
[PRINT2_SYT] IMPRESORA LASER		

a.2 IMPACTO RESIDUAL

Tabla 20

IMPACTO RESIDUAL

DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD
[INF_SYT] INFORMACIÓN LOGÍSTICA [10]	[INF_SYT] INFORMACIÓN LOGÍSTICA [10]	[INF_SYT] INFORMACIÓN LOGÍSTICA [10]
INT_SYT] INFORMACIÓN X DEPTO [7]	INT_SYT] INFORMACIÓN X DEPTO [7]	

Continúa

DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD
[LOG_SYT] INFORMACIÓN DE REGISTROS DE INGRESOS SOBRE SERVIDORES [9]	[LOG_SYT] INFORMACIÓN DE REGISTROS DE INGRESOS SOBRE SERVIDORES [9]	[LOG_SYT] INFORMACIÓN DE REGISTROS DE INGRESOS SOBRE SERVIDORES [9]
[TC_SYT] TRANSPORTE DE CARGA [9]	[ZM_SYT] SERVIDOR DE CORREO ZIMBRA [10]	[BACKUP_SYT] SERVICIO DE COPIAS DE RESPALDO [3]
[AC_SYT] ALQUILER DE CONTENEDORES [6[	[IP_SYT] TELEFONÍA IPA [6]	[NIGISU_SYT] SISTEMA FINANCIERO CONTABLE NIGISU [6]
[SMD_SYT] SERVICIO DE MONTAJE Y DESMONTAJE [6]	[BACKUP_SYT] SERVICIO DE COPIAS DE RESPALDO [3]	[AV_SYT] ANTIVIRUS [7]
[WEB_SYT] PORTAL WEB [1] [ZM_SYT] SERVIDOR DE CORREO ZIMBRA [10]	[NIGISU_SYT] SISTEMA FINANCIERO CONTABLE NIGISU [6]	[SBD_SYT] SERVIDOR DE BASE DE DATOS [10] [LAPTOP_SYT] COMPUTADORAS PORTÁTILES [2]
[IP_SYT] TELEFONÍA IPA [7]	[SBD_SYT] SERVIDOR DE BASE DE DATOS [10]	
[BACKUP_SYT] SERVICIO DE COPIAS DE RESPALDO [3]		

Continúa

DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD
[PRINT1_SYT] IMPRESORAS MATRICIALES [1]		
[PRINT2_SYT] IMPRESORA LASER [2]		
[UPS_SYT] SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA [4]		
[CCTV_SYT] CIRCUITO CERRADO DE TELEVISIÓN [4]		
[RASTREO_SYT] SISTEMA DE RASTREO [4]		
[GER_SYT] RESPONSABLE EL ÁREA DE SISTEMAS [10]		

Sobre el Impacto Residual se puede analizar que los activos que mayor muestra de criticidad tienen son: la información de Logística, el servidor de correo electrónico, el servidor de datos, el detalle del Impacto Residual se muestra en el Anexo IV de Estado de Riesgo .

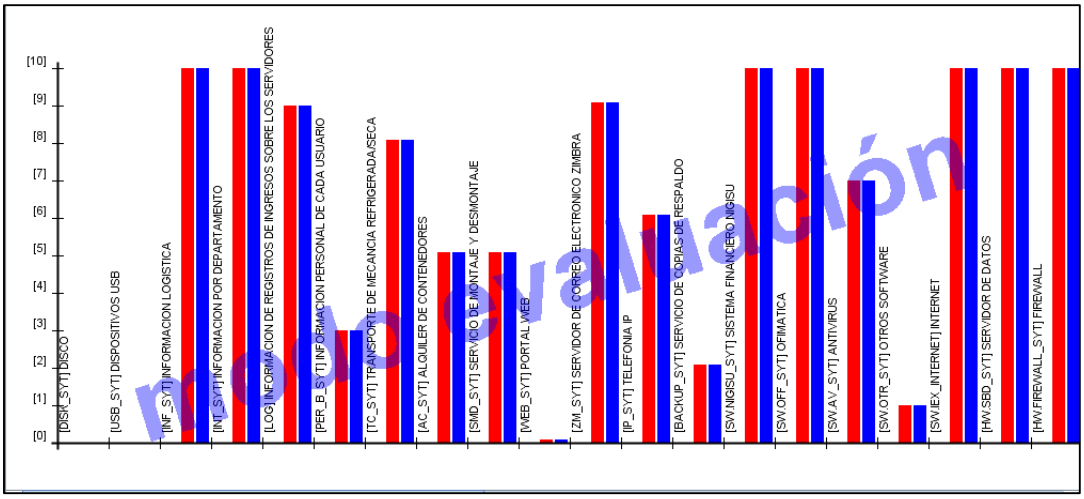


Figura 6. Impacto Potencial

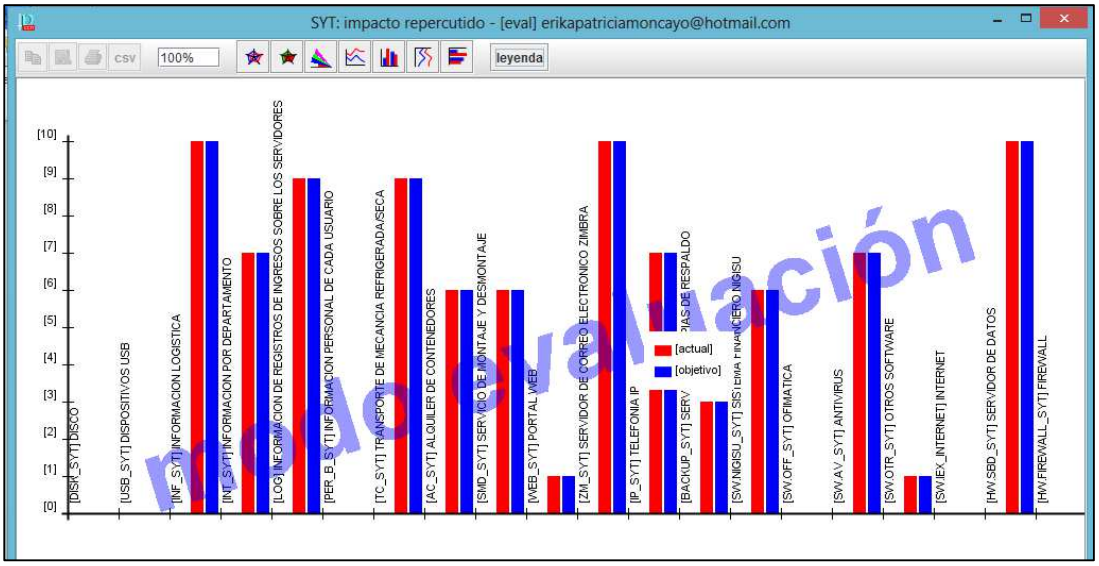


Figura 7. Impacto Potencial

b. ESTIMACIÓN DEL RIESGO

En esta etapa se estima el riesgo al que están sometidos los activos del sistema. Se analiza el riesgo potencial y el riesgo residual.

El riesgo potencial es el riesgo al que está sometido el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas, pero no las salvaguardas desplegadas

b.1 RIESGO POTENCIAL

El riesgo potencial se lo evalúa según la siguiente tabla dada por Pilar

Tabla 21

TABLA PARA MEDICIÓN DEL RIESGO ACUMULADO

7-8-9-10	Extremadamente Crítico
6	Muy Crítico
5	Crítico
4	Muy Alto
3	Alto
2	Medio
1	Bajo
0	Despreciable

Según el análisis realizado y según las amenazas los riesgos en orden de importancia son:

Existe un riesgo Extremadamente crítico sobre las siguientes amenazas

- **[A11] ACCESO NO AUTORIZADO**. Esta amenaza se convierte en crítica por el mismo hecho de que las instalaciones donde actualmente se encuentra es compartida con otro departamento, no hay controles en el acceso del personal.

- **[A.3] MANIPULACIÓN DE LOS REGISTROS DE ACTIVIDAD**.

  Esta amenaza es crítica porque al no tener los registros de actividad o Logs no se puede verificar ni establecer el usuario, la hora de acceso en el cual fueron modificados, dañados o borrados la información de nuestros servidores.

- **[A6] ABUSO DE PRIVILEGIOS DE ACCESO**

  Al no poseer una norma clara sobre el uso de privilegios sobre la información todos los usuarios pueden acceder, manipular o borrar la información sin ningún control alguno.

- **[A19] REVELACIÓN DE LA INFORMACIÓN**

  Al no manejar políticas de seguridad claras cualquier usuario puede hacer uso de la información y divulgar o compartir con cualquier institución o persona.

- **[A15] MODIFICACIÓN DE LA INFORMACIÓN**

  De igual forma la falta de manejo de políticas claras los usuarios pueden alterar información no perteneciente a él.

- **[E24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS**

  Al no contar con los recursos necesarios para que los equipos activos de la empresa trabajen 24/7 365 días se corre el riesgo de no poseer la información en el momento más útil.

- **[A18] DESTRUCCIÓN DE LA INFORMACIÓN**

  Por no contar con las políticas de seguridad adecuadas los usuarios puede eliminar y destruir información perteneciente a la empresa.

- **[A24] DENEGACIÓN DEL SERVICIO**

  Debido al manejo de ancho de banda sobre internet se tiene caídas de servicios básico (correo).

El riesgo en el nivel Muy Crítico está analizado sobre las siguientes amenazas:

- **[A8] DIFUSIÓN DE SOFTWARE DAÑINO**

  La falta de capacitación al personal hace que los usuarios instalen aplicativos sin verificar la procedencia de dicho software.

- **[I6] CORTE DEL SUMINISTRO ELÉCTRICO**

  Debido a la falta de generadores eléctricos en línea y/o bancos de baterías tenemos la caída total de nuestros equipos activos.

- **[I7] CONDICIONES INADECUADAS DE TEMPERATURA Y/O HUMEDAD**

Por falta de un Centro de Datos la empresa corre riesgos de pérdida de información, destrucción y/o mal funcionamiento de los equipos de la empresa.

- **[I2] DAÑOS POR AGUA**

  Por la falta de un Centro de Datos apropiado ha existido en la empresa por varias ocasiones la presencia de inundaciones y daños a la parte física de los equipos.

- **[A7] USO NO PREVISTO**

  Por falta de políticas de seguridad y mal manejo de los usuarios existen utilización de los recursos para fines no previstos de interés personal como son juegos o información perteneciente al usuario. Etc.

- **[E1] ERRORES DE LOS USUARIOS**

  De igual forma la falta de políticas donde se incluya capacitaciones a los usuarios para manejo de la información hace de esta amenaza una amenaza persistente.

Riesgo, nivel Crítico

- **[N*] DESASTRES NATURALES**

  Por la falta de instalación de un pararrayos en la empresa al existir tormentas eléctricas ha causado daño de equipos físicos dentro de las instalaciones.

- **[E2] ERRORES DEL ADMINISTRADOR**

  La falta de control ha ocasionado pérdida de información y el mal uso de los sistemas.

- **[E19] FUGAS DE INFORMACIÓN**

  Como en los casos anteriores la falta de políticas que establezcan normas claras sobre el uso de la información.

- **[E23] ERRORES DE MANTENIMIENTO/ACTUALIZACIÓN DE EQUIPOS (HARDWARE)**

  Falta de control en la actualización de los equipos ha provocado el no desempeño óptimo del manejo dela información.

Riesgo Alto

- **[[A25] ROBO DE EQUIPOS**

  Esta amenaza se genera más sobre los equipos portátiles, el usuario no realiza la respectiva sincronización de datos para que en caso de existir una pérdida no se vea afectada en su totalidad.

- **[I5] AVERÍA DE ORIGEN FÍSICO O LÓGICO**

  La falta de mantenimiento preventivo y correctivo de los equipos ha producido que dichos equipos presenten daños físicos y lógicos causando la mala operación en la empresa.

- **[I8] FALLO DE SERVICIOS DE COMUNICACIONES**

  La falta de un Data Center adecuado se ha producido que por desastres naturales se haya perdido la comunicación en algunas ocasiones.

Riesgo Medio

- **[E2] ERRORES DEL ADMINISTRADOR DEL SISTEMA / DE LA SEGURIDAD**

  En la empresa se ha venido suscitando errores de software por falta de supervisión del administrador

Riesgo Bajo

- **[A26] ATAQUE DESTRUCTIVO**

  Han existido pérdidas de información de carácter personal por el mal manejo del sistema.

Riesgo Despreciable

- **[A6] ABUSO DE PRIVILEGIOS DE ACCESO**

  El uso inadecuado sobre la asignación de claves a producido abuso de recursos como el uso de la Red Wifi.

CAPÍTULO 4

DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD

4.1 DESCRIPCIÓN GENERAL DEL SISTEMA DE GESTIÓN Y CONTROL DE SEGURIDAD.

En esta etapa de estudio se va a determinar el diseño del Sistema de Gestión de Seguridad, con el objetivo de establecer una cultura de la seguridad en la empresa en el área Informática. Se definirá nuevos procedimientos o mejoras en los que actualmente se tiene, con el propósito de proteger la información y los activos de la organización, con efectos de conseguir confidencialidad, integridad y disponibilidad de los datos así como también las responsabilidades que debe asumir cada uno de los integrantes del proceso. La información hoy en día se ha tornado un activo muy importante dentro de las organizaciones por tal razón es de vital importancia su resguardo.

En el capítulo anterior se definió los activos, se determinó las amenazas y se estipuló el impacto y los riesgos a los que los activos pueden verse expuestos, por tal razón son las políticas de seguridad las que intenta minimizar al máximo los riesgos, pero el éxito de la política radica en el compromiso que debe adquirir la gerencia, la difusión y un compromiso serio por parte de los usuarios.

Todas las decisiones y cambios adoptados serán con el afán de mejorar la seguridad en un determinado tiempo para un caso específico de la gestión.

Se tomará en cuenta los escenarios existentes en cuanto a los riesgos e impactos, creando objetivos de control con el fin de brindar respuestas a los escenarios creados.

4.2 OBJETIVOS DE CONTROL

- Alcanzar los objetivos previstos en el diseño del plan**.**
- Establecer tiempos que permiten implementar los controles establecidos.
- Generar la lista de activos a mitigar para proveer a los miembros del equipo claridad sobre los activos a gestionar.
- Ejecutar el plan de seguridad apoyado en el análisis realizado para determinar acciones específicas.

4.3 RESPONSABILIDAD

La responsabilidad es de todo el personal que interviene en el proceso, son responsables de observar y cumplir la Política de Seguridad dentro del área al que pertenezcan y de la misma forma hacer cumplir al personal que está bajo su cargo si el caso lo amerita. Como principales tenemos

- Responsable de Área de Sistemas quien es el encargado de las diferentes tareas relacionadas con la seguridad de los sistemas de información, es el responsable de supervisar todos los aspectos de la política de seguridad.

- Los usuarios, dueños de la información son los responsables de clasificar y relacionar según su nivel de confidencialidad y criticidad, mantener documentada y actualizada la información definiendo que usuarios pueden o no acceder a la misma en función de sus competencias.

- Responsable del Departamento de Seguridad y Calidad, deberá notificar a todos el personal que ingresa la responsabilidad de cumplir con la política de seguridad de la información y de todas las normas administrativas que se apliquen.

- Usuarios de la información y de los sistemas, son responsables de conocer, difundir y fomentar el cumplimiento de la política en toda acción, función o tarea relacionada directa o indirectamente con la información que accede o maneja.

- Auditor, es necesario que luego de la Implementación del Sistema de Gestión de Seguridad y Control se realicen auditorías que permitan asegurar el cumplimiento de lo establecido, en este caso de la presente Tesis, la Certificación BASC una auditoría anual.

4.4 POLÍTICAS DE SEGURIDAD

Las Políticas de Seguridad son normativas o patrones que se deben seguir según las solicitudes en las que la información se ve relacionada. Su objetivo es el de asegurar que la información solamente sea accedida por personal autorizado, el de mantener la confidencialidad de la información y garantizar la integridad de la información durante todo su ciclo de vida. La Política de Seguridad también permite asegurar que todo el personal cuente con capacitación en materia de seguridad de la información, garantizando que todas las vulnerabilidades y debilidades sean reportadas.

Mediante la Política de Seguridad se establece la necesidad de crear procedimientos como soporte a la misma

Según el estándar que ISO/IEC27001 la Política de Seguridad de la información incluye lo siguiente:

- Aspectos organizativos de la Seguridad de la información
- Gestión de Activos
- Seguridad relacionada con los Recursos Humanos
- Seguridad Física y del Entorno
- Gestión de Comunicaciones y Operaciones
- Control de Acceso
- Adquisición, desarrollo y mantenimiento de los sistemas de información.
- Gestión de incidentes de seguridad de la información
- Gestión de la continuidad del negocio.
- Cumplimiento.

El Responsable del Área de Sistemas debe revisar continuamente los lineamientos de la política con la finalidad de mantenerla actualizada o si hay que realizar la respectivas modificación sea por cambios en la infraestructura o por alguna variación en los procedimientos internos, etc.

4.4.1 Aspectos Organizativos de la Seguridad de la Información

En este aspecto la Política de la seguridad de la información debe ir acorde a los objetivos y políticas organizacionales establecidas es por esto que debe haber una persona encargada de gestionar y establecer responsabilidades sobre ciertas tareas como lo son la aprobación de nuevas políticas o modificaciones y los roles dentro de este proceso. Es necesario el apoyo de entidades externas es decir con otras instituciones o empresas, por tanto la información puede verse en riesgo, es importante entonces establecer normativas y procedimientos para su protección.

Política

- Establecer de forma adecuada las funciones y responsabilidades de la gestión de los sistemas de información.

- Descubrir y documentar nuevos riesgos a los que la información se pueda ver sometida incluyendo formas para minimizar estos riesgos. Estar atento a los incidentes de seguridad y documentarlos.

- Promover la cultura de seguridad de la información

- Constancia de compromiso por escrito por parte de la persona que se encuentre a cargo de esta función.

- La persona a cargo será responsable de actualizar, modificar la política según sea la necesidad, deberá realizar la contratación de servicios o adquisiciones de bienes tecnológicos, etc.

- En el caso que sea la necesidad de añadir nuevos elementos al proceso la decisión será tomada en conjunto entre el responsable y el departamento involucrado realizando un análisis e inspección del hardware o software.

- Designar personal calificado externo para realizar auditorías con el objetivo de garantizar de que se esté cumpliendo la política de seguridad y que se esté aplicando en las diferentes labores cotidianas donde la

información se vea involucrada. En este punto es importante que cada solicitud realizada por la entidad externa sea analizada por la persona responsable siguiendo por supuesto las políticas de seguridad. Se debe realizar contratos que especifiquen procedimientos donde se proteja la información, los servicios esperados, obligaciones, controles de acceso.

4.4.2 Gestión de Activos

La empresa debe mantener un alto conocimiento sobre todos los activos sean estos hardware o software, información o datos no procesados para clasificarlos a fin de realizar un riguroso control de riesgos. En el capítulo anterior se identificó y clasificó los activos tales como equipos informáticos, comunicaciones, medios de almacenamiento, equipos de acondicionamiento, etc. Todo esto con el deseo de mantener una protección adecuada de los activos, clasificándolos y estableciendo niveles de protección.

Política

- En cuanto a inventario de activos se refiere se debe identificar los activos según su importancia y la relación con los sistemas de información, este inventario debe estar actualizado sobre todo en casos que se realice modificaciones**.** La revisión periódica no debe ser superior a 6 meses. El inventario debe constar de: Nombre del Equipo, Dirección IP, Mascara de Subred, Nombre del Dominio, Ubicación Física, Modelo del Procesador, Marca y Modelo del Equipo, Número de Procesadores, Velocidad del Procesador, Versión del Sistema Operativo, Service Pack Instalado, Función del Equipo, Memoria RAM, Almacenamiento en Disco, Numero Seriales de Componentes.

- Todos los activos pertenecen a la Empresa Sytsa por tanto la compartición externa queda prohibida salvo en los casos que exista autorizaciones.

- Al existir la correspondencia del activo de la información con la persona que se encuentre a cargo se crea la responsabilidad de No Repudio sobre el uso que se dé a la información.

- Toda modificación, instalación o mantenimiento del equipo debe ser realizado exclusivamente por el personal del departamento de sistemas.

- Se debe seguir lineamientos en cuanto al uso del equipo informáticos es decir: No ingerir alimentos o bebidas, no fumar cerca de equipos, mantener protección contra variaciones de voltajes, no insertar objetos en las ranuras de los equipos, no realizar cambios o mantenimientos sobre el hardware, conservar los equipos bajos adecuadas condiciones ambientales, no dejar los equipos encendidos sino apagarse cuando no estén en uso.

- Sobre los equipos portátiles: deben ser utilizados para el cumplimiento de las actividades relacionadas. Si existiere para uso personal debe ser en lo mínimo y que no obstaculice las actividades laborales.

- De igual forma se debe mantener un inventario de este tipo de equipos donde se debe incluir la misma descripción.

- Los equipos portátiles deben permanecer dentro de la institución, en caso de su salida será de completa responsabilidad del usuario al que se le ha designado el equipo.

- En caso de ser equipos pertenecientes a terceros se debe tomar las siguientes medidas: se debe tener acceso al equipo con el fin de preservar la información, mantener actualizado el software de antivirus, utilizar aplicaciones necesarias.

- Sobre los Sistemas de Información: las herramientas tecnológicas, servicios informáticos, correo electrónico, internet serán utilizados solamente con la autorización del Responsable del Área de Sistemas previa solicitud del Jefe Departamental. La información creada, almacenada o transmitida es de propiedad de la empresa, la divulgación de la información sin autorización está totalmente prohibida. Los software y utilitarios deben tener su respectiva licencia vigente, los mismos que solo podrán ser instalados por personal autorizado. No se podrá reproducir los medios de instalación de las aplicaciones utilizados.

- La empresa es la responsable de asignar una cuenta a cada usuario con sus respectivas seguridades como los son las contraseñas, controles de acceso, monitoreos, etc. Los usuarios deben cumplir todas las normas de uso y cada uno es responsable de sus códigos de acceso.
- Es objeto de sanción el acceder a información o a un buzón de correo que no sea el asignado. El correo electrónico es de propiedad de la empresa por tanto se reserva el derecho de monitorear o auditar; el correo será de uso laboral exclusivamente y no para asuntos personales. En caso de

ausencias personales debe existir la opción de respuesta automáticas informando la ausencia de la persona.

- El Área de Sistemas es el encargado de verificar que el Internet y correo electrónico funcione adecuadamente y tenga las respectivas seguridades instaladas como: firewall, antivirus, etc. Es prohibido el acceso a sitios dudosos y queda prohibidas las descargas de software desde Internet. Por ende debe establecerse restricciones a través de perfiles según sea el caso: Acceso total, Acceso Intermedio, Acceso Restringido.

4.4.3 Seguridad Relacionada con los Recursos Humanos

Es importante tomar en cuenta el papel que juega el recurso humano, es necesario educar y mantener informado al personal desde su ingreso a la empresa sobre las políticas establecidas y las sanciones en caso de incumplimiento. De esta manera se reduce riesgos que provengan por error humano, omisiones o uso no apropiado de los activos de información.

Política

- Es importante establecer compromisos de confidencialidad con todo el personal interno que tengo acceso a la información. En cuanto a proveedores se debe establecer pautas compartidas entre el responsable del área de sistema y el jefe departamental que solicita el servicio.

- Para la selección se debe realizar un análisis e investigación sobre el persona a ser contratado, mediante el uso de pruebas, referencias, record que acrediten no poseer problemas.

- En cuando a la selección de Proveedores debe existir una precalificación para verificar todos los aspectos legales, éticos e historial de comportamiento para que la participación de los mismos no sea causal de amenaza para la seguridad.

- Cuando exista terminación de las relaciones laborales es importante que se lo realice con 15 días de antelación, con el fin de que a quien le corresponda sea el encargado de supervisar la entrega formal del cargo. El responsable del área de sistemas será el que cancele todas las credenciales de acceso a todos los sistemas de información.

- Dentro de este mismo proceso es importante la entrega formal de los activos que incluirá, devolución de software, documentos, equipos, herramientas, medios de almacenamientos, etc.

4.4.4 Seguridad Física y del Entorno

Este aspecto es importa porque trata de reducir en gran medida daños por accesos físicos no adecuados mediante la definición de zonas restringidas y perímetros de seguridad. También es relevante el control de los factores ambientales que permitan garantizar el correcto funcionamiento de los equipos.

Política

- Se debe establecer barreras o medidas de control físico previamente analizado con el fin de no vulnerar la seguridad de los activos. Es decir establecer perímetros o áreas seguras para proteger equipos, red de datos, red eléctrica, sistemas de aire acondicionado, etc.

- En cuanto a la estructura del sitio debe ser de paredes sólidas, las puertas externa protegidas contra accesos no autorizados, protegidos por sistemas de vigilancia, alarmas, sensores de movimientos.

- El área de sistemas deber ser restringida a personal no autorizado y se debe siempre mantener controlado el acceso a la misma.
- Solicitar identificación a las personas que ingresan y confirmar su acceso o no. Se debe llevar un registro o bitácora de visitas donde conste el nombre del visitante, hora de entrada y de salida, persona a la que visita y área a la que accede

- Se recomienda el uso de Identificaciones para todo el personal interno y credenciales para los visitantes.

- Se debe establecer controles que permite proteger la infraestructura contra daño por fuego, inundación o terremoto, explosión o cualquier otra forma de desastre natural. Se debe cumplir con las regulaciones locales solicitadas por el Cuerpo de Bomberos. (Proporcionar equipo contra-incendios ubicado adecuadamente).

- Es importante mantener los materiales peligrosos o combustibles a una distancia considerable del área segura. El equipo de reemplazo debe ser colocado a una distancia segura para evitar el daño de un desastre que afecte el local principal.

- La Sala de Servidores debe estar ubicada estratégicamente, siempre supervisada y vigilada sobre el uso de la misma. Se debe realizar minuciosas evaluaciones sobre las condiciones ambientales para constatar de que no afecten a los equipos repositorios y procesadores de información.

- Los equipos deben estar protegidos y tolerantes a fallas en el suministro eléctrico. Contar con múltiples tomas de energía y acometidas para no tener un punto de falla.

- Contar suministro eléctrico de emergencia (UPS) que permita tener suficiente tiempo para realizar un apagado sistemático de los equipos.

- Analizar la cantidad de equipos a protegerse determinando cuales son los más críticos en función del servicio que cumplan o la información que contenga.

- En cuanto al cableado este debería ser en lo posible subterráneo o contar con la protección como canaletas, tuberías, etc. Evitar desplegar el cableado a través de áreas de acceso público o no controladas. Los puntos

de red deben estar claramente identificados en el patch panel. Mantener documentado las diferentes conexiones para no incurrir en errores de manipulación

- Para los sistemas más sensibles como lo son los servidores se debe utilizar tubos blindados, cajas con llaves para los puntos de inspección de cableado utilizando una ruta de cableado estratégica que brinde seguridad y protección.

4.4.5 Gestión de Comunicaciones y Operaciones

Con esto nos referimos a herramientas como el Internet, correo electrónico o mensajería instantánea ya que constituyen un punto de entrada para los virus, troyanos, software malicioso, convirtiéndose en un punto vulnerable para la entrada de piratas informáticos. El objetivo de establecer políticas en este ámbito es el de garantizar que la información se encuentre siempre disponible, de manera segura estableciendo controles y procedimientos que mitiguen los riesgos.

Política

- Elaborar documentación sobre procesamiento de información, instructivo para manejo de errores comunes y generales, aplicación de procedimientos para reinicio de sistemas o servicios, procedimientos de instalación, cambio o reemplazo de componentes, mantenimiento de equipos, resguardo de información y respaldo, información sobre el personal técnico a contactar en caso de inconvenientes.

- En el caso de los servicios brindados por terceros estos deben ser monitoreados y revisados periódicamente, sometidos a auditorías para

asegurar el fiel cumplimiento según lo acordado. Los puntos a monitorear son: nivel de desempeño del servicio, revisión de reporte de servicios emitidos, recopilación de información sobre incidentes de seguridad de la información, realizar un nuevo análisis de las nuevas necesidades de la empresa.

- Para la protección de software malicioso se debe establecer controles técnicos definiendo una política que prohíba el uso de software no autorizado. Todo software debe ser adquirido por las leyes vigentes. Se llevará un inventario detallado del software instalado y se realizará inspecciones periódicas de forma aleatoria.

- Se debe instalar en todos los equipos software de detección y eliminación de virus y software malicioso. Establecer políticas de revisión y escaneo de los archivos recibidos previo a su uso. Políticas de uso de dispositivos removibles

- Los sistemas operativos deben estar actualizados con los parches de seguridad. Así como también la actualización de las definiciones de virus en todos los equipos.

- Es responsabilidad del usuario el reportar inmediatamente al departamento de sistemas sobre cualquier problema relacionado con la infección de virus o software malicioso.

- En cuanto a respaldo de la información la persona designada se encargará de controlar la realización de las copias periódicas de los datos y de llevar a cabo pruebas periódicas de restauración. Generar procedimientos operativos relacionados con el respaldo de la información.

- Sobre la red de datos, esta debe ser monitoreada incluyendo equipos de comunicación, routers, switches y canales de comunicación, Debe existir controles con el fin de asegurar la confidencialidad de la información trasmitida por rede públicas como internet o redes inalámbricas.

- Los servicios de red deben contar con mecanismos de seguridad como controles de autenticación, control de acceso y de conexión y cifrado.

4.4.6 Control de Acceso

Se refiere a la implementación de controles y procedimientos para garantizar que el control de privilegios y acceso a sistemas sea el adecuado, puede ser desde o hacia redes públicas o el acceso a la información al utilizar equipos portátiles. Estos controles deben mantenerse documentados y actualizados. Es importante concientizar a los usuarios sobre la importancia de la seguridad de acceso.

Política

- Identificar la información ligada a los sistemas de información y que debe ser protegida para que de esta manera exista consistencia entre los niveles de acceso establecidos el nivel de criticidad con el que fue asignado.
- Definir niveles de acceso de usuarios estándar para personal que se ajuste a labores básicas dentro de la institución.

- Los permisos de acceso a los sistemas de información son entregados por el administrador de la base de datos previa a una solicitud y aprobación por escrito del permiso.

- Los permiso de acceso deben seguir procedimientos como: utilizar nombres de usuarios únicos (Asegurarse de que no haya repetidos), chequeo del nivel de acceso sea el estrictamente necesario, firma de un formulario al momento de registrar un usuario donde debe constar en forma detallada todos los privilegios de acceso

- Al momento de asignar una clave esta será de forma temporal y en sobre sellado, establecer los permisos para que el usuario pueda realizar el cambio, existiendo una constancia escrita y firmada de la recepción de la misma.

- De igual forma el personal encargado de administrar los servidores debe suministrar una lista que contenga la clave de todos los servidores según el formato que se establezca. Estas claves no deben ser reveladas a ninguna otra persona.

- En cuanto a los dispositivos móviles considerados tales como: PDA, Teléfonos celulares y sus tarjetas de memoria, Dispositivos de almacenamiento, tarjetas de identificación, dispositivos criptográficos, cámaras digitales, se debe asegurar la protección física del dispositivo, un acceso seguro, utilización de técnicas criptográficas para el momento de

transmitir o almacenar información, reportar al momento cualquier incidente ocurrido con la finalidad de tomar las acciones de inmediato.

- Sobre el tele-trabajo o acceso remoto se debe definir qué tipo de tareas están permitidas realizarse de manera remota, restringir el acceso por horarios, proveer mecanismos de comunicación seguros, encriptación, túneles vpn, incluir lineamientos de seguridad física, efectuar auditorías y monitoreo de la seguridad

4.4.7 Adquisición Desarrollo y mantemiento de los Sistemas de Información

Respecto en este caso al Sistema de información utilizado se debe realizar un análisis y diseño de los procesos que soportan estas aplicaciones, identificar, documentar y aprobar los requerimientos o mecanismos de seguridad que se van a concentrar, diseñando controles de validación de datos de entrada, procesamiento interno y salida de datos.

Es importante tomar en cuenta que al tener conocimiento total de la lógica los programadores y analistas es necesario implementar controles de seguridad para evitar acciones dolosas.

Política

- Establecer normas y procedimientos en la etapa de análisis y diseño del sistema incluyendo los requerimientos, la evaluación de los mismos, cuantificar los riesgos, costos económicos y rendimiento al momento de ser aplicado.

- Validar los datos de entrada regulando a través de procedimientos considerando: control de secuencia, control del monto límite por operación, control del rango de valores, control de paridad, control contra valores cargados, control por oposición, procedimiento para revisión periódica de contenido de campo clave, documento donde existe alternativas a existir errores

- Sobre el procesamiento interno deben existir procedimientos para establecer controles y verificaciones para prevenir la ejecución de programas fuera de secuencia o cuando falle. Procedimientos para la revisión periódica de los registros de auditoría para detectar cualquier anomalía, procedimientos para validar datos generados, procedimiento para verificar y controlar la integridad de los mismos.

- Respecto a las firmas digitales debe brindarse un mecanismo de protección de la autenticidad e integridad de los documentos electrónicos. Las claves deben ser resguardadas bajo el control exclusivo de su titular.
- Para la solicitud de cambios en el sistema debe notificarse por escrito, sobre todo en el caso de que incluya manipulación de los datos debe existir la aprobación del propietario de tal forma se garantiza que no se violen los requerimientos de seguridad que debe cumplir el software.

4.4.8 Gestión de incidentes de seguridad de la información

Trata sobre el establecimiento de procedimientos formales de reporte y de la intensificación de un evento que pueden tener un impacto en la seguridad de los activos organizacionales.

Política

- Existencia de Formato de reportes de eventos de seguridad que puedan ser utilizados como sustento y evidencia de la incidencia con el objeto de justificar las acciones correctivas,

- Detallar cada uno de los eventos como por ejemplo mal funcionamiento, no cumplimiento o violación, conducta extraña, etc. Sin realizar ninguna acción por cuenta propia.

- En el caso de ambientes altamente críticos se puede implementar un sistema de alertas automáticas.

- Es importante capacitar al usuario sobre la obligación de reportar cualquier incidente de inmediato. Entendiéndose por incidente en este caso a cualquier evento que ponga en riesgo la integridad, disponibilidad, confiabilidad y consistencia de la información.

- Clasificar los eventos dependiendo de su tipo como por ejemplo: Fallas del sistema de información, código malicioso, negación del servicio, errores resultantes de datos incompletos, violaciones de la confidencialidad e integridad, uso indebido de los sistemas de información.

- Después de la recepción del incidente se debe analizar e identificar el incidente, existiendo una planeación e implementación de la acción

correctiva para evitar que se genere un nuevo evento, comunicación con los afectados, reportar la acción a la autoridad apropiada, recolectar y asegurar rastros de auditoría.

4.4.9 Gestión de la continuidad del negocio

En este proceso interviene el Plan de Continuidad y Plan de Contingencia como una herramienta básica para garantizar el desenvolvimiento de las actividades de la empresa. Es importante realizar revisiones constantes como parte del proceso de gestión de la seguridad cumpliendo cuidadosamente los controles destinados a identificar riesgos y su posible atenuación, todo esto con el fin de minimizar los efectos de pérdidas temporales o permanentes en la disponibilidad de los sistemas, servicios o información sea por la causa que hubiere ocurrido.

El Plan de Continuidad debe incluir una especificación clara de los procedimientos a ejecutarse a fin de mantener la continuidad del negocio, establecer el nivel aceptable de pérdida de servicio o información., implementar los procedimientos de recuperación y restauración de las operaciones, documentar los procesos y controles, capacitar al personal sobre los procesos y las implicaciones técnicas y no técnicas que esto conlleva y por último un plan de pruebas y mejoramiento continuo de los procesos.

El Plan de Contingencia debe incluir los siguientes aspectos: Notificación/Activación donde el encargado debe siempre estar pendiente de cualquier ocurrencia, Reanudación; para iniciar las operaciones nuevamente de manera total o parcial, Recuperación: lograr el funcionamiento normal y original de los sistemas o servicios informáticos.

Política

- El personal encargado de la parte de sistema será el responsable de identificar amenazas, evaluar riesgos identificados determinando su gravedad, identificar controles, y desarrollar estratégicamente un plan que permita garantizar la continuidad de las actividades.

- Es importante conocer los riesgos, el impacto, identificar los activos de información críticos envueltos, evaluar la posibilidad de asegurar económicamente los activos, garantizar la seguridad e integridad del personal, desarrollar y mantener documentado los planes de contingencia.

4.4.10 Cumplimiento

Es necesario e importante que el cumplimiento de la política de seguridad sea puesta en marcha tanto por los usuarios internos o funcionarios como el personal externo mediante normativas que lo aseguren. Es decir cumplir con todas las disposiciones que se relacionen con la seguridad de la información, para ello se debe revisar continuamente los sistemas de información a fin de garantizar que las políticas de seguridad están siendo cumplidas.

Política

- Revisión continua del cumplimiento del procesamiento de la información dentro de su área de responsabilidad, si existiere una falta, determinar las causas de la misma y tomar las acciones para asegurar que no se repita el evento.

- Realizar pruebas de vulnerabilidad de manera controlada y planificada debidamente documentada emitiendo un informe de novedades presentadas

4.5 CONTROLES

A continuación se gestionan los activos con riesgos críticos, estableciendo controles acorde a las amenazas analizadas.

SERVICIOS

Conociendo las amenazas, salvaguardas existentes y causantes del riesgo, se ha obtenido un riesgo Muy Crítico 7,2 en el ámbito de Disponibilidad e Integridad, al materializarse la amenaza con mayor nivel de riesgo, el atacante podría acceder a los recursos del sistema dejando vulnerable al sistema.

Control:

- Inicialmente se ha sugerido el generar un mayor control sobre todos los sucesos y diagnósticos diarios, realizar una mejora sobre las políticas de seguridad existentes. Acotar todo el espectro de seguridad en lo que hace las plataformas, procedimientos y estrategias. De esta manera se puede controlar todo un conjunto de vulnerabilidades aunque no se logra la seguridad total.

- Reestructuración del Data Center. Es importante que se realice este cambio debido a que el sitio donde actualmente se encuentran los equipos no es el adecuado y es causal de que varias amenazas puedan materializarse, y provocar daños en la organización irreparables. Por

lo que se recomienda realizar una análisis y estudio para la reubicación del centro de datos o la mejora del lugar destinado a esta área

- Control y supervisión por parte del personal encargado, es en realidad necesario tener procedimientos y controles por el departamento de sistemas para manejar los respectivos procesos y análisis de errores ocurridos ya que al momento, se realiza las correcciones sin un análisis, ni bitácoras de cambios.

DATOS/INFORMACIÓN

Se obtuvo un Riesgo muy Crítico de 7,2, que al igual, que el caso anterior al materializarse las amenazas más fuertes provocaría un alto impacto sobre el resguardo de la información de la empresa.

Control

- Cambiar y mejorar las políticas de seguridad adecuadas a los usuarios, estableciendo una norma clara sobre el uso de privilegios (acceso, manipulación, etc.). para que la información y datos de la empresa sea salvaguardados y tengan sus respectivas políticas de acceso.

APLICACIONES (SW)

En este caso también se tiene un riesgo Muy Crítico de 7,2, donde el Sistema Financiero que se utiliza en la empresa es el más afectado tanto en Disponibilidad, Integridad y Confidencialidad. En la mayor parte de los casos se debe a errores

generados por los mismos usuarios, a acceso no autorizados, errores de configuración.

El atacante puede llegar a burlar los sistemas de identificación y autorización, propagar virus, gusanos, etc. Los controles que se sugiere aplicar son:

Controles

- Cambio de políticas sobre el acceso al sistema para que los usuarios tenga los niveles de acceso de acuerdo al área establecida.
- Licenciamiento sobre el software
- Capacitación y manejo de errores internos.
- Reestructuración de políticas de mantenimiento
- En este punto también se considera importante la Reestructuración del Data Center.

EQUIPOS INFORMÁTICOS (HW)

En cuanto a valores presente el mismo riesgo Muy Crítico de 8,6 sobre la Integridad y Confidencialidad que el de Aplicaciones. Las condiciones inadecuadas de temperatura y/o humedad, los daños por agua hacen de los equipos informáticos una amenaza crítica. El hecho de que el afectado sea el Servidor de Datos al materializarse una amenaza provocaría que la información que se genera en los departamentos no ingrese ni salga de manera correcta.

Controles

- Como parte importante se sugiere la Reestructuración del Data Center.

- Control de Acceso y Salida de personal Autorizados.
- Restablecer las políticas de uso adecuado del equipo.
- Control de inventario semestral.
- Restauración de políticas de Uso.
- Mejorar las políticas de Manejo de Claves.

COMUNICACIONES (COM)

Existe un riesgo Muy Crítico de 7,2 sobre la Disponibilidad. Las amenazas más comunes que se presentan sobre este activo son: Avería de origen físico/lógico, cortes del suministro eléctrico, contaminación electromagnética, para lo cual se ha establecido los siguientes controles.

Controles

- Se debe reorganizar el Cableado estructurado, al realizar la reestructuración del Data Center lo cual se deberá unificar marcas, y sus respectivas identificaciones de puntos de acceso para un mayor control, realizar el análisis de carga para la verificación e instalación de las respectivas vlans y switch de acceso para la no saturación de la red

- Es necesario tener un backup de enlace de datos e internet por las respectivas caídas sucedidas.

EQUIPOS AUXILIARES (AUX)

Se presente un Riesgo Crítico sobre la Disponibilidad y la Confidencialidad, presenta cierta similitud en cuanto al anterior activo, las amenazas se concentran en los cortes de suministro eléctrico y averías de origen físico o lógico

Los controles a aplicarse son los siguientes

Controles

- Actualización y por ende cambios de los equipos.
- Mejora en los bancos de batería para un mayo tiempo de respaldo
- Realizar los respectivos PLC para el cambio automático entre los suministros de energía y los generadores eléctricos
- Implementación de procedimientos para la modificación del cableado.
- Capacitación y Manejo de Políticas sobre el uso de los equipos de respaldos al personal.

INSTALACIONES (L)

Respecto a las Instalaciones se muestra un Riesgo Crítico de 6,8 y 6,9 sobre la Disponibilidad y Confidencialidad respectivamente. La amenaza más fuerte se centra sobre el uso no previsto, el acceso no autorizado y daños por agua que al materializarse causaría daños físicos y económicos, impidiendo también el ingreso del personal a las instalaciones para ejercer su trabajo Los controles a aplicarse son:

Controles

- Reestructuración del Data Center, y o construcción de un nuevo centro de datos

- Manejo de políticas de seguridad. Para el acceso, y manejar la integridad de la información.
- Supervisar normas de conducta
- Implementar un plan de protección frente a desastres.
- Implementar un control de acceso, podría ser el de la huella dactilar.

PERSONAL

El Riesgo Crítico presentado en este activo es de 7,2 sobre. La amenaza que se genera aquí es sobre la Indisponibilidad del personal.

Controles

- Manejar tipos de contratos donde exista por lo menos 4 horas diarias personal de sistema de soporte para resolver incidencias leves graves y criticas dicho personal debe estar calificado y respaldado por la empresa contratada para realizar el análisis y la seguridad informática

Antes de la aplicación de los controles es importante tomar muy en cuenta la Variable Costo-Beneficio, con el fin de controlar que el costo de la aplicación de la salvaguarda no supere el costo de la amenaza al materializarse.

En este punto al efectuarse el Diseño del Sistema de Gestión y Seguridad se procede a ordenar en lapsos de tiempos todo lo expuesto anteriormente, considerando el nivel de criticidad, gravedad de los impactos y/o riesgos que se van a atenuar. Esto se puede llevar a cabo en un espacio de tiempo a corto plazo o largo plazo.

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- Conocer la importancia de la seguridad dentro de una empresa en sus aspectos de confidencialidad, integridad y disponibilidad se ha tornado una parte imprescindible para los procesos de negocio. Por ello es relevante en realizar un Análisis y Gestión de Riesgos para un correcto funcionamiento de la organización.

- La elaboración de esta tesis se la realizó también como requisito para aplicar a la Certificación BASC en la empresa, esta certificación es encargada de facilitar y agilizar el Comercio Internacional mediante el establecimiento de estándares y procedimientos globales de seguridad aplicados a la cadena logística del Comercio Internacional, uno de estos procedimientos y estándares es enunciado para la Seguridad de los Sistemas de Información.

- La prevención, detección y mitigación de los riesgos es imprescindible, en este caso se consideró la metodología Magerit la más adecuada debido a que ayuda a descubrir y planificar las medidas oportunas para que se minimicen los riesgos, además permite preparar a la empresa para procesos de evaluación de auditoría.

- Después de realizado el Análisis se llega a la conclusión que los activos con mayor riesgo son los Datos/Información y los Equipos (Hardware), en primera

instancia por el espacio que actualmente ocupan los equipos como Área de Sistemas y segundo por la falta de implementación de normas y políticas como lo constituye el Código de Buenas Prácticas para la Gestión de la Seguridad de la Información.

- Un adecuado uso de las políticas y normas bien documentadas y poniendo como compromiso el de proteger el activo más importante de la empresa, la información, son de gran ayuda para los futuros procesos de auditoría**.** Actualmente la empresa ha empezado a implementar ciertas salvaguardas con el afán de mitigar ciertas amenazas y proteger la información.

- El uso de la Herramienta Pilar fue de gran beneficio para la realización de este proyecto al permitir cotejar la información obtenida de la empresa mediante entrevistas con el área de sistemas para realizar el respectivo análisis.

5.2 RECOMENDACIONES

- Se recomienda realizar análisis de gestión en ciertos períodos de tiempo, utilizando estándares como los que dicta la ISO 27002:2005

- Se recomienda que el presente trabajo sea considerado como una pauta de inicio para realizar todas las mejoras necesarias no solo con el afán de obtener una certificación sino como una política propia de la organización.

- Documentar los procedimientos operativos de cualquier índole detallando para cada área los requerimientos, tareas y procedimientos útiles}

- Se debe definir un comité de recuperación ante contingencias para que se pueda definir de forma clara las funciones y responsabilidades de cada miembro frente a un desastre.

- La seguridad de la información debe ser considerada como un proceso de mejoramiento continuo y no algo estático, en donde los nuevos requerimientos de seguridad se ajusten a los cambios de la empresa.

- Es necesario empezar mejorando la infraestructura del espacio que ocupa el Área de Sistemas debido que actualmente se ha convertido en un punto muy vulnerable para todos los activos mencionados.

ANEXO I

INFORMACIÓN SOBRE LA EMPRESA

Transportes y Servicios Asociados SYTSA, es una empresa ecuatoriana que en 1996 nace como una empresa de servicios de transporte General de mercancías. En el año 2002 sus directivos deciden orientar la empresa para especializar sus servicios en el transporte masivo de perecibles. Para el año 2003 SYTSA cuentas con más de 40 furgones refrigerados constituyendo en la empresa más grande a nivel nacional de transporte refrigerado.

SYTSA hoy cubre todas las rutas nacionales y de la comunidad andina brindando además servicios complementarios como almacenamiento, montajes y desmontajes, alquiler y venta de contenedores.

Cuenta con una Matriz ubicada en Quito, al norte de la ciudad en la Av. Diego de Vásquez N77-670 y sucursales en Tulcán (Panamericana Norte Sector El Rosal), Guayaquil y Huaquillas, un patio en Aloag para alquiler de espacio y de contenedores, etc.

Figura 8 Logo de SYTSA

Los servicios que la empresa brinda son:

a. Transporte de Carga

- SYTSA se encarga del Transporte de carga de productores perecibles, productos refrigerados o secos, utilizando tecnología de punta y personal constantemente capacitado

- Transporte y manejo de contenedores desde los puertos hacia otras ciudades
- Transporte de productos peligrosos
- Transporte de productos líquidos
- Transporte de maquinaria extra dimensionada.

Figura 9 Parte de la Flota de SYTSA

b. Almacenaje

- Ubicado en la ciudad de Tulcán. Bodegaje en la modalidad de Almacén Temporal, depósitos aduaneros y comerciales

- Servicios de Trámites Aduaneros

Figura 10. Área de Almacenaje

c. Montaje y Desmontaje

d.

- Cargue y descargue con personal, montacargas, grúa o elevador lateral

Figura 11. Ilustración de una Grúa

Figura 12 Ilustración del Hammar

SYTSA cuenta con permisos de funcionamiento

- Permiso de Operación 064-DT-CI-2004-CNNT
- Permiso de Idoneidad CI-EC-0055-02
- Permiso de Prestación de Servicios Internacionales 012-CPO-017-2001-CNNT
- Permiso de Prestación de Servicios Aduaneros CAE 8309
- Código Aduanero para la emisión de CPI y tránsitos aduaneros CAE 6293

SYTSA cuenta con:

- 2 grúas de 110 toneladas
- 2 grúas de 35 toneladas
- 1 grúa de 20 toneladas
- 37 cabezales (23 propios y el resto afiliados)

- 18 Plataformas cama alta y 14 de varias capacidades
- 35 furgones refrigerados de entre 40 y 48 pies capacidad de carga hasta 30 toneladas
- 30 contenedores de 20 pies y 40 pies secos y refrigerados con capacidad de congelamiento de hasta 30 grados centígrados bajo cero.
- 2 elevador lateral Hidráulico (Hammar)
- 5 montacargas

ANEXO II

FICHAS PARA LA RECOLECCIÓN DE DATOS

Tabla 22

FICHA PARA LA RECOPILACIÓN DE ACTIVOS DATOS

FICHAS PARA LA RECOPILACIÓN DE DATOS		
[S] SERVICIOS		
NOMBRE :		
DESCRIPCIÓN :		
RESPONSABLE :		
TIPO	**MARQUE LAS OPCIONES QUE PERTENEZCAN**	**CARASTERÍSTICAS**
( )	[ANOM] ANÓNIMO (SIN REQUERIR IDENTIFICACIÓN DEL USUARIO)	
( )	[PUB] AL PÚBLICO EN GENERAL (SIN RELACIÓN CONTRACTUAL)	
( )	[EXT] A USUARIOS EXTERNOS (BAJO UNA RELACIÓN CONTRACTUAL)	
( )	[INT] INTERNO (USUARIOS Y MEDIOS DE LA PROPIA ORGANIZACIÓN)	
( )	[CONT] CONTRATADO A TERCEROS (SE PRESTA CON MEDIOS AJENOS)	
( )	[WWW] WORLD WIDE WEB	
( )	[TELNET] ACCESO REMOTO A CUENTA LOCAL	
( )	[EMAIL] CORREO ELECTRÓNICO	
( )	[VOIP] VOZ SOBRE IP	
( )	[FILE] ALMACENAMIENTO DE FICHEROS	
( )	[PRINT] SERVICIO DE IMPRESIÓN	
( )	[FTP] TRANSFERENCIA DE FICHEROS	
( )	[BACKUP] SERVICIO DE COPIAS DE RESPALDO (BACKUP)	
( )	[EDI] INTERCAMBIO ELECTRÓNICO DE DATOS	
( )	[DIR] SERVICIO DE DIRECTORIO	
( )	[DNS] SERVIDOR DE NOMBRES DE DOMINIO	
( )	[IDM] GESTIÓN DE IDENTIDADES	
( )	[IPM] GESTIÓN DE PRIVILEGIOS	
( )	[CRYPTO] SERVICIOS CRIPTOGRÁFICOS	
	( ) [KEY_GEN] GENERACIÓN DE CLAVES	
	( ) [INTEGRITY] PROTECCIÓN DE LA INTEGRIDAD	
	( ) [ENCRYPTION] CIFRADO	
	( ) [AUTH] AUTENTICACIÓN	
	( ) [SIGN] FIRMA ELECTRÓNICA	
	( ) [TIME] FECHADO ELECTRÓNICO	
( )	[PKI] PKI- INFRAESTRUCTURA DE CLAVE PÚBLICA	

Tabla 23

FICHA PARA LA RECOPILACIÓN DE ACTIVOS INFORMACIÓN

FICHAS PARA LA RECOPILACIÓN DE DATOS		
[D] DATOS/INFORMACIÓN		
NOMBRE :		
DESCRIPCIÓN : RESPONSABLES		
RESPONSABLE :		
TIPO	**MARQUE LAS OPCIONES QUE PERTENEZCAN**	**CARASTERÍSTICAS**
( )	[VR] DATOS VITALES (VITAL RECORDS)	
( )	[COM] DATOS DE INTERÉS COMERCIAL	
( )	[ADM] DATOS DE INTERÉS PARA LA ADMINISTRACIÓN PÚBLICA	
( )	[INT] DATOS DE GESTIÓN INTERNA	
( )	[SOURCE] CÓDIGO FUENTE	
( )	[EXE] CÓDIGO EJECUTABLE	
( )	[CONF] DATOS Y CONFIGURACIÓN	
( )	[LOG] REGISTO DE ACTIVDAD (log)	
( )	[TEST] DATOS DE PRUEBA	
( )	[PER] DATOS DE CARÁCTER PERSONAL	
( )	( ) [A] DE NIVEL ALTO	
	( ) [M] DE NIVEL MEDIO	
	( ) [B] DE NIVEL BÁSICO	
	[LABEL] DATOS CLASIFICADOS	
	( ) [S] SECRETO	
	( ) [R] RESERVADO	
	( ) [C] CONFIDENCIAL	
	( ) [DL] DIFUSIÓN LIMITADA	
	( ) [SC] SIN CLASIFICAR	

Tabla 24

FICHA PARA LA RECOPILACIÓN DE ACTIVOS SOFTWARE

FICHAS PARA LA RECOPILACIÓN DE DATOS		
[SW] APLICACIONES DE SOFTWARE		
NOMBRE :		
DESCRIPCIÓN :		
RESPONSABLE :		
TIPO	**MARQUE LAS OPCIONES QUE PERTENEZCAN**	**CARASTERÍSTICAS**
( )	[PRP] DESARROLLO PROPIO (IN HOUSE)	
( )	[SUB] DESARROLLO A MEDIDA (SUBCONTRATADO)	
( )	[STD] ESTANDAR (OFF THE SHELF)	
( )	( ) [BROWSER] NAVEGADOR WEB	
( )	( ) [WWW] SERVIDOR DE PRESENTACIÓN	
( )	( ) [APP] SERVIDOR DE APLICACIONES	
( )	( ) [EMAIL_CLIENT] CLIENTE DE CORREO ELECTRÓNICO	
( )	( ) [EMAIL_SERVER] SERVIDOR DE CORREO ELECTRÓNICO	
( )	( ) [DIRECTORY] SERVIDOR DE DIRECTORIO	
( )	( ) [FILE] SERVIDOR DE FICHEROS	
( )	( ) [DBMS] SISTEMA DE GESTIÓN DE BASE DE DATOS	
( )	( ) [TM] MONITOR TRANSACCIONAL	
( )	( ) [OFFICE] OFIMÁTICA	
( )	( ) [AV] ANTI VIRUS	
( )	( ) [OS] SISTEMA OPERATIVO	
	( ) [WINDOWS] WINDOWS	
	( ) [SOLARIS] SOLARIS	
	( ) [LINUX] LINUX	
	( ) [OTHERS] OTROS	
( )	( ) [TS] SERVIDOR DE TERMINALES	
( )	( ) [BACKUP] SISTEMA DE BACKUP	
( )	( ) [OTHERS] OTROS	

Tabla 25

FICHA PARA LA RECOPILACIÓN DE ACTIVOS EQUIPOS INFORMÁTICOS

FICHAS PARA LA RECOPILACIÓN DE DATOS		
[HW] EQUIPOS INFORMÁTICOS		
NOMBRE :		
DESCRIPCIÓN :		
RESPONSABLE :		
TIPO	**MARQUE LAS OPCIONES QUE PERTENEZCAN**	**CARASTERÍSTICAS**
( )	[HOST] GRANDES EQUIPOS (HOST)	
( )	[MID] EQUIPOS MEDIOS	
( )	[PC] INFORMÁTICA PERSONAL	
( )	[VHOST] EQUIPOS VIRTUALES	
( )	[CLUSTER] CLUSTER	
( )	[MOBILE] INFORMÁTICA MOVIL	
( )	[PDA] AGENDAS ELECTRÓNICAS	
( )	[EASY] FACILMENTE REEMPLAZABLES	
( )	[DATA] QUE ALMACENAN DATOS	
( )	[PERIPHERAL] PERIFÉRICOS	
	( ) [PRINT] MEDIOS DE IMPRESIÓN	
	( ) [SCAN] SCANNER	
	( ) [CRYPTO] DISPOSITIVO CRIPTOGRÁFICO	
	( ) [OTHERS] OTROS	
( )	[BD] DISPOSITIVO DE FRONTERA	
( )	[NETWORK] SOPORTE DE RED	
	( ) [MODEM] MODEM	
	( ) [HUB] CONCENTRADOR	
	( ) [SWITCH] CONMUTADOR	
	( ) [ROUTER] ENCAMINADOR	
	( ) [BRIDGE] PUENTE	
	( ) [GTWY] PASARELA	
	( ) [FIREWALL] CORTAFUEGOS	
	( ) [WAP] PUNTO DE ACCESO WIRELESS	
	( ) [OTHERS] OTROS	
( )	[PABX] CENTRAL TELEFÓNICA	

Tabla 26

FICHA PARA LA RECOPILACIÓN DE ACTIVOS COMUNICACIONES

FICHAS PARA LA RECOPILACIÓN DE DATOS		
[COM] COMUNICACIONES		
NOMBRE :		
DESCRIPCIÓN : MARCA CANTIDAD Y MODELO :		
RESPONSABLE :		
TIPO	**MARQUE LAS OPCIONES QUE PERTENEZCAN**	**CARASTERÍSTICAS**
( )	[PSTN] RED TELEFÓNICA	
( )	[ISDN] RSDI RED DIGITAL	
( )	[X25] X25 RED DE DATOS	
( )	[ADSL] ADSL	
( )	[PP] PUNTO A PUNTO	
( )	[RADIO] RED INHALÁMBRICA	
( )	[WIFI] WIFI	
( )	[MOBILE] TELEFONÍA MOVIL	
( )	[SAT] SATELITE	
( )	[LAN] RED LOCAL	
( )	[VLAN] LAN VIRTUAL	
( )	[MAN] RED METROPOLITANA	
( )	[WAN] RED DE ÁREA AMPLIA	
( )	[INTERNET] INTERNET	
( )	[VPN] RED PRIVADA VIRTUAL	
( )	[OTHERS] OTROS	

Tabla 27

FICHA PARA LA RECOPILACIÓN DE ACTIVOS SOPORTES DE INFORMACIÓN

FICHAS PARA LA RECOPILACIÓN DE DATOS		
[SI] SOPORTES DE INFORMACIÓN		
NOMBRE :		
DESCRIPCIÓN : MARCA, CAPACIDAD, CANTIDAD		
RESPONSABLE :		
TIPO	**MARQUE LAS OPCIONES QUE PERTENEZCAN**	**CARASTERÍSTICAS**
( )	[ELECTRONICS] (ELECTRÓNICOS)	
	( ) [DISK] DISCOS	
	( ) [VDISK] DISCOS VIRTUALES	
	( ) [SAN] ALMACENAMIENTO EN RED	
	( ) [DISQUETTE] DISQUETTES	
	( ) [CD] CD-ROM	
	( ) [USB] DISPOSITIVOS USB	
	( ) [DVD] DVD	
	( ) [TAPE] CINTA MAGNÉTICA	
	( ) [MC] TARJETAS DE MEMORIA	
	( ) [IC] TARJETAS INTELIGENTES	
	( ) [OTHERS] OTROS	
( )	[NON_ELECTRONICS] (NO ELECTRÓNICOS)	
	( ) [PRINTED] MATERIAL IMPRESO	
	( ) [TAPE] CINTA DE PAPEL	
	( ) [FILM] MICROFILM	
	( ) [CARDS] TARJETAS PERFORADAS	
	( ) [OTHERS] OTROS	

Tabla 28

FICHA PARA LA RECOPILACIÓN DE EQUIPAMIENTO AUXILIAR

FICHAS PARA LA RECOPILACIÓN DE DATOS		
[AUX] EQUIPAMIENTO AUXILIAR		
NOMBRE :		
DESCRIPCIÓN : MARCA TIPO		
RESPONSABLE :		
TIPO	**MARQUE LAS OPCIONES QUE PERTENEZCAN**	**CARASTERÍSTICAS**
( )	[POWER] FUENTES DE ALIMENTACIÓN	
( )	[UPS] SAI-SISTEMAS DE ALIMENTACIÓN ININTERRUMPIDA	
( )	[GEN] GENERADORES ELÉCTRICOS	
( )	[AC] EQUIPOS DE CLIMATIZACIÓN	
( )	[CABLING] CABLEADO	
	( ) [WIRE] CABLEADO ELÉCTRICO	
	( ) [FIBER] FIBRA ÓPTICA	
( )	[ROBOTS] ROBOTS	
	( ) [TAPE] _____ DE CINTAS	
	( ) [DISK] _____ DE DISCOS	
( )	[SUPPLY] SUMINISTROS ESENCIALES	
( )	[DESTROY] EQUIPOS DE DESTRUCCIÓN DE SOPORTES DE INFORMACIÓN	
( )	[FURNITURE] MOBILIARIO, ARMARIO, ETC	
( )	[SAFE] CAJA FUERTES	
( )	[OTHERS] OTROS	

Tabla 29

FICHA PARA LA RECOPILACIÓN DE ACTIVOS SUBCONTRATADOS

FICHAS PARA LA RECOPILACIÓN DE DATOS		
[SS] SERVICIOS SUBCONTRATADOS		
NOMBRE :		
DESCRIPCIÓN : SERVICIO		
RESPONSABLE :		
TIPO	**MARQUE LAS OPCIONES QUE PERTENEZCAN**	**CARASTERÍSTICAS**
( )	[ANON] ANÓNIMO SIN REQUERIR IDENTIFICACIÓN DE USUARIO	
( )	[PUB] AL PÚBLICO EN GENERAL (SIN RELACIÓN CONTRACTUAL	
( )	[EXT] USUARIOS EXTERNOS BAJO UNA RELACIÓN CONTRACTUAL	
( )	[INT] INTERNO (USUARIOS Y MEDIOS DE LA PROPIA ORGANIZACIÓN	
( )	[CONT] CONTRATADO A TERCEROS SE PRESTA CON MEDIOS AJENOS	
( )	[WWW] WORLD WIDE WEB	
( )	[TELNET] ACCESO REMOTO A CUENTA LOCAL	
( )	[EMAIL] CORREO ELECTRÓNICO	
( )	[VOIP] VOZ SOBRE IP	
( )	[FILE] ALMACENAMIENTO DE FICHEROS	
( )	[PRINT] SERVICIO DE IMPRESIÓN	
( )	[FTP] TRANSFERENCIA DE FICHEROS	
( )	[BACKUP] SERVICIO DE COPIAS DE RESPALDO (BACKUP)	
( )	[EDI] INTERCAMBIO ELECTRÓNICO DE DATOS	
( )	[DIR] SERVICIO DE DIRECTORIO	
( )	[DNS] SERVIDOR DE NOMBRES DE DOMINIO	
( )	[IDM] GESTIÓN DE IDENTIDADES	
( )	[IPM] GESTIÓN DE PRIVILEGIOS	
( )	[CRYPTO] SERVICIOS CRIPTOGRÁFICOS	
	( ) [KEY_GEN] GENERACIÓN DE CLAVES	
	( ) [INTEGRITY] PROTECCIÓN DE LA INTEGRIDAD	
	( ) [ENCRYPTION] CIFRADO	
	( ) [AUTH] AUTENTICACIÓN	
	( ) [SIGN] FIRMA ELECTRÓNICA	
	( ) [TIME] FECHADO ELECTRÓNICO	

Tabla 30

FICHA PARA LA RECOPILACIÓN DE ACTIVOS INFRAESTRUCTURA

FICHAS PARA LA RECOPILACIÓN DE DATOS		
[L] INFRAESTRUCTURA		
NOMBRE :		
DESCRIPCIÓN : TIPO, DIRECCION Y TELEFONOS		
RESPONSABLE :		
TIPO	**MARQUE LAS OPCIONES QUE PERTENEZCAN**	**CARASTERÍSTICAS**
( )	[SITE] EMPLAZAMIENTO	
( )	[BUILDING] EDIFICIO	
( )	[LOCAL] LOCAL	
( )	[MOBILE] PLATAFORMAS MOVILES	
	( ) [CAR] VEHÍCULO TERRESTRE: COCHE, CAMIÓN, ETC	
	( ) [PLANE] VEHÍCULO AÉREO: AVIÓN, ETC	
	( ) [SHIP] VEHÍCULO MARITIM: BUQUE, LANCHA, ETC	
	( ) [SHELTER] CONTENEDORES	
	( ) [CHANNEL] CANALIZACIÓN	
	( ) [OTHERS] OTROS	

Tabla 31

FICHA PARA LA RECOPILACIÓN DE ACTIVOS PERSONAL

FICHAS PARA LA RECOPILACIÓN DE DATOS		
[P] PERSONAL		
NOMBRE :		
DESCRIPCIÓN : RESPONSABLES		
RESPONSABLE :		
TIPO	**MARQUE LAS OPCIONES QUE PERTENEZCAN**	**CARASTERÍSTICAS**
( )	[UE] USUARIOS EXTERNOS	
( )	[UI] USUARIOS INTERNOS	
( )	[OP] OPERADORES	
( )	[ADM] ADMINISTRADORES DEL SISTEMA	
( )	[COM] ADMINISTRADORES DE COMUNICACIONES	
( )	[DBA] ADMINISTRADORES DE BASE DE DATOS	
( )	[SEC] ADMINISTRADORES DE SEGURIDAD	
( )	[DES] DESARROLLADORES Y PROGRAMADORES	
( )	[SUB] SUBCONTRTAS	
( )	[PROV] PROVEEDORES	
( )	[OTHERS] OTROS	

ANEXO III

MODELO DE VALOR

NOMBRE PROYECTO: [PROY_SYTSA] DISEÑO DE UN SISTEMA DE GESTIÓN EN CONTROL Y SEGURIDAD.

1. DATOS DEL PROYECTO

PROY_SYTSA	**DISEÑO DE UN SISTEMA DE GESTIÓN EN CONTROL Y SEGURIDAD**
DESCRIPCIÓN	Análisis a los Sistemas de Información
DIRECCIÓN	Carcelén, Diego Vásquez N77-670
TELÉFONO	2473006
RESPONSABLE	Erika Moncayo
EMPRESA	TRANSPORTES Y SERVICIOS ASOCIADOS SYTSA

Descripción:

El proyecto es elaborado en la Empresa Transportes y Servicios Asociados SYTSA, en la oficina Matriz en Quito

2. DIMENSIONES

- [D] Disponibilidad

- [I] Integridad en los Datos
- **[**C] Confidencialidad

3. ÁRBOL DE ACTIVOS

ACTIVOS

3.1 Capa [S] Servicios

Capa_[SE] Servicios Externos

[TC_SYT] Transporte de Carga de Mercancía Refrigerada/Seca

[AC_SYT] Alquiler de Contenedores

[SMD_SYT] Servicio de Montaje y Desmontaje

Capa [SI] Servicios Internos

[WEB_SYT] Portal Web

[ZM_SYT] Servidor de Correo Electrónico ZIMBRA

[IP_SYT] Telefonía IP

[BACKUP_SYT] Servicio de copias de respaldo

3.2 Capa [D] Datos/Información

[INF_SYT] Información de Logística

[INT_SYT] Información por cada Departamento

[**LOG_SYT]** Información de Registros de ingreso sobre los servidores

[PER_M_SYT] Información personal de cada usuario

3.3 Capa [E] Equipamiento

[SW] Aplicaciones

[NIGISU_ SYT]Sistema Financiero NIGISU

[OFF_SYT] Ofimática

[AV_SYT] Antivirus

[OTR_SYT] Otro software

[INT_INTERNET] Internet

[HW] Equipos

[SBD_SYT] Servidor de Datos

[FIREWALL] Firewall

[DESKTOP_SYT] Computadoras de Escritorio

[LAPTOPS_SYT] Computadoras Portátiles

[SCAN_SYT] Scanner

[PRINT1_SYT] Impresoras Matriciales

[PRINT2_SYT] Impresora Laser

[SWITCH_SYT] Switch

[ROUTER_SYT] Router

[GTWY_SYT] Gateway

[WIFI_SYT] Puntos de Acceso Wireless

[PABX_SYTS] Central Telefónica

3.4 [COM] Comunicaciones

[PSTN_SYT] Red Telefónica

[WIFI_SYT] Red Wifi

[LAN_SYT] Red LAN

[WAN_SYT] Red WAN

3.5 [SI] Soportes de Información

[DISK_SYT] Discos

[USB_SYT] Dispositivos USB

3.6 [AUX] Elementos Auxiliares

[UPS_SYT] Sistemas de Alimentación Ininterrumpida

[CCTV_SYT] Circuito Cerrado de Televisión

[RASTREO_SYT] Sistema de Rastreo

3.7 Capa [SS] Servicios Subcontratados

[SS01_SYT] Internet PUNTONET

[SS02_SYT] NIC EC

[SS03_SYT] TELEFONÍA MOBIL

3.8 Capa [L] Instalaciones

[L_SYT] Unidad de Sistema de Redes y Comunicaciones

3.9 Capa [P] Personal

[GER_SYT] Responsable del Área de Sistemas

[UI_SYT] Soporte a Usuarios

[ITL_SYT] Infraestructura y Telecomunicaciones

[DBA_SYT] Administrador de la Base de Datos

[SEG_SYT] Seguridad y Calidad

[RASTREO_SYT]Monitoreo y Sopor te de Rastreo

4. RESUMEN DE VALORACIÓN

En base a las entrevistas realizadas y la información recopilada se ha obtenido los siguientes datos de valoración que a continuación se detalla:

Tabla 32

Detalle y valoración de los Servicios Externos

[SE] SERVICIOS EXTERNOS

ACTIVO	D	I	C
[TC_SYT] TRANSPORTE DE MERCANCÍA REFRIGERADA O SECA	9(1)		
[AC_SYT] ALQUILER DE CONTENEDORES	6(2)		
[SMD] SERVICIO DE MONTAJE Y DESMONTAJE	4(3)		

(1) [9.da] Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones.

(2) [6.pi1] Información personal: probablemente afecte gravemente a un grupo de individuos.

(3) [4. pi1] Información personal: probablemente afecte gravemente a un grupo de individuos.

Tabla 33

Detalle y valoración de los Servicios Internos

[SI] SERVICIOS INTERNOS

ACTIVO	D	I	C
[WEB_SYT] PORTAL WEB	1(1)		
[ZM_SYT] SERVIDOR DE CORREO ELECTRÓNICO ZIMBRA	10(2)	10(3)	
[IP_SYT] TELEFONÍA IP	7(4)	7(5)	
[BACKUP_SYT] SERVICIO DE COPIAS DE RESPALDO	3(6)	3(7)	3(8)

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

[1.lg] Pudiera causar una pérdida menor de la confianza dentro de la Organización

(2) [10.olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística.

(3) [10.olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística.

(4) [7.da] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones.

(5) [7.da] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones.

[7.adm] Administración y gestión probablemente impediría la operación efectiva de la organización.

(6) [3.olm] Probablemente merme la eficacia o seguridad de la misión operativa logística (alcance local).

[3.cei.e] Constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros.

(7) [3.pi1] Información personal: probablemente afecte a un individuo.

(8) [3.pi1] Información personal: probablemente afecte a un individuo.

Tabla 34

Detalle y valoración de los Datos/información

[D] DATOS/INFORMACIÓN

ACTIVO	D	I	C
[INF_SYT] INFORMACIÓN DE LOGÍSTICA	10(1)	10(2)	10(3)
[INT_SYT] INFORMACIÓN POR CADA DEPARTAMENTO	7(4)	7(5)	7(6)
[LOG_SYT] INFORMACIÓN DE REGISTROS DE INGRESOS SOBRELOS SERVIDORES	9(7)	9(8)	9(9)
PERM_B_SYT] INFORMACIÓN PERSONAL DE CADA USUARIO			

(1) [10.olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística.

(2) [10.olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística.

(3) [10.olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística.

(4) [7.adm] Administración y gestión probablemente impediría la operación efectiva de la organización.

(5) [7.adm] Administración y gestión probablemente impediría la operación efectiva de la organización.

(6) [7.adm] Administración y gestión probablemente impediría la operación efectiva de la organización.

(7) [9.lg.a] Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones con otras organizaciones

[9.iic] Probablemente cause serios daños a misiones muy importantes de inteligencia o información.

(8) [9.si] Seguridad: probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios.

(9) [9.lg.a] Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones con otras organizaciones.

Tabla 35

Detalle y valoración de Aplicaciones/Software

[SW] APLICACIONES/SOFTWARE

ACTIVO	D	I	C
[NIGISU_SYT] SISTEMA FINANCIERO NIGISU	6(1)	6(2)	6(3)
[OFF_SYT] OFIMÁTICA	1(4)		
[AV_SYT] ANTIVIRUS			7(5)
[OTR_SYT] OTROS SOFTWARE	1(6)		
[IEX_SYT] INTERNET	2(7)		

(1) [6.pi1] Información personal: probablemente afecte gravemente a un grupo de individuos

(2) [6.pc] Orden público: probablemente cause manifestaciones o presiones significativas.

(3) [6.lbl] Datos clasificados como de difusión limitada.

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

[1.adm] Administración y gestión: pudiera impedir la operación efectiva de una parte de la organización.

[1.pi1] Información personal: pudiera causar molestias a un individuo

[1.lbl] Datos clasificados como sin clasificar.

(5) [7.olm] Probablemente cause o perjudique la eficacia o seguridad de la misión operativa o logística

[7.cei.e] Interese comerciales o económicos constituye un serio incumplimiento de obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros.

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

(7) [2.lg] Probablemente cause una pérdida menor de la confianza dentro de la organización.

Tabla 36

Detalle y valoración de Equipos

[HW] EQUIPOS

ACTIVO	D	I	C
[SBSC_SYT] SERVIDOR DE DATOS	10(1)	10(2)	
[FIREWALL_SYT] FIREWALL	10(3)		
[DESKTOP_SYT] COMPUTADORAS DE ESCRITORIO	3(4)		
[LAPTOPS_SYT] COMPUTADORA PORTÁTILES	3(5)		10(6)
[SCAN_SYT] SCANNER			
[PRINT1_SYT] IMPRESORAS MATRICIALES	1(7)		
[PRINT2_SYT] IMPRESORA LASER	1(8)		
[SWITCH_SYT] SWITCH	10(9)		
[ROUTER_SYT] ROUTER	1(10)		
[GTWY_SYT] GATEWAY	1(11)		
[WIFI_SYT] PUNTOS DE ACCESO WIRELESS	1(12)		
[PABX_SYT] CENTRAL TELEFÓNICA	7(13)		

(1) [10.olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística.

(2) [10.olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística.

(3) [10.olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística.

(4) [3.da] Probablemente cause la interrupción de actividades propias de la organización.

[3.pi1] Información personal: probablemente afecte a un individuo.

(5) [3.da] Probablemente cause la interrupción de actividades propias de la organización.

(6) [10.olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística.

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

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

(9) [10.olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística.

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

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

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

(13) [7.da] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones.

Tabla 37

Detalle y valoración de Comunicaciones

[COM] COMUNICACIONES			
ACTIVO	D	I	C
[PSTN_SYT] RED TELEFÓNICA	7(1)		
[WIFI_SYT] RED WIFI	1(2)		
[LAN_SYT] RED LAN	10(3)		
[WAN_SYT] RED WAN	2(4)		

(1) [7.da] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones.

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

(3) [10.olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística.

(4) [2.lg] Probablemente cause una pérdida menor de la confianza dentro de la organización.

Tabla 38

Detalle y valoración de Soportes de Información

[SI] SOPORTES DE INFORMACIÓN			
ACTIVO	D	I	C
[DISK_SYT] DISCOS	3(1)		
[USB_SYT] DISPOSITIVOS USB	3(2)		

(1) [3.olm] Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local).

(2) [3.olm] Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local).

Tabla 39

Detalle y valoración de Elementos Auxiliares

[AUX] ELMENTOS AUXILIARES

ACTIVO	D	I	C
[UPS_SYT] SISTEMAS DE ALIMENTACIÓN ININTERRUMPIDA	4(1)		
[CCTV_SYT] CIRCUITO CERRADO DE TELEVISIÓN	4(2)		
[RASTREO_SYT] SISTEMA DE RASTREO	4(3)		

(1) [4.pi1] Información personal: probablemente afecte gravemente a un individuo.

(2) [4.pi1] Información personal: probablemente afecte gravemente a un individuo.

(3) [4.pi1] Información personal: probablemente afecte gravemente a un individuo.

[4.crm] Dificulte la investigación o facilite la comisión de delitos.

Tabla 40

Detalle y valoración de Servicios Subcontratados

[SS] SERVICIOS SUBCONTRATADOS			
ACTIVO	D	I	C
[SS01_SYT] INTERNET PUNTO NET	2(1)		
[SS02_SYT] NIC EC	10(2)		
[SS03_SYT] TELEFONÍA MOBIL	9(3)		

(1) [2.lg] Probablemente cause una pérdida menor de la confianza dentro de la organización.

(2) [10.olm]] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística.

(3) [9.olm] Probablemente cause serios daños a misiones muy importantes de inteligencia o información.

[[9.lg.a] Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones con otras organizaciones.

Tabla 41

Detalle y valoración de Instalaciones

[L] INSTALACIONES			
ACTIVO	D	I	C
[L_SYT] UNIDAD DE SISTEMA DE REDES Y COMUNICACIONES	10(1)		

(1) [10.olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística.

Tabla 42

Detalle y valoración de Personal

[P] PERSONAL

ACTIVO	D	I	C
[GER_SYT] RESPONSABLE DEL ÁREA DE SISTEMAS	7(1)		10(2)
[UI_SYT] SOPORTE USUARIOS	2(3)		
[ITL_SYT] INFRAESTRUCTURA Y TELECOMUNICACIONES	2(4)		
[DBA_SYT] ADMINISTRADOR DE LA BASE DE DATOS	2(5)		
[SEG_SYT] SEGURIDAD Y CALIDAD	1(6)		
[RASTREO_SYT] MONITOREO Y SOPORTE DE RASTREO	1(7)		

(1) [7.da] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones.

[10.olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística.

(2) [2.lg] Probablemente cause una pérdida menor de la confianza dentro de la organización

(3) [2.lg] Probablemente cause una pérdida menor de la confianza dentro de la organización.

(4) [2.lg] Probablemente cause una pérdida menor de la confianza dentro de la organización

(5) [2.lg] Probablemente cause una pérdida menor de la confianza dentro de la organización

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

(7) [2.lg] Probablemente cause una pérdida menor de la confianza dentro de la organización.

5. ACTIVOS DESCRIPCIÓN

5.1 [TC_SYT] TRANSPORTE DE CARGA DE MERCANCÍA REFRIGERADA/SECA

- **[S.PUB]** Al público en general (sin relación contractual)
- **[S.EXT]** A usuarios externos (bajo una relación contractual)
- **[S.CONT]** Contratados a terceros

Dominio de Seguridad

- **[BASE]** SYTSA Transportes y Servicios Asociados

Datos

Tabla 43

Datos del activo Transporte de Mercancía Refrigerada/Seca

Transporte de Mercancía Refrigerada	Corresponde al 70% de los servicios
Transporte de Mercancía Seca	Corresponde al 30% restante

Descripción

Transportes y Servicios Asociados se encarga del Transporte e Mercadería Refrigerada y Seca mediante el uso de furgones especializados para este tipo de productos, nacional e internacionalmente a Colombia, Perú y Venezuela.

Cuenta con vehículos y furgones propios especializados en el área de transporte según se requiera.

Activos de los que depende

- [INF_SYT] INFORMACIÓN LOGÍSTICA
- [INT_SYT] INFORMACIÓN POR DEPARTAMENTO
- [SIST_RASTREO_SYT] SISTEMA DE RASTREO

Valoración

Tabla 44

Valoración del activo Transporte de carga de mercancía Refrigerada/Seca

DIMENSIÓN	VALOR	VALOR ACUMULADO
[D] DISPONIBILIDAD	**[9](1)**	**[9](1)**

(1) [9.da] Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones.

5.2 [AC_SYT] ALQUILER DE CONTENEDORES

- **[S.PUB]** Al público en general (sin relación contractual)
- **[S.EXT]** A usuarios externos (bajo una relación contractual)
- **[S.CONT]** Contratados a terceros

Dominio de Seguridad

- **[BASE]** SYTSA Transportes y Servicios Asociados

Datos

Tabla 45

Datos del activo Alquiler de contenedores

Alquiler Contenedores Refrigerados	Corresponde al 70% de este servicio
Alquiler Contenedores Secos	Corresponde al 30% restante

Descripción

Transportes y Servicios Asociados alquila contenedores secos sea estos adecuados para oficinas, campamentos mineros, bodegas, etc. o contenedores refrigerados para el almacenamiento de productos refrigerados o congelados, mediante el uso de un dispositivo especializado.

Activos de los que depende

- [INF_SYT] INFORMACIÓN LOGÍSTICA
- [INT_SYT] INFORMACIÓN POR DEPARTAMENTO

Valoración

Tabla 46

Valoración del activo Alquiler de contenedores

DIMENSIÓN	VALOR	VALOR ACUMULADO
[D] DISPONIBILIDAD	[6](1)	[6](1)

(1) [6.pi1] Información personal: probablemente afecte gravemente a un grupo de individuos.

5.3 [SMD_SYT] SERVICIO MONTAJE Y DESMONTAJE

- **[S.PUB]** Al público en general (sin relación contractual)
- **[S.EXT]** A usuarios externos (bajo una relación contractual)
- **[S.CONT]** Contratados a terceros

Dominio de Seguridad

- **[BASE]** SYTSA Transportes y Servicios Asociados

Datos

Tabla 47

Datos del Activo Servicio de montaje y desmontaje

Servicio de Montacargas	Montacargas de 2, 5, 10 toneladas
Servicio de Grúa	Grúas de 20, 35, 110 ton y Hammar

Descripción

Transportes y Servicios Asociados brinda el servicio de Montaje y Desmontaje mediante el uso de equipos como Grúas, Montacargas, Hammar, para contenedores, isotanques, maquinaria pesada, etc.

Activos de los que depende

- [INF_SYT] INFORMACIÓN LOGÍSTICA
- [INT_SYT] INFORMACIÓN POR DEPARTAMENTO

Valoración

Tabla 48

Valoración del activo Servicio de montaje y desmontaje

DIMENSIÓN	VALOR	VALOR ACUMULADO
[D] DISPONIBILIDAD	[4](1)	[4](1)

(1) [4. pi1] Información personal: probablemente afecte gravemente a un grupo de individuos.

5.4 [WEB_SYT] PORTAL WEB

- **[S.PUB]** Al público en general (sin relación contractual)
- **[S.WWW]** World Wide Web
- **[S.EMAIL]** Correo Electrónico
- **[S.DNS]** Servidor de Nombres de Dominio

Dominio de Seguridad

- **[BASE]** SYTSA Transportes y Servicios Asociados

Datos

Tabla 49

Datos del activo Portal Web

PORTAL WEB	HOSTING ALOJADO FUERA DEL PAIS SOBRE UNA VPS

Descripción

Mediante el Portal Web SYTSA informa a sus clientes y no clientes todos los servicios que ofrece la empresa como tal.

Activos de los que depende

- [IEX_SYT] INTERNET
- [SUB02_SYT] NIC

Valoración

Tabla 50

Valoración del activo Portal Web

DIMENSIÓN	VALOR	VALOR ACUMULADO
[D] DISPONIBILIDAD	[1](1)	[1](1)

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

5.5 [ZM_SYT] SERVIDOR DE CORREO ELECTRÓNICO ZIMBRA

- **[S]** Servicios
- **[S.INT]** Usuarios y medios de la propia organización
- **[S.EMAIL]** Correo electrónico

Dominio de Seguridad

- **[BASE]** SYTSA Transportes y Servicios Asociados

Datos

Tabla 51

Datos del activo Servidor de correo electrónico Zimbra

APLICACIÓN	WEB MAIL (SERVIDOR DE CORREOS)
PROCESADOR	CORE 2 QUAD
MODELO	CORE 2 QUAD
DISCO DURO	500 GIGAS
DESARROLLADOR	ZIMBRA Inc
DIRECCIÓN IP	LAN: 192.168.30.101
SISTEMA OPERATIVO	CENTOS (ZIMBRA)

Descripción

Este servicio tiene como función el envío y recepción de correo electrónico para los empleados de la Empresa SYTSA.

La empresa cuenta con un sistema único de correo tanto para mail interno como externo, este se encuentra alojado en el servidor interno que es de uso exclusivo del correo, se encuentra bajo Centos-Linux y es administrado a través de Zimbra.

La empresa tiene adquirido en NIC un dominio (sytsa.com.ec), este constituye el dominio de todas las cuentas de correo que se crean.

El correo se lee a través de la web por el mismo cliente Zimbra que utiliza, este no es necesario instalar en cada máquina para acceder a él.

La configuración del servidor permite que toda la información quede almacenada en la nube (correos, contactos, calendario, tareas entre otros)

Características principales

- Correo electrónico, contactos, calendario y documentos, todos en una sola aplicación.
- Sincroniza Zimbra, Yahoo! Mail y Gmail email, contactos y calendarios
- Lee el correo electrónico desde cualquier cuenta POP o IMAP, incluyendo AOL, Hotmail o de negocios de correo electrónico.
- Funciona en Windows, Apple, o equipos de escritorio Linux.

- No hay límite para el tamaño de su almacenamiento de correo electrónico.
- Funciona conectado y desconectado.
- Disponible en más de 20 idiomas.

Si un empleado necesita una dirección de mail, porque su puesto de trabajo lo amerita, el Gerente del área al que pertenece le notifica al encargado de sistemas y éste crea la cuenta de correo respectiva.

Activos de los que depende

- [IEX_SYT] INTERNET
- [SUB02_SYT] NIC

Valoración

Tabla 52

Valoración del activo Servidor de correo electrónico Zimbra

DIMENSIÓN	VALOR	VALOR ACUMULADO
[D] DISPONIBILIDAD	**[**10**]**(1)	**[**10**]**(1)
[I] INTEGRIDAD	**[**10**]**(2)	

(1) [10.olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística.

(2) [10.olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística.

5.6 [IP_SYT] TELEFONÍA IP

- **[S]** Servicios
- **[S.INT]** Interno (usuarios y medios de la propia organización)
- **[S.VOIP]** Voz sobre IP

Dominio de Seguridad

- **[BASE]** SYTSA Transportes y Servicios Asociados

Datos

Tabla 53

Datos del activo Telefonía IP

APLICACIÓN	TELEFONÍA IP
PROCESADOR	XEON 2.0
MODELO	ML 150
CANTIDAD	
SISTEMA OPERATIVO	CENTOS+ELASTIK
DIRECCIÓN IP	LAN: 192.168.30.6
TIPO	

Descripción

Aproximadamente hace 11 meses se instaló la Telefonía IP con la finalidad de reducir costos y de simplificar la comunicación entre Sucursales.

La capacitación al Personal aún no se ha realizado en su totalidad por tanto no se ha aprovechado en la totalidad todos los beneficios que este sistema conlleva.

Así mismo en la sucursal en Tulcán solo existe 2 extensiones IP para la comunicación con Quito, no existe un servidor, está integrado actualmente con una Central Panasonic.

Activos de los que depende

- [PABX_SYT] CENTRAL TELEFÓNICA

Valoración

Tabla 54

Valoración del activo Telefonía IP

DIMENSIÓN	VALOR	VALOR ACUMULADO
[D] DISPONIBILIDAD	**[**7**]**(1)	**[**7**]**(1)
[I] INTEGRIDAD	[7] (2)	

(1) [7.da] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones.

(2) [7.da] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones.

[7.adm] Administración y gestión probablemente impediría la operación efectiva de la organización.

5.7 [BACKUP_SYT] SERVICIO DE COPIAS DE RESPALDO

- **[S]** Servicios
- **[S.INT]** Interno (usuarios y medios de la organización)
- **[S.BACKUP]** Servicio de Copias de Respaldo

Dominio de Seguridad

- **[BASE]** SYTSA Transportes y Servicios Asociados

Datos

Tabla 55

Datos del Activo Servicio de copias de respaldo

DISCO DURO	TB SATA DE 5400 RPM

Descripción

Es un disco duro que se encuentra en cada servidor para realizar los respectivos respaldos.

Activos de los que depende

- [INF_SYT] INFORMACIÓN LOGÍSTICA
- [INT_SYT] INFORMACIÓN POR DEPARTAMENTO
- [PER_B_SYTS] INFORMACIÓN PERSONAL DE CADA USUARIO

Valoración

Tabla 56

Valoración del activo Servicios de copia de respaldo

DIMENSIÓN	VALOR	VALOR ACUMULADO
[D] DISPONIBILIDAD	[3](1)	[3](1)
[I] INTEGRIDAD	[3] (2)	
[C] CONFIDENCIALIDAD	[3] (3)	

(1) [3.olm] Probablemente merme la eficacia o seguridad de la misión operativa logística (alcance local).

[3.cei.e] Constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros.

(2) [3.pi1] Información personal: probablemente afecte a un individuo.

(3) [3.pi1] Información personal: probablemente afecte a un individuo.

5.8 [INF_SYT] INFORMACIÓN DE LOGÍSTICA

- **[D]** Datos e Información
- **[D.COM]** Datos de interés comercial
- **[D.INT]** Datos de gestión interna
- **[D.LABEL.DL]** Datos de difusión Limitada

Dominio de Seguridad

- **[BASE]** SYTSA Transportes y Servicios Asociados

Datos

Tabla 57

Datos del Activo Información Logística

INFORMACIÓN DE VIAJES REALIZADOS	ORDENES DE MOVIMIENTO POR CADA RUTA O ALQUILER DE CONTENEDORES O CARGUES Y DESCARGUES
INFORMACIÓN DE PROVEEDORES	INGRESO DE FACTURAS DE COMPRA ASIGNADAS POR UNA OMT
FACTURACIÓN DE CLIENTES	INGRESO DE FACTURAS ASIGNADAS POR UNA OMT

Descripción

La información correspondiente al módulo de logística y operaciones, se enfoca en el ingreso de información de cada uno de los viajes realizados por cada vehículo, diariamente. Conjuntamente con esto se ingresa facturas de compra y facturas de venta a las cuales se les asocia uno o varios de los viajes que se han creado según sea el caso.

Esta información es ingresada por la Asistente del Coordinador de Tráfico que es la persona que está al tanto de las operaciones realizadas.

Activos de los que depende

- [NIGISU_SYT] SISTEMA FINANCIERO
- [OFF_SYT] OFIMÁTICA

Activos que dependen de este

- [TC_SYT] TRANSPORTE REFRIGERADO
- [AC_SYT] ALQUILER DE CONTENEDORES
- [SMD_SYT] SERVICIO DE MONTAJE Y DESMONTAJE
- [BACKUP_SYT] SERVICIO DE COPIAS DE RESPALDO

Valoración

Tabla 58

Valoración del activo Información logística

DIMENSIÓN	VALOR	VALOR ACUMULADO
[D] DISPONIBILIDAD	[10](1)	[10](1)
[I] INTEGRIDAD	[10](2)	
[C] CONFIDENCIALIDAD	[10](3)	

(1) [10.olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística.

(2) [10.olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística.

(3) [10.olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística.

5.9 [C.INT] INFORMACIÓN POR DEPARTAMENTO

- **[D]** Datos e Información
- **D.INT]** Datos de gestión interna

- **[D.LABEL.DL]** Datos de difusión Limitada
- **[D.COM]** Datos de interés comercial

Dominio de Seguridad

- **[BASE]** SYTSA Transportes y Servicios Asociados

Datos

Tabla 59

Datos del activo Información por departamento

Departamento Contable	Recopilación de la información de todos los departamentos, para generar los reportes contables
Departamento Cobranzas	Información que contiene los datos para conocer la cartera pendiente.
Departamento Jurídico	Información sobre los datos legales que debe tener la empresa como por ejemplo: documentos de los vehículos, furgones, etc.
Departamento Comercial	Información sobre los datos de clientes y nuevos clientes, estrategias, etc.
Departamento de Mantenimiento	Información sobre los datos del mantenimiento de las unidades, equipos, contenedores, etc.

Descripción

En Transportes y Servicios Asociados Sytsa, se tiene una división por departamentos y es así que la información está clasificada de igual manera, cada departamento según la función que cumple almacena sus datos en el Servidor.

Activos de los que depende

- [NIGISU_SYT] SISTEMA FINANCIERO
- [OFF_SYT] OFIMÁTICA

Activos que dependen de este

- [TC_SYT] TRANSPORTE REFRIGERADO
- [AC_SYT] ALQUILER DE CONTENEDORES
- [SMD_SYT] SERVICIO DE MONTAJE Y DESMONTAJE
- [BACKUP_SYT] SERVICIO DE COPIAS DE RESPALDO

Valoración

Tabla 60

Valoración del activo Información por departamento

DIMENSIÓN	VALOR	VALOR ACUMULADO
[D] DISPONIBILIDAD	[7](1)	[7](1)
[I] INTEGRIDAD	[7](2)	
[C] CONFIDENCIALIDAD	[7](3)	

(1) [7.adm] Administración y gestión probablemente impediría la operación efectiva de la organización.

(2) [7.adm] Administración y gestión probablemente impediría la operación efectiva de la organización.

(3) [7.adm] Administración y gestión probablemente impediría la operación efectiva de la organización.

5.10 [LOG_SYT] INFORMACIÓN DE REGISTROS DE INGRESOS SOBRE LOS SERVIDORES

- **[D]** Datos e Información
- **[D.LOG]** Registro de actividad (log)

Dominio de Seguridad

- **[BASE]** SYTSA Transportes y Servicios Asociados

Datos

Tabla 61

Datos del activo Información de registros de ingresos sobre los servidores

REGISTROS (LOG)	REGISTRO DE LAS ACTIVIDADES DEL SERVIDOR DE CORREOS

Descripción

Es un registro de todos los sucesos y eventos ocurridos en un sistema (Servidor), el cual especifica horas de acceso autorizados y no autorizados.

Activos de los que depende

- [SBS_SYT] SERVIDOR DE BASE DE DATOS

Valoración

Tabla 62

Datos del activo Información de registros de ingresos sobre los servidores

DIMENSIÓN	VALOR	VALOR ACUMULADO
[D] DISPONBILIDAD	[9](1)	[9](1)
[I] INTEGRIDAD	[9](2)	
[C] CONFIDENCIALIDAD	[9](3)	

(1) [9.lg.a] Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones con otras organizaciones

[9.iic] Probablemente cause serios daños a misiones muy importantes de inteligencia o información.

(2) [9.si] Seguridad: probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios.

(3) [9.lg.a] Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones con otras organizaciones.

5.11 D.INT_SYT] INFORMACIÓN PERSONAL DE CADA USUARIO

- **[D]** Datos e Información
- **[D.PER.B]** Registro de carácter personal nivel medio

Dominio de Seguridad

[BASE] SYTSA Transportes y Servicios Asociados

Datos

DATOS DE CADA USUARIO	INFORMACIÓN CORRESPONDIENTE A LA FUNCIÓN DE CADA USUARIO Y TAMBIÉN INFORMACIÓN PERSONAL

Descripción

Los usuarios guardan información correspondiente a cada uno de sus funciones como datos, documentos, reportes, archivos de imágenes y también información personal.

Activos de los que depende

- [DESKTOP_SYT] COMPUTADORAS DE ESCRITORIO
- [LAPTOPS_SYT] COMPUTADORAS PORTÁTILES

Activos que dependen de este

- [BACKUP_SYT] SERVICIO DE COPIAS DE RESPALDO

Valoración

Tabla 63

Valoración del activo Información personal de cada usuario

DIMENSIÓN	VALOR	VALOR ACUMULADO
[ ]	**[ ]**	**[])**

5.12 **[SW.NIGISU_SYT]** Sistema Financiero NIGISU

- **[D.VR]** Datos muy importantes (vitales)
- **[D.BIZ]** Datos de interés para el negocio
- **[D.INT]** Datos de gestión interna
- **[D.LOG]** Registro de actividad
- **[SW]** Aplicaciones SW
- **[SW.SUB]** Desarrollo a medida (subcontratado)
- **[SW.STD.DBMS]** Sistema de Gestión de Base de Datos
- **[SW.STD.OS]** Sistema Operativo Windows

Dominio de Seguridad

- **[BASE]** SYTSA Transportes y Servicios Asociados

Datos

Tabla 64

Datos del activo Sistema financiero Nigisu

APLICACIÓN	SERVIDOR DE DATOS + SISTEMA CONTABLE	
PROCESADOR	XEON 2.4	SOCKET MICRO S 755
MODELO	HP DL 180	
DISCO DURO	500 GIGAS + 500 GIGAS HOT SW	
MEMORIA	4 GIGAS	
DIRECCIÓN IP	LAN: 192.168.30.1	WAN: 200.105.246.122/29 A 126
SISTEMA OPERATIVO	2008 SERVER ENTERPRISE	

Descripción

El sistema Nigisu posee varios módulos entre ellos el de Contabilidad, el perteneciente al desarrollo del Negocio (Operaciones-Transporte).

En la empresa se utiliza SQL Anyware de Sybase para el almacenamiento y la administración de los datos, los cuales están almacenados en su repositorio respectivo de Base de Datos, el cual maneja las seguridades propias de la Sybase.

La única persona que puede tener acceso a los archivos de la base de datos es el administrador del sistema y todo aquel que opere el servidor de aplicaciones (es decir las personas que tengan acceso físico al equipo y con clave).

Solo existe una aplicación informática de uso de la Empresa, este aplicativo está formado por algunos módulos como Contabilidad, inventario, personal, CXC (Dentro de este se encuentra el módulo sobe el cual gira el negocio), CXP, entre otros,

El nivel de acceso a la aplicación, se lo realiza a través del propio aplicativo, en el módulo de administración, donde se registran y se dan los accesos respectivos a cada uno de los usuarios del sistema informático.

Los aplicativos que administran la base de datos disponen de recursos suficientes para su funcionamiento, ya que aproximadamente el 80% de los recursos del servidor están en uso,

Cada una de las transacciones efectuadas en las distintas tablas de la base de datos, se almacenan en el registro de Auditoria creado en la base de datos donde se registran el usuario y la fecha y desde que IP se realiza el cambio, con lo que se

puede determinar entre otras cosas que usuario, desde que máquina y en qué fecha realizó alguna transacción.

Activos de los que depende

- [SBD_SYT] SERVIDOR DE BASE DE DATOS
- [WIFI_SYT] PUNTOS DE ACCESO WIRELESS]
- [SWITCH_SYT] SWITCH

Activos que dependen de este

- [INF:SYT] INFORMACIÓN LOGÍSTICA
- [INT_SYT] INFORMACIÓN POR DEPARTAMENTO

Valoración

Tabla 65

Valoración del activo Sistema financiero Nigisu

DIMENSIÓN	VALOR	VALOR ACUMULADO
[D] DISPONIBILIDAD	[6](1)	[6](1)
[I] INTEGRIDAD	[6](2)	
[C] CONFIDENCIALIDAD	[6](3)	

(1) [6.pi1] Información personal: probablemente afecte gravemente a un grupo de individuos

(2) [6.pc] Orden público: probablemente cause manifestaciones o presiones significativas.

(3) [6.lbl] Datos clasificados como de difusión limitada.

5.13 [OFF_SYT] OFIMÁTICA

- **[SW]** Aplicaciones SW
- **[SW.STD]** Estándar (off the Shelf)
- **[SW.STD.OFFICE]** Ofimática
- **[SW.STD.OS]** Sistema Operativo

Dominio de Seguridad

[BASE] SYTSA Transportes y Servicios Asociados

Datos

Tabla 66

Datos del activo Ofimática

BAJO	MICROSOFT OFFICE, VERSION
WINDOWS	OFFICE 2010

Descripción

Aplicaciones que se utilizan para la elaboración de hojas de cálculo, procesamiento de datos, presentaciones, elaboración de reportes, etc.

Activos de los que depende

- [SBD_SYT] SERVIDOR DE BASE DE DATOS
- [SWITCH_SYT]

- [GTWY_SYT] GATEWAY

Activos que dependen de este

- [INF:SYT] INFORMACIÓN LOGÍSTICA
- [INT_SYT] INFORMACIÓN POR DEPARTAMENTO

Valoración

Tabla 67

Valoración del activo Ofimática

DIMENSIÓN	VALOR	VALOR ACUMULADO
[D]	[1](1)	[1](1)

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

[1.adm] Administración y gestión: pudiera impedir la operación efectiva de una parte de la organización.

[1.pi1] Información personal: pudiera causar molestias a un individuo

[1.lbl] Datos clasificados como sin clasificar.

5.14 [AV_SYT] ANTIVIRUS

- **[SW]** Aplicaciones SW

- **[SW.STD_SYT]** Estándar (off the Shelf)
- **[SW.STD.AV]** Antivirus
- **[SW.STD.OS]** Sistema Operativo

Dominio de Seguridad

[BASE] SYTSA Transportes y Servicios Asociados

Datos

Tabla 68

Datos del activo Antivirus

SOFTWARE 1	KASPERSKY 2013
SOFTWARE 2	MICROSOFT SECURITY ESSENTIAL
SOFTWARE 3	CLAM AV

Descripción

La empresa adquirió a inicios del 2010 Licencias Corporativas del Antivirus Kaspersky Internet Security con lo cual se tienen protegidas a las estaciones de trabajo.

El Servidor de Correo cuenta con el antivirus ClamAV, el Servidor de Datos cuenta con Microsoft Security Essentials y las otras computadoras (Laptops) se mantienen con el Microsoft Security Essentials, incorporado en Windows.

No han existido muchos inconvenientes con virus, a excepción de algunos dispositivos extraíbles.

Desde Internet se actualizan las listas de virus del KIS, el mismo que se actualiza en el Servidor. Las actualizaciones en todos los equipos son automáticas, el usuario no hace ningún proceso en este caso.

Se realizan escaneos automáticos cada 15 días en todas las estaciones, esto hace que los equipos trabajen más lento, pero se aumenta la seguridad.

Activos de los que depende

- [DESKTOP_SYT]
- [LAPTOPS_SYT]

Valoración

Tabla 69

Valoración del activo Antivirus

DIMENSIÓN	VALOR	VALOR ACUMULADO
[C] CONFIDENCIALIDAD	[7](1)	[7](1)

(1) [7.olm] Probablemente cause o perjudique la eficacia o seguridad de la misión operativa o logística

[7.cei.e] Interese comerciales o económicos constituye un serio incumplimiento de obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros.

5.15 [OTR_SYT] OTROS SOFTWARE

- **SW]** Aplicaciones SW
- **[SW.STD]** Estándar (off the Shelf)

- **[SW.STD.OS]** Sistema Operativo
- **[SW.STD.OTHER]** Otros

Dominio de Seguridad

[BASE] SYTSA Transportes y Servicios Asociados

Datos

Tabla 70

Datos del activo Otros Software

SOFTWARE 1	PROYECT
SOFTWARE 2	PAQUETE ADOBE
SOFTWARE 3	VISIO
SOFTWARE 4	WIN TRAC

Descripción

Los anteriormente anotados son los principales software que se utilizan en la empresa para diferentes funciones.

Activos de los que depende

- [SWITCH_SYT] SWITCH

Valoración

Tabla 71

Valoración del activo Otros Software

DIMENSIÓN	VALOR	VALOR ACUMULADO
[D] DISPONIBILIDAD	[1](1)	[1](1)

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

5.16 [IEX_SYT] INTERNET

- **[SW]** Aplicaciones SW
- **[SW.STD]**
- **[SW.STD.OS.WINDOWS]** Windows

Dominio de Seguridad

[BASE] SYTSA Transportes y Servicios Asociados

Datos

Tabla 72

Datos del activo Internet

DISEÑO	HTML,CSSS,XML
INTERFAZ DE USUARIO	FTP
PROTOCOLO	HTTP FTP
SISTEMA OPERATIVO	WINDOWS
AMBITO	SOFTWARE LIBRE

Descripción.

Navegación internet, browser para acceso al sistema y configuración.

Activos de los que depende

- [SWITCH_SYT] SWITCH
- [ROUTER_SYT] ROUTER
- [FIREWALL] FIREWALL
- [WIFI_SYT] PUNTOS DE ACCESO WIRELESS
- [WAN_SYT] RED WAN

Activos que dependen de este

- [WEB_SYT] PORTAL WEB
- [ZM_SYT] SERVIDOR DE CORREO ELECTRÓNICO
- [IP_SYT] TELEFONÍA IP

Valoración

Tabla 73

Valoración del activo Internet

DIMENSIÓN	VALOR	VALOR ACUMULADO
[D] DISPONIBILIDAD	[2](1)	[2](1)

(1) [2.lg] Probablemente cause una pérdida menor de la confianza dentro de la organización.

5.17 [SBD_SYT] SERVIDOR DE DATOS

- **[D]** Datos e Información
- **D.INT]** Datos de gestión interna
- **[SW]** Aplicaciones (software)
- **[SW.STD]** Estándar (off the shelf)
- **[SW.STD.FILE]** Servidor de Ficheros
- **[HW]** Equipamiento Informático (hardware)
- **[HW.HOST]** Grandes equipos
- **[HW.DATA]** Que almacena datos

Dominio de Seguridad

[BASE] SYTSA Transportes y Servicios Asociados

Datos

Tabla 74

Datos del activo Servidor de Datos

APLICACIÓN	SERVIDOR DE DATOS	
PROCESADOR	XEON 2.4	SOCKET MICRO S 755
MODELO	HP DL 180	
DISCO DURO	500 GIGAS + 500 GIGAS HOT SW	
MEMORIA	4 GIGAS	
DIRECCIÓN IP	LAN: 192.168.30.1	WAN: 200.105.246.122/29 A 126
SISTEMA OPERATIVO	2008 SERVER ENTERPRISE	

Descripción

El servidor dedicado que se encarga de almacenar la información de todos los usuarios mediante el uso del Active Directory también se encuentra instalado el Sistema Contable para uso interno de los usuarios.

Activos de los que depende

- [SIWTCH] SWITCH
- [UPS_SYT] SISTEMAS DE ALIMENTACIÓN ININTERRUMPIDA

Activos de los que depende este

- **[**NIGISU_SYT] SISTEMA FINANCIERO NIGISU
- **[**LOG_SYT] INFORMACIÓN DE REGISTROS DE INGRESOS SOBRE LOS SERVIDORES
- [OFF_SYT] OFIMÁTICA

Valoración

Tabla 75

Valoración del activo Servidor de datos

DIMENSIÓN	VALOR	VALOR ACUMULADO
[D] DISPONIBILIDAD	[10](1)	[10](1)
[I] INTEGRIDAD	[10](2)	[10](2)

(1) [10.olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística.

(2) [10.olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística.

5.18 [FIREWALL_SYT] FIREWALL

- **[HW]** Equipamiento Informático (hardware)
- **[HW.NETWORK]** Soporte de Red
- **[HW.NETWORK.FIREWALL]** Cortafuegos

Dominio de Seguridad

[BASE] SYTSA Transportes y Servicios Asociado

Datos

Tabla 76

Datos del activo Firewall

APLICACIÓN	FIREWALL	
PROCESADOR	AMD TURION II	
MODELO	MICRO SERVER HP	
DISCO DURO	500 GIGAS	
MEMORIA	2 GIGAS	
DIRECCIÓN IP	LAN: 192.168.30.100	WAN: 200.105.246.122/29 A 126
SISTEMA OPERATIVO	LINUX EMBEBIDO	

Descripción

Es un Servidor real con un Sistema Operativo Linux manejado y controlado por un SQUID (programa para manejo de control de tráfico, ancho de banda, bloqueo de filtro URL, etc.

Activos de los que depende

- [ROUTER] ROUTER

Activos que dependen de este

- [IEX] INTERNET

Valoración

Tabla 77

Valoración del activo Firewall

DIMENSIÓN	VALOR	VALOR ACUMULADO
[D] DISPONIBILIDAD	[10](1)	[ ]

(1) [10.olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística.

5.19 [DESKTOP_SYT] Computadoras de Escritorio

- **[HW]** Equipamiento Informático (hardware)
- **[HW.MID]** Equipos medios

Dominio de Seguridad

[BASE] SYTSA Transportes y Servicios Asociados

Datos

Tabla 78

Datos del activo Computadoras de escritorio

APLICACIÓN	PROCESADOR	MODELO	MAINBOARD	DISCO DURO	MEMORIA	SISTEMA OPERATIVO
OPERACIONES 1	PENTIUM 4	ESCRITORIO ZIP	INTEL D945GTP	160 GIGAS	2 GIGAS	WINDOWS 7
OPERACIONES 2	INTEL CORE 2 DUO	ESCRITORIO ALTEK	DG4ICN	160 GIGAS	3 GIGAS	WINDOWS 7
OPERACIONES 3	INTEL CELERON	ESCRITORIO ALTEK	ECS 9456CT-M	160 GIGAS	2 GIGAS	WINDOWS 7
MANTENIMIENTO	INTEL CORE 2 DUO	ESCRITORIO IBM	DG3 PR	250 GIGAS	2 GIGAS	WINDOWS 7
RECEPCION	CORE I5	ESCRITORIO HP	COMPAQ 6200	500 GIGAS	2 GIGAS	WINDOWS 7
CONTABILIDAD 1	DUAL CORE	ESCRITORIO SAZ	DG31PR	160 GIGAS	2 GIGAS	WINDOWS 7
CONTABILIDAD 2	CORE I5	ESCRITORIO HP	COMPAQ 6200	500 GIGAS	2 GIGAS	WINDOWS 7
CONTABILIDAD 3	CORE I5	ESCRITORIO HP	COMPAQ 6200	500 GIGAS	2 GIGAS	WINDOWS 7
ADMINISTRATIVO	PENTIUM 4	ESCRITORIO HP	AWRDACPI	80 GIGAS	1 GIGA	WINDOWS 7

Descripción

Son computadoras clones y de marca (HP, DELL) de uso del personal de la empresa, sobre estos equipos se encuentra instalados sistemas operativos Windows 7, XP e instalado el software necesario para el buen funcionamiento de la organización.

Activos de los que depende

- [LAN_SYT] RED LAN
- [UPS_SYT] SISTEMAS DE ALIMENTACIÓN ININTERRUMPIDA

Activos que dependen de este

- [PER_B] INFORMACIÓN DE CADA USUARIO
- [AV_SYT] ANTIVIRUS

Valoración

Tabla 79

Valoración del activo Computadoras de escritorio

DIMENSIÓN	VALOR	VALOR ACUMULADO
[D] DISPONIBILIDAD	[3](1)	[3](1)

(1) [3.da] Probablemente cause la interrupción de actividades propias de la organización.

[3.pi1] Información personal: probablemente afecte a un individuo.

5.20 [LAPTOPS_SYT] COMPUTADORAS PORTÁTILES

- **[HW]** Equipamiento Informático (hardware)
- **[HW.PC]** Informática personal
- **[HW.MOBILE]** Informática móvil

Dominio de Seguridad

[BASE] SYTSA Transportes y Servicios Asociados

Datos

Tabla 80

Datos del activo Computadoras portátiles

APLICACIÓN	PROCESADOR	MODELO	MAINBOARD	DISCO DURO	MEMORIA	SISTEMA OPERATIVO
OPERACIONES 1	INTEL CORE 2 DUO	DELL LAPTOP	MXC062	160 GIGAS	3 GIGAS	WINDOWS 7
MANTENIMIENTO 1		SONY VAIO	MXC062	750 GIGAS	8 GIGAS	WINDOWS 7
MANTENIMIENTO 2	AMD PETHOM II	HACER	ASPIRE 5552	500 GIGAS	4 GIGAS	WINDOWS 7
RECURSOS HUMANOS	GENUINE INTEL	TOSHIBA	SATELLITE A135	80 GIGAS	2 GIGAS	WINDOWS 7
CONTABILIDAD	GENUINE INTEL	HP	PAVILLION DV2000	80 GIGAS	1 GIGA	WINDOWS 7
ADMINISTRATIVO	CORE I5	HP	PAVILLION DM 4	500 GIGAS	4 GIGAS	WINDOWS 7
SEGURIDAD	CORE I5	HP	DV4 NOTEBOOK	250 GIGAS	4 GIGAS	WINDOWS 7
COMERCIAL	CORE I5	SONY VAIO	SUE 14117	750 GIGAW	6 GIGAS	WINDOWS 7
COMERCIAL						WINDOWS 7
JURÍDICO	CORE 2 DUO	HP	COMPAQ 6530B	160 GIGAS	3 GIGAS	WINDOWS 7

Descripción

Las computadora portátiles en su mayoría son de marca HP, las cuales se encuentran instalados varios sistemas operativos como Windows 7 u 8, y son más para uso a nivel Gerencial y Administrativo.

Activos de los que depende

- [UPS_SYT] SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA

Activos que dependen de este

- [PER_B] INFORMACIÓN DE CADA USUARIO
- [AV_SYT] ANTIVIRUS

Valoración

Tabla 81

Valoración del activo Computadoras Portátiles

DIMENSIÓN	VALOR	VALOR ACUMULADO
[D] DISPONIBILIDAD	[3](1)	
[C] CONFIDENCIALIDAD	[1](1))	[1](1)

(1) [3.da] Probablemente cause la interrupción de actividades propias de la organización.

(2) [10.olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística.

5.21 [SCAN_SYT] SCANNER

- **HW]** Equipamiento Informático (hardware)
- **[HW.PERIPHERAL]** Periféricos
- **[HW.PERIPHERAL.SCAN]** Scanner

Dominio de Seguridad

[BASE] SYTSA Transportes y Servicios Asociados

Datos

Tabla 82

Datos del activo Scanner

MARCA	RICOH AFICIO
MODELO	3225 C

Descripción

El scanner es un dispositivo que funciona sobre una Impresora Multifunción el cual nos permite realizar la digitalización de los documentos y enviarlos directamente a un correo.

Activos de los que depende

- **[**LAN_SYT] RED LAN
- UPS_SYT] SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA

Valoración

Tabla 83

Valoración del activo Scanner

DIMENSIÓN	VALOR	VALOR ACUMULADO
[D] DISPONIBILIDAD	[]	[ ]
[C] CONFIDENCIALIDAD	[]	
[INTEGRIDAD]	[]	

5.22 [PRINT1_SYT] IMPRESORAS MATRICIALES

- **HW]** Equipamiento Informático (hardware)
- **[HW.PERIPHERAL]** Periféricos
- **[HW.PERIPHERAL.PRINT]** Medios de Impresión

Dominio de Seguridad

[BASE] SYTSA Transportes y Servicios Asociados

Datos

Tabla 84

Datos del activo Impresoras matriciales

MARCA	EPSON
MODELO	LX-300
	FX-890
	LQ-590

Descripción

Son dispositivos periféricos de salida que normalmente se utiliza para realizar las operaciones contables de la empresa como facturación, retenciones, asientos, ingresos, egresos, etc.

Activos de los que depende

- [LAN_SYT] RED LAN
- [UPS_SYT] SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA

Valoración

Tabla 85

Valoración del activo Impresoras matriciales

DIMENSIÓN	VALOR	VALOR ACUMULADO
[D] DISPONIBILIDAD	[1](1)	[1](1)

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

5.23 [PRINT2_SYT] IMPRESORA LASER

- **[HW]** Equipamiento Informático (hardware)
- **[HW.PERIPHERAL]** Periféricos
- **[HW.PERIPHERAL.PRINT]** Medios de Impresión

Dominio de Seguridad

[BASE] SYTSA Transportes y Servicios Asociados

Datos

Tabla 86

Datos del activo Impresora Laser

MARCA	RICOH AFICIO
MODELO	3225 C

Descripción

Periférico de salida que normalmente se utiliza para la impresión de informes y reportes, cotizaciones entre otros

Activos de los que depende

- [LAN_SYT] RED LAN
- [UPS_SYT] SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA

Valoración

Tabla 87

Valoración del activo Impresora Laser

DIMENSIÓN	VALOR	VALOR ACUMULADO
[D] DISPONIBILIDAD	[1](1)	[ ]

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

5.24 [SWITCH_SYT] SWITCH

- **[HW]** Equipamiento Informático (hardware)
- **[HW.NETWORK]** Soporte de Red
- **[HW.NETWORK.SWITCH]** Conmutador

Dominio de Seguridad

[BASE] SYTSA Transportes y Servicios Asociados

Datos

Tabla 88

Datos del activo Switch

MARCA	HP
MODELO	24 PUERTOS BASE LINE
CANTIDAD	2 SWITCHES

Descripción

El switch es un dispositivo especial diseñado para resolver problemas de rendimiento en la red y manejo de ancho de bandas pequeño y embotellamientos sobre el cual se maneja todos los datos de la empresa.

Activos de los que depende

- [LAN_SYT] RED LAN
- [UPS_SYT] SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA

Activos que dependen de este

- [SBD_SYT] SERVIDOR DE BASE DE DATOS
- [IEX] INTERNET
- [OTR_SW] OTROS SOFTWARE

Valoración

Tabla 89

Valoración del activo Switch

DIMENSIÓN	VALOR	VALOR ACUMULADO
[D] DISPONIBILIDAD	[10](1)	[ ]

(1) [10.olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística.

5.25 [ROUTER_SYT] ROUTER

- **[HW]** Equipamiento Informático (hardware)
- **[HW.NETWORK]** Soporte de Red
- **[HW.NETWORK.ROUTER]** Encaminador

Dominio de Seguridad

[BASE] SYTSA Transportes y Servicios Asociados

Datos

Tabla 90

Datos del activo Router

MARCA	CISCO
MODELO	SERIE 800

Descripción

Router como su nombre mismo lo indica es un enrutador o encaminador que nos sirve para interconectar la subred de nuestro proveedor de internet hacia puertos de acceso de internet.

Activos de los que depende

- [WAN_SYT] RED WAN
- [UPS_SYT] SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA

Activos que dependen de este

- **[**FIREWALL] FIREWALL

Valoración

Tabla 91

Valoración del activo Router

DIMENSIÓN	VALOR	VALOR ACUMULADO
[D] DISPONIBILIDAD	[1](1)	[ ]

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

5.26 [GTWY_SYT] GATEWAY

- **[HW]** Equipamiento Informático (hardware)
- **[HW.NETWORK]** Soporte de Red
- **[HW.NETWORK.GTWY]** Pasarela

Dominio de Seguridad

[BASE] SYTSA Transportes y Servicios Asociados

Datos

Tabla 92

Datos del activo Gateway

APLICACIÓN	FIREWALL	
PROCESADOR	AMD TURION II	
MODELO	MICRO SERVER HP	
DISCO DURO	500 GIGAS	
MEMORIA	2 GIGAS	
DIRECCIÓN IP	LAN: 192.168.30.100	WAN: 200.105.246.122/29 A 126
SISTEMA OPERATIVO	LINUX EMBEBIDO	

Descripción

Es nuestro servidor firewall el que se encarga de hacer Gateway (Puerta de Enlace), permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación, el propósito principal es de traducir la información del protocolo utilizado en una red al protocolo utilizado en la red de destino

Activos de los que depende

- [GTWY_SYT] GATEWAY

Valoración

Tabla 93

Valoración del activo Gateway

DIMENSIÓN	VALOR	VALOR ACUMULADO
[D] DISPONIBILIDAD	[1](1)	[ ]

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

5.27 [WIFI_SYT] PUNTOS DE ACCESO WIRELESS

- **[HW]** Equipamiento Informático (hardware)
- **[HW.NETWORK]** Soporte de Red
- **[HW.NETWORK.WAP]** Punto de Acceso Wireless

Dominio de Seguridad

[BASE] SYTSA Transportes y Servicios Asociados

Datos

Tabla 94

Datos del activo Puntos de acceso Wireless

MARCA	TRICOM
MODELO	7760 LONG RANGE

Descripción

Es un equipo de conexión de todos los dispositivos electrónicos de la empresa de forma inalámbrica, tales como Smart phones, tablets, reproductores digitales y computadoras portátiles entre otros.

Activos de los que depende

- [RADIO_SYT] RED INHALÁMBRICA
- [UPS_SYT] SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA

Activos que dependen de este

- [NIGISU_SYT] SISTEMA FINANCIERO CONTABLE
- [IEX_SYT] INTERNET

Valoración

Tabla 95

Datos del activo Puntos de acceso Wireless

DIMENSIÓN	VALOR	VALOR ACUMULADO
[D] DISPONIBILIDAD	[1](1)	[ ]

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

5.28 [PABX_SYT] CENTRAL TELEFÓNICA

- **[HW]** Equipamiento Informático (hardware)
- **[HW.PABX]** Central Telefónica

Dominio de Seguridad

[BASE] SYTSA Transportes y Servicios Asociados

Datos

Tabla 96

Datos del activo Central Telefónica

APLICACIÓN	TELEFONÍA IP	
PROCESADOR	XEON 2.0	SOCKET MICRO S 755
MODELO	ML 150	
DISCO DURO	1 TERA	
MEMORIA	2 GIGAS	
DIRECCIÓN IP	LAN: 192.168.30.6	WAN: 200.105.246.122/29 A 126
SISTEMA OPERATIVO	CENTOS+ELASTIK	

Descripción

Actualmente SYTSA cuenta con Telefonía IP, instalada en la Central en Quito y con sucursales en Aloag, Tulcán, Guayaquil.

Aproximadamente hace 9 meses se instaló la Telefonía IP con la finalidad de reducir costos y de simplificar la comunicación entre Sucursales.

Activos de los que depende

- [UPS_SYT] SISTEMA DE ALIMENTACIÓN ININTERRUMPUDA
- [PSTN_SYT] RED TELEFÓNICA

Activos que dependen de este

- [IP_SYT] TELEFONÍA IP

Valoración

Tabla 97

Valoración del activo Central Telefónica

DIMENSIÓN	VALOR	VALOR ACUMULADO
[D] DISPONIBILIDAD	[7](1)	[ ]

(1) [7.da] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones.

5.29 [PSTN_SYT] RED TELEFÓNICA

- **[COM]** Comunicaciones
- **[COM.PSTN]** Red Telefónica

Dominio de Seguridad

[BASE] SYTSA Transportes y Servicios Asociados

Datos

Tabla 98

Datos del activo Red telefónica

TIPO	CABLE UTP
	CAT6 LAN PRO

Descripción

La red telefónica utilizada en la empresa ésta realizada a través de un cable UTP Cat 6 de marca LANPRO por el cual viaja toda la comunicación con sus respectivos accesorios.

Activos de los que depende

- [L_SYT] UNIDAD DE SISTEMAS DE REDES Y COMUNICACIONES

Activos que dependen de este

- [PABX_SYT] CENTRAL TELEFÓNICA

Valoración

Tabla 99

Valoración el activo Red telefónica

DIMENSION	VALOR	VALOR ACUMULADO
[D] DISPONIBILIDAD	[7](1)	[ ]

(1) [7.da] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones.

5.30 [RADIO_SYTS] RED INÁLAMBRICA

- **[COM]** Comunicaciones
- **[COM.RADIO]** Red Inalámbrica

Dominio de Seguridad

[BASE] SYTSA Transportes y Servicios Asociados

Datos

Tabla 100

Datos del activo Red inalámbrica

MARCA	TRICOM
MODELO	7760 LONG RANGE

Descripción

Es un equipo de conexión de todos los dispositivos electrónicos de la empresa de forma inalámbrica, tales como Smart phones, tablets, reproductores digitales y computadoras portátiles entre otros.

Activos de los que depende

- [L_SYT] UNIDAD DE SISTEMAS DE REDES Y COMUNICACIONES

Activos que dependen de este

- [WIFI_SYT] PUNTOS DE ACCESO WIRELESS

Valoración

Tabla 101

Valoración del activo Red inalámbrica

DIMENSIÓN	VALOR	VALOR ACUMULADO
[D] DISPONIBILIDAD	[1](1)	[ ]

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

5.31 [LAN_SYT] RED LAN

- **[COM]** Comunicaciones
- **[COM.LAN]** Red Local

Dominio de Seguridad

[BASE] SYTSA Transportes y Servicios Asociados

Datos

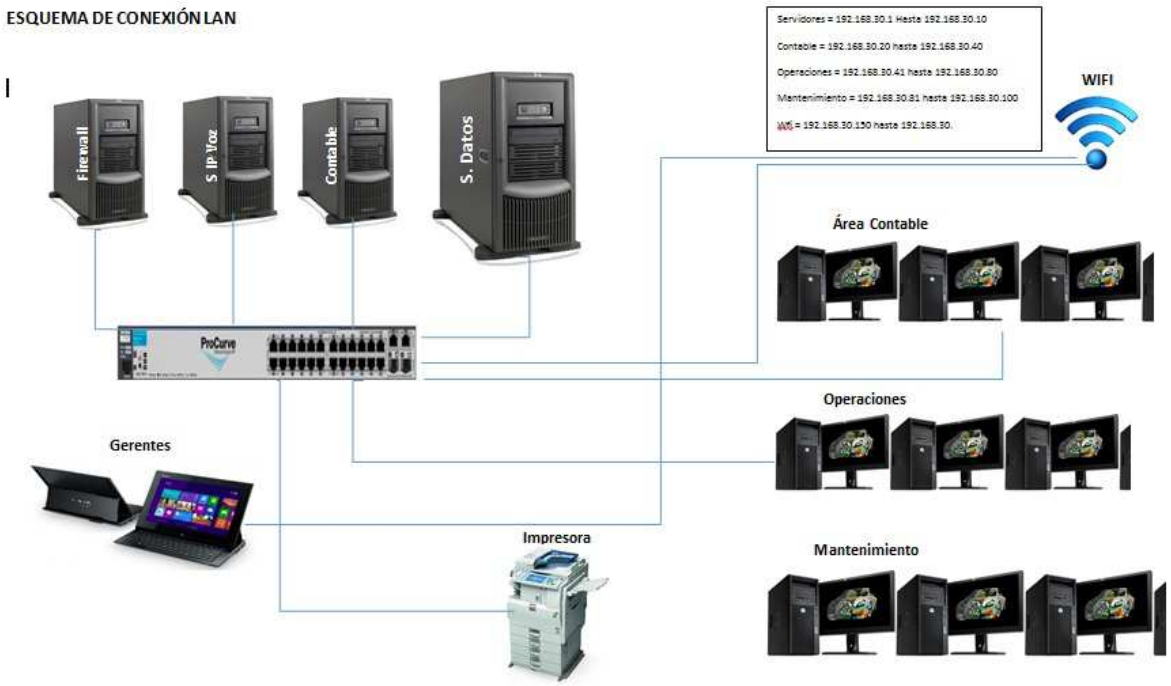


Figura 13 Esquema de la Red Lan de Sytsa

Descripción

La red LAN de la empresa SYTSA (Matriz) en la ciudad de Quito cuenta con 6 Servidores, 23 Estaciones de trabajo de las cuales 11 son computadores de escritorio y 11 son portátiles.

El cuarto de servidores actualmente se encuentra compartiendo el mismo lugar del Departamento de Calidad y Seguridad

Los servidores están dentro de un gabinete conectados a un UPS de 2 Kva. Hay dos Switches Hp 10/1000 Base Line.

En la ciudad de Tulcán cuenta con 4 Servidores y 10 Estaciones de Trabajo de las cuales 9 son computadoras de escritorio 1 Laptop.

En la ciudad de Guayaquil se encuentran instalados 2 Servidores y 4 Estaciones de Trabajo, de las cuales 2 son de escritorio y 2 son Laptop.

Activos de los que depende

- [L_SYT] UNIDAD DE SISTEMAS DE REDES Y COMUNICACIONES.
-

Activos que dependen de este

- [SWITCH_SYT] SWITCH

- [DESKTOP´_SYT] COMPUTADORAS DE ESCRITORIO
- [SCAN_SYT] SCANNER
- [PRINT1_SYT] IMPRESORAS MATRICIALES
- [PRINT2_SYT] IMPRESORA LASER

Valoración

Tabla 102

Valoración del activo Red Lan

DIMENSIÓN	VALOR	VALOR ACUMULADO
[D] DISPONIBILIDAD	[10](1)	[ ]

[10.olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística.

5.32 [WAN_SYT] RED WAN

- **[COM]** Comunicaciones
- **[COM.WAN]** Red de Área Amplia

Dominio de Seguridad

[BASE] SYTSA Transportes y Servicios Asociados

Datos

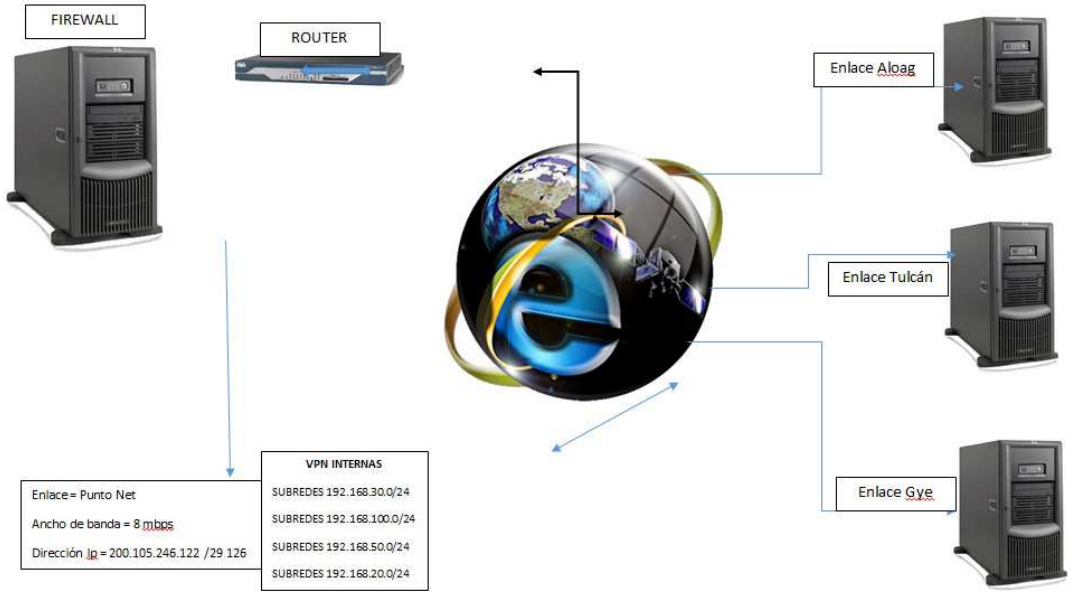


Figura 14 Esquema de la Red Wan de Sytsa

Descripción

La Empresa SYTSA cuenta con 1 enlace de Internet por Fibra Óptica de 8 Megas Sincrónico con tecnología de última milla de Fibra Óptica, además de un Backup de Enlace vía Radio manejando los mismos Anchos de Banda.

Activos de los que depende

- [L_SYT] UNIDAD DE SISTEMA DE REDES Y COMUNICACIONES
- [SS01_SYT] PUNTO NET

Activos que dependen de este

- [ROUTER_SYT] ROUTER
- [IEX_SYT] INTERNET

Valoración

Tabla 103

Valoración del activo Red Wan

DIMENSIÓN	VALOR	VALOR ACUMULADO
[D] DISPONIBILIDAD	[2](1)	[ ]

(1) [2.lg] Probablemente cause una pérdida menor de la confianza dentro de la organización.

5.33 [DISK_SYT] DISCO DURO

- **[SI]** Soporte de Información
- **[SI.ELECTRONICS]** Electrónicos
- **[SI.ELCTRONICS.DISK]** Discos

Dominio de Seguridad

[BASE] SYTSA Transportes y Servicios Asociados

Datos

Tabla 104

Datos del activo Disco Duro

MARCA	SEAGATE
TAMAÑO	1 TERA 5400 RPMS

Descripción

Disco Duros colocados en los servidores para respaldar la información, soporta RAID, el respaldo se lo realiza a diario

Valoración

Tabla 105

Valoración del activo Disco Duro

DIMENSIÓN	VALOR	VALOR ACUMULADO
[D] DISPONIBILIDAD	[3](1)	[ ]

(1) [3.olm] Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local).

5.34 [USB_SYT] DISPOSITIVOS USB

- **[SI]** Soporte de Información
- **[SI.LECTRONICS]** Electrónicos
- **[SI.LECTRONICS.USB]** Dispositivos USB

Dominio de Seguridad

[BASE] SYTSA Transportes y Servicios Asociados

Datos

Tabla 106

Datos del activo Dispositivos USB

MARCA	KINGSTON
TAMAÑO	8 GIGAS
CANTIDAD	20

Descripción

Se encuentran bajo la custodia del encargado de Sistemas, se las entrega bajo pedido.

Valoración

Tabla 107

Valoración del activo Dispositivos USB

DIMENSIÓN	VALOR	VALOR ACUMULADO
[D] DISPONIBILIDAD	[3](1)	[ ]

(1) [3.olm] Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local).

5.35 [UPS_SYT] SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA

[AUX] Elementos Auxiliares

[AUX.UPS] SAI Sistemas de Alimentación Ininterrumpida

Dominio de Seguridad

[BASE] SYTSA Transportes y Servicios Asociados

Datos

Tabla 108

Datos del activo Sistemas de Alimentación Ininterrumpida

UPS	TRIPLE LITE DE 3KVA

Descripción

Tiene un banco de baterías incorporado para soporte de 30 minutos para uso en los servidores. Está diseñado para manejar las interrupciones de corrientes y estabilizar la energía eléctrica y remover las interferencias.

Activos de los que depende

- [L_SYT] UNIDAD DE SISTEMA DE REDES Y COMUNICACIONES

Activos que dependen de este

- [WIFI_SYT] PUNTOS DE ACCESO WIRELESS
- [PABX_SYT] CENTRAL TELEFÓNICA
- [ROUTER_SYT] ROUTER
- [SWITCH_SYT] SWITCH
- [SBD_SYT] SERVIDOR DE BASE DE DATOS
- [SCAN_SYT] SCANNER
- [FIREWALL_SYT] FIREWALL
- [DESKTOP_SYT] COMPUTADORAS DE ESCRITORIO
- [LAPTOPS_SYT] COMPUTADORAS PORTÁTILES
- [PRINT1_SYT] IMPRESORAS MATRICIALES
- [PRINT2_SYT] IMPRESORA LASER

Valoración

Tabla 109

Valoración del activo Sistemas de Alimentación Ininterrumpida

DIMENSIÓN	VALOR	VALOR ACUMULADO
[D] DISPONIBILIDAD	[4](1)	[ ]

(1) [4.pi1] Información personal: probablemente afecte gravemente a un individuo.

5.36 [CCTV_SYT] CIRCUITO CERRADO DE TELEVISIÓN

- **[AUX]** Elementos Auxiliares
- **[AUX.OTHERS]** CCTV

Dominio de Seguridad

[BASE] SYTSA Transportes y Servicios Asociados

Datos

Tabla 110

Datos del activo Circuito cerrado de televisión

CAN	MARCA	MODELO	TIPO	CIUDAD	DETALLE	UBICACIÓN
1	HIKVISION	8 CH	DVR	QUITO	GRABADOR	SERVIDORES
1	STV	TV150	CÁMAR	QUITO	C.420 TVL	PATIO
1	STV	TV150	CÁMAR	QUITO	C. 420 TVL	TALLER
1	HK	ST	CÁMAR	QUITO	C. 500 TVL	BODEGA
1	STV	DOMO	CÁMAR	QUITO	C. 500 TVL	INGRESO POSTERIOR
1	HK	ST	CÁMAR	QUITO	C. 500 TVL	INGRESO
1	HIKVISION	4 CH	DVR	QUITO	GRABADOR	SERVIDORES
1	HIKVISION	4 CH	DVR	QUITO	GRABADOR	SERVIDORES
1	STV HIK	TV 150	CÁMAR	QUITO	C 420 TVL	PATIO

Descripción

Con el deseo de incrementar mayor seguridad en sus instalaciones y cumplir con los Estándares requeridos, SYTSA ha empezado a implementar el Sistema de Circuito Cerrado tanto en la Matriz como en las Sucursales. Se ha iniciado colocando los equipos en lugares específicos pero se está estudiando la necesidad de colocar en otros sitios que se han tornado estratégicos.

Activos de los que depende

- [L_SYT] UNIDAD DE SISTEMA DE REDES Y COMUNICACIONES

Valoración

Tabla 111

Valoración del activo Circuito cerrado de televisión

DIMENSIÓN	VALOR	VALOR ACUMULADO
[D] DISPONIBILIDAD	[4](1)	[4]

(1) [4.pi1] Información personal: probablemente afecte gravemente a un individuo.

(2) [4.crm] Dificulte la investigación o facilite la comisión de delitos.

5.37 [SISTEMA DE RASTREO_SYT] SISTEMA DE RASTREO

- **[AUX]** Elementos Auxiliares
- **[AUX.OTHERS]** Sistema de Rastreo

Dominio de Seguridad

[BASE] SYTSA Transportes y Servicios Asociados

Datos

Tabla 112

Datos del activo Sistema de rastreo

Modelo	ST1
Dimensiones (L x A x P)	87 x 48 x 26 mm
GSM Modulo	Quad-band 850/900/1800/1900 MHz
GPS Modulo	Alta sensibilidad GPS
Voltaje de funcionamiento	8V ~ 40V DC
Tipos de funcionamiento	3 modos – Normal, Dormir, Dormir
Memoria	profundamente
Entradas y salidas	2 MB
Serial Port	Entradas digitales x 2, Salidas digitales x 2
Sensor de movimiento	1 RS232 Puerto Serie
Reloj interno	Sensor de Shock
Carcasa	Incorporado
Temperatura de funcionamiento	ABS Alto impacto -20°C ~ +70°C
Batería	Interna
Antena GSM	Interna
Antena GPS	Externa

Descripción

Al momento SYTSA tiene contratado el Servicio de Rastreo Satelital en los Cabezales y Furgones.

Para cabezales está instalado el equipo ABORDO FM 3306-3316, es un computador de Abordo OBC de la gama 300 que cuenta con comunicación GPS y GSM con batería de respaldo, con comunicación a módulo electrónico de Motor (ECU) y 8 entradas análogas/digitales adicionales.

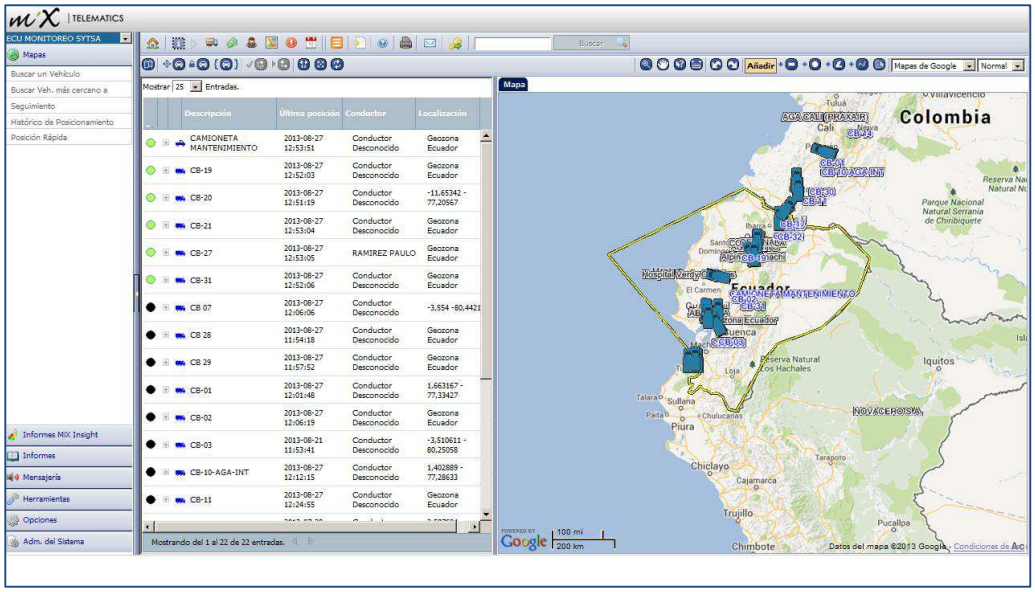


Figura 15. Sistema de Rastreo

Activos de los que depende

- [L_SYT] UNIDAD DE SISTEMA DE REDES Y COMUNICACIONES

Activos que dependen de este

- [TC_SYT] TRANSPORTE DE CARGA REFRIGERADA
- [AC_SYT] ALQUILER DE CONTENEDORES

Valoración

Tabla 113

Valoración del activo Sistema de rastreo

DIMENSIÓN	VALOR	VALOR ACUMULADO
[D] DISPONIBILIDAD	[4](1)	[ ]

(1) [4.crm] Dificulte la investigación o facilite la comisión de delitos.

5.38 [SS01_SYT] INTERNET PUNTO NET

[SS] Servicios Subcontratados
[SS.INTERNET] Internet

Dominio de Seguridad

[BASE] SYTSA Transportes y Servicios Asociados

Datos

Tabla 114

Datos del activo Internet Punto Net

QUITO	
PROVEEDOR	PUNTONET
TELÉFONO	1700786638
CONTACTO	FERNANDO RODRIGUEZ
ANCHO DE BANDA	8 MB 1a1
NÚMERO DE CONTRATO	
DIRECCIONES IP REALES	200.105.246.122 / 126
DESCRIPCIÓN ENLACE	DEDICADO USO EXCLUSIVO DEDICADO PARA CORREO Y SISTEMA CONTABLE
TECNOLOGÍA	FIBRA ÓPTICA Y RADIO

Descripción

Punto Net como Proveedor de Servicios de Internet da la siguiente infraestructura en la Matriz y sus sucursales.

- Soporte y Monitoreo de la Red bajo un esquema NX724X365
- Un Router CISCO 1800 Series.
- Caja Multimedia Patch Cord de Fibra Óptica.

Activos que dependen de este

- [WAN_SYT] RED WAN

Valoración

Tabla 115

Valoración del activo Internet Punto Net

DIMENSIÓN	VALOR	VALOR ACUMULADO
[D] DISPONIBILIDAD	[2](1)	[ ]

(1) [2.lg] Probablemente cause una pérdida menor de la confianza dentro de la organización.

5.39 [SS02_SYT] NIC EC

- **[SS]** Servicios Subcontratados
- **[SS.INTERNET]** Internet

Dominio de Seguridad

[BASE] SYTSA Transportes y Servicios Asociados

Datos

Tabla 116

Datos del activo NIC EC

QUITO	
PROVEEDOR	NIC EC
TELÉFONO	593 (4) 251-5912
CORREO	info@nic.ec
DOMINIO	WWW.SYTSA.COM.EC

Descripción

El registro de Nombres de Dominio bajo el CCTLD.EC es administrado por NIC.EC por delegación de ICANN a través de IANA. El dominio por el cual está registrado es www.sytsa.com.ec,

Activos que dependen de este

- [WEB_SYT] PORTAL WEB
- [ZM_SYT] SERVIDOR DE CORREO ELECTRÓNICO

Valoración

Tabla 117

Valoración del activo Nic Ec

DIMENSIÓN	VALOR	VALOR ACUMULADO
[D] DISPONIBILIDAD	[10](1)	[ ]

(1) [10.olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística.

5.40 [SS03_SYT] TELEFONÍA MOBIL

- **[SS]** Servicios Subcontratados
- **[SS.**MOBILE**]** Telefonía Móvil

Dominio de Seguridad

[BASE] SYTSA Transportes y Servicios Asociados

Descripción

SYTSA cuenta con un Plan de Telefonía Celular, distribuido al personal como una herramienta muy importante para el desarrollo del Negocio de la empresa es decir el Transporte y la Logística.

Valoración

Tabla 118

Valoración del activo Telefonía Móbil

DIMENSIÓN	VALOR	VALOR ACUMULADO
[D] DISPONIBILIDAD	[9](1)	[ ]

(1) [9.da] Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la organización con un serio impacto en otras organizaciones

5.41 [L_SYT] UNIDAD DE SISTEMA DE REDES Y COMUNICACIONES

- **[**L**.]** Infraestructura
- **[**L.BUILDING**]** Edificio

Dominio de Seguridad

[BASE] SYTSA Transportes y Servicios Asociados

Descripción

SYTSA está ubicado en Carcelén Diego de Vásquez N77-670, en la ciudad de Quito, al momento el lugar donde está ubicado el cuarto de servidores es en una habitación que comparte junto con el Departamento de Seguridad y Calidad.

Activos que dependen de este

- **[**PSTN_SYT] RED TELEFÓNICA
- **[**RADIO_SYT] RED INHALÁMBRICA
- [LAN_SYT] RED LAN
- **[**WAN_SYT] RED WAN
- **[**UPS_SYT] SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA
- **[**CCTV_SYT] CIRCUITO CERRADO DE TELEVISIÓN
- [SIS_RASTREO_SYT] SISTEMA DE RASTREO

Valoración

Tabla 119

Valoración del activo de la Unidad de Sistema de redes y comunicaciones.

DIMENSIÓN	VALOR	VALOR ACUMULADO
[D] DISPONIBILIDAD	[10](1)	[ ]

(1) [10.olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística.

5.42 [GER_SYT] RESPONSABLE DEL ÁREA DE SISTEMAS

- [P] Personal
- [P.ADM] Administrador del Sistema

Dominio de Seguridad

[BASE] SYTSA Transportes y Servicios Asociados

Descripción

La persona responsable del Área de Sistema es el Sr. Pablo Pesantez Navas

Valoración

Tabla 120

Valoración del activo Responsable del área del sistema

DIMENSIÓN	VALOR	VALOR ACUMULADO
[D] DISPONIBILIDAD	[7](1)	[ ]
[C] CONFIDENCIAL	[10] (2)	

(1) [7.da] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones.

[10.olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística.

5.43 [UI_SYT] SOPORTE DE USUARIOS

- [P] Personal
- [P.OP] Operadores

Dominio de Seguridad

[BASE] SYTSA Transportes y Servicios Asociados

Descripción

La persona responsable de ésta área es Roberto Pesantes

Valoración

Tabla 121

Valoración del activo Soporte de usuarios

DIMENSIÓN	VALOR	VALOR ACUMULADO
[D] DISPONIBILIDAD	[2](1)	[ ]

(1) [2.lg] Probablemente cause una pérdida menor de la confianza dentro de la organización.

5.44 [ITL_SYT] INFRAESTRUCTURA Y TELECOMUNICACIONES

- [P] Personal
- [P.COM] Administrador de Comunicaciones

Dominio de Seguridad

[BASE] SYTSA Transportes y Servicios Asociados

Descripción

La persona responsable de ésta área es Roberto Pesantes

Valoración

Tabla 122

Valoración del activo Infraestructura y telecomunicaciones

DIMENSIÓN	VALOR	VALOR ACUMULADO
[D] DISPONIBILIDAD	[2](1)	[ ]

(1). [2.lg] Probablemente cause una pérdida menor de la confianza dentro de la organización.

5.45 [DBA_SYT] ADMINISTRADOR DE LA BASE DE DATOS

- [P] Personal
- [P.ADM] Administrador de la Base de Datos

Dominio de Seguridad

[BASE] SYTSA Transportes y Servicios Asociados

Descripción

La persona responsable de ésta área es Freddy Constante

Valoración

Tabla 123

Valoración del activo Administrador de la base de datos

DIMENSIÓN	VALOR	VALOR ACUMULADO
[D] DISPONIBILIDAD	[2](1)	[ ]

(1). [2.lg] Probablemente cause una pérdida menor de la confianza dentro de la organización.

5.46 [SEG_SYT] SEGURIDAD Y CALIDAD

- [P] Personal
- [P.SEC] Administrador del Seguridad

Dominio de Seguridad

[BASE] SYTSA Transportes y Servicios Asociados

Descripción

La persona responsable de ésta área es Lauro Sánchez

Valoración

Tabla 124

Valoración del activo Seguridad y calidad

DIMENSIÓN	VALOR	VALOR ACUMULADO
[D] DISPONIBILIDAD	[1](1)	[ ]

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

5.47 [RASTREO_SYT] MONITOREO Y SOPORTE DE RASTREO

- [P] Personal
- [P.SEC] Administrador de Seguridad

Dominio de Seguridad

[BASE] SYTSA Transportes y Servicios Asociados

Descripción

La persona responsable de ésta área es Edgar Toalombo

Valoración

Tabla 125

Valoración del activo Monitoreo u soporte de rastreo

DIMENSIÓN	VALOR	VALOR ACUMULADO
[D] DISPONIBILIDAD	[1](1)	[ ]

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

ANEXO IV

MAPA DE RIESGOS

4.1 DATOS DEL PROYECTO

PROY_SYTSA	**DISEÑO DE UN SISTEMA DE GESTIÓN EN CONTROL Y SEGURIDAD**
DESCRIPCIÓN	Análisis a los Sistemas de Información
DIRECCIÓN	Carcelén, Diego Vásquez N77-670
TELÉFONO	2473006
RESPONSABLE	Erika Moncayo
EMPRESA	TRANSPORTES Y SERVICIOS ASOCIADOS SYTSA

Descripción:

El proyecto es elaborado en la Empresa Transportes y Servicios Asociados SYTSA, en la oficina Matriz en Quito

4.2 DIMENSIONES

- [D] Disponibilidad
- [I] Integridad en los Datos
- **[**C] Confidencialidad

4.3 AMENAZAS POR ACTIVO

Tabla 126

Amenazas del [TC_SYT] Transporte de Carga de Mercancía Refrigerada/Seca

AMENAZA	FRECUENCIA	[D]	[I]	[C]
[E1] Errores de los usuarios	12	50%		
[E2] Errores del administrador				
[E4] Errores de configuración				
[E9] Errores de [re-] encaminamiento				
[E10] Errores de secuencia				
[E24] Caída del sistema por agotamiento de recursos				
[A4] Manipulación de la configuración				
[A5] Suplantación de la identidad del usuario				
[A6] Abuso de privilegios de acceso				
[A7] Uso no previsto				
[A9] [Re-] encaminamiento de mensajes	4			50%
[A10] Alteración de secuencia				
[A11] Acceso no autorizado				
[A24] Denegación de servicio				

Tabla 127

Amenazas del [AC_SYT] Alquiler de Contenedores

AMENAZA	FRECUENCIA	[D]	[I]	[C]
[E1] Errores de los usuarios	12	50%		
[A9] [Re-] encaminamiento de mensajes	4			50%
[A10] Alteración de secuencia				
[A11] Acceso no autorizado				
[A24] Denegación de servicio				

Tabla 128

Amenazas del [SMD_SYT] Servicio de Montaje y Desmontaje

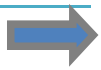
AMENAZA	FRECUENCIA	[D]	[I]	[C]
[E1] Errores de los usuarios	12	50%		
[E2] Errores del administrador				
[E4] Errores de configuración				
[E9] Errores de [re-] encaminamiento				
[E10] Errores de secuencia				
[E24] Caída del sistema por agotamiento de recursos				
[A4] Manipulación de la configuración				
[A5] Suplantación de la identidad del usuario				
[A6] Abuso de privilegios de acceso				
[A7] Uso no previsto				
[A9] [Re-] encaminamiento de mensajes	4			50%
[A10] Alteración de secuencia				
[A11] Acceso no autorizado				
[A24] Denegación de servicio				

Tabla 129

Amenazas del [WEB_SYT] Portal Web

AMENAZA	FRECUENCIA	[D]	[I]	[C]
[E1] Errores de los usuarios				
[E2] Errores del administrador				
[E4] Errores de configuración				
[E9] Errores de [re-] encaminamiento				
[E10] Errores de secuencia				
[E24] Caída del sistema por agotamiento de recursos	2	25%	25%	25%

Continúa



AMENAZA	FRECUENCIA	[D]	[I]	[C]
[A4] Manipulación de la configuración				
[A5] Suplantación de la identidad del usuario				
[A6] Abuso de privilegios de acceso				
[A7] Uso no previsto	2	25%		
[A9] [Re-] encaminamiento de mensajes				
[I8] Fallo de los servicios de comunicaciones	2	25%		
[I6] Corte del suministro eléctrico	2	25%		
[I5] Avería de origen físico o lógico	2	25%		

Tabla 130

Amenazas del [ZM_SYT] Servidor de Correo Electrónico ZIMBRA

AMENAZA	FRECUENCIA	[D]	[I]	[C]
[E1] Errores de los usuarios	12	25%		
[E2] Errores del administrador				
[E4] Errores de configuración				
[E9] Errores de [re-] encaminamiento				
[E10] Errores de secuencia				
[E14] Escapes de Información	2			25 %
[E21] Errores de mantenimiento/actualiz progra (software)	2			25 %
[A4] Manipulación de la configuración				
[A5] Suplantación de la identidad del usuario	2			25 %
[A6] Abuso de privilegios de acceso				
[A9] [Re-] encaminamiento de mensajes				
[A10] Alteración de secuencia				
[I6] Corte del suministro eléctrico	2	25%		

Tabla 131

Amenazas de [IP_SYT] Telefonía IP

AMENAZA	FRECUENCIA	[D]	[I]	[C]
[E1] Errores de los usuarios	2	25%	25%	25%
[E2] Errores del administrador				
[E4] Errores de configuración	2	25%	25%	25%
[E9] Errores de [re-] encaminamiento	2		25%	25%
[E10] Errores de secuencia				
E21] Errores de mantenimiento/actualiz progra (software)	2	25%	25%	
[A4] Manipulación de la configuración				
[A5] Suplantación de la identidad del usuario				
[A6] Abuso de privilegios de acceso				
[A7] Uso no previsto				
[A9] [Re-] encaminamiento de mensajes				
[A10] Alteración de secuencia				
[A11] Acceso no autorizado	2		25%	25%
[A24] Denegación de servicio				

Tabla 132

Amenazas de [BACKUP_SYT] Servicio de copias de respaldo

AMENAZA	FRECUENCIA	[D]	[I]	[C]
[E1] Errores de los usuarios	2	25%	25%	
[E2] Errores del administrador				
[E4] Errores de configuración	2	25%	25%	25%
[E9] Errores de [re-] encaminamiento				
[E10] Errores de secuencia				

Continúa 

AMENAZA	FRECUENCIA	[D]	[I]	[C]
[E15] Alteración de la información	2	25%		
[I8] Fallo de los servicios de comunicaciones				
[A5] Suplantación de la identidad del usuario				
[A6] Abuso de privilegios de acceso				
[A7] Uso no previsto				
[A9] [Re-] encaminamiento de mensajes				
[A10] Alteración de secuencia				
[A11] Acceso no autorizado				
[A24] Denegación de servicio	2	25%		

Tabla 133

Amenazas de [INF_SYT] Información de Logística

AMENAZA	FRECUENCIA	[D]	[I]	[C]
[E1] Errores de los usuarios	2	25%	25%	
[E2] Errores del administrador				
[E3] Errores de monitorización (log)	2	25%	25%	25%
[E14] Escapes de información				
[E15] Alteración de la información	2		50%	
[E16] Introducción de información incorrecta	12		50%	
[E17] Degradación de la información				
[E18] Destrucción de información	2	25%		
[A4] Manipulación de la configuración				
[A11] Acceso no autorizado	2		25%	25%
[A14] Interceptación de información (escucha)				
[A15] Modificación de la información	2		50%	
[A16] Introducción de falsa información				
[A17] Corrupción de la información				
[A18] Destrucción de la información				

Tabla 134

Amenazas de [INT_SYT] Información por cada Departamento

AMENAZA	FRECUENCIA	[D]	[I]	[C]
[E1] Errores de los usuarios	4	50%	50&	
[E2] Errores del administrador				
[E3] Errores de monitorización (log)				
[E14] Escapes de información				
[E15] Alteración de la información	2		50%	
[E16] Introducción de información incorrecta	12		50%	
[E17] Degradación de la información				
[E18] Destrucción de información				
[A4] Manipulación de la configuración				
[A11] Acceso no autorizado	2		25%	25%
[A14] Interceptación de información (escucha)				
[A15] Modificación de la información	2		50%	
[A16] Introducción de falsa información				
[A17] Corrupción de la información				
[A18] Destrucción de la información				

Tabla 135

Amenazas de [LOG_SYT] Información de Registros de ingreso sobre los servidores

AMENAZA	FRECUENCIA	[D]	[I]	[C]
[E1] Errores de los usuarios				
[E2] Errores del administrador	12	25%	25%	25%
[E3] Errores de monitorización (log)	12	50%	50%	50%
[E14] Escapes de información				

Continúa

AMENAZA	FRECUENCIA	[D]	[I]	[C]
[E15] Alteración de la información				
[E16] Introducción de información incorrecta				
[E17] Degradación de la información	2		25%	
[E18] Destrucción de información	1	25%		
[A4] Manipulación de la configuración	12	25%	25%	25%
[A11] Acceso no autorizado	4		25%	25%
[A14] Interceptación de información (escucha)				
[A15] Modificación de la información				
[A16] Introducción de falsa información				
[A17] Corrupción de la información				
[A18] Destrucción de la información				

Tabla 136

Amenazas de [PER_M_SYT] Información personal de cada usuario

AMENAZA	FRECUENCIA	[D]	[I]	[C]
[E1] Errores de los usuarios	4	10%	10%	10%
[E2] Errores del administrador				
[E3] Errores de monitorización (log)				
[E14] Escapes de información				
[E15] Alteración de la información				
[E16] Introducción de información incorrecta	4	10%	10%	10%
[E17] Degradación de la información				
[A11] Acceso no autorizado				
[A14] Interceptación de información (escucha)				
[A15] Modificación de la información	4	10%	10%	10%
[A16] Introducción de falsa información				
[A17] Corrupción de la información				
[A18] Destrucción de la información				

Tabla 137

Amenazas del [NIGISU_ SYT] Sistema Financiero NIGISU

AMENAZA	FRECUENCIA	[D]	[I]	[C]
[E1] Errores de los usuarios	4	25%	25%	
[E2] Errores del administrador				
[E4] Errores de configuración				
[E8] Difusión de software dañino				
[E9] Errores de [re-] encaminamiento				
[E10] Errores de secuencia				
[E14] Escapes de información				
[E20] Vulnerabilidad de los programas (software)				
[E21] Errores de mantenimiento/actualiza de prog	4	25%	25%	
[A4] Manipulación de la configuración				
[A5] Suplantación de la identidad del usuario				
[A6] Abuso de privilegios de acceso				
[A7] Uso no previsto				
[A8] Difusión de software dañino				
[A9] [Re-] encaminamiento de mensajes				
[A15] Modificación de la información	4		25%	
[A16] Introducción de falsa información	4		25%	
[I6] Cortes de Suministro eléctrico	2	25%		
[I8] Fallo de los servicios de comunicaciones	4	50%		

Tabla 138

Amenazas de la [OFF_SYT] Ofimática

AMENAZA	FRECUENCIA	[D]	[I]	[C]
[E1] Errores de los usuarios	4	25%	25%	
[E2] Errores del administrador				
[E4] Errores de configuración				
[E8] Difusión de software dañino				
[E9] Errores de [re-] encaminamiento				
[E10] Errores de secuencia				
[E14] Escapes de información				
[E20] Vulnerabilidad de los programas (software)				
[E21] Errores de mantenimiento/actualiza de prog	4	25%	25%	
[A4] Manipulación de la configuración				
[A5] Suplantación de la identidad del usuario				
[A6] Abuso de privilegios de acceso				
[A7] Uso no previsto				
[A8] Difusión de software dañino				
[A9] [Re-] encaminamiento de mensajes				
[A10] Alteración de secuencia				
[A11] Acceso no autorizado				
[I5] Avería de origen físico o lógico	4	25%		
[I6] Corte del suministro eléctrico	4	25%		

Tabla 139

Amenazas del [AV_SYT] Antivirus

AMENAZA	FRECUENCIA	[D]	[I]	[C]
[E1] Errores de los usuarios	4	25%	25%	
[E2] Errores del administrador				
[E4] Errores de configuración				
[E8] Difusión de software dañino				
[E9] Errores de [re-] encaminamiento				
[E10] Errores de secuencia				
[E14] Escapes de información				
[E20] Vulnerabilidad de los programas (software)				
[E21] Errores de mantenimiento/actualiza de prog	4	25%	25%	
[A4] Manipulación de la configuración	1	25%	25%	25%
[A5] Suplantación de la identidad del usuario				
[A6] Abuso de privilegios de acceso				
[A7] Uso no previsto				
[A8] Difusión de software dañino	4	25%	25%	25%
[A9] [Re-] encaminamiento de mensajes				
[I5] Avería de origen físico o lógico	4	25%		
[A11] Acceso no autorizado				
[A14] Interceptación de información (escucha)				
[A22] Manipulación de programas				

Tabla 140

Amenazas de[OTR_SYT] Otro software

AMENAZA	FRECUENCIA	[D]	[I]	[C]
[E1] Errores de los usuarios	4	25%	25%	
[E2] Errores del administrador				
[E4] Errores de configuración				
[E8] Difusión de software dañino				
[E9] Errores de [re-] encaminamiento				
[E10] Errores de secuencia				
[E14] Escapes de información				
[E20] Vulnerabilidad de los programas (software)				
[E21] Errores de mantenimiento/actualiza de prog	4	25%	25%	
[A4] Manipulación de la configuración	4	25%		
[A5] Suplantación de la identidad del usuario				
[A6] Abuso de privilegios de acceso				
[A7] Uso no previsto				
[A8] Difusión de software dañino				
[A9] [Re-] encaminamiento de mensajes				
[A10] Alteración de secuencia				
[A11] Acceso no autorizado				
[A14] Interceptación de información (escucha)				
[A22] Manipulación de programas				

Tabla 141

Amenazas del [IEX_INTERNET] Internet

AMENAZA	FRECUENCIA	[D]	[I]	[C]
[E1] Errores de los usuarios				
[E2] Errores del administrador				
[E4] Errores de configuración	2	25%	25%	25%
[E8] Difusión de software dañino				
[E9] Errores de [re-] encaminamiento				
[E10] Errores de secuencia				
[E14] Escapes de información				
[E20] Vulnerabilidad de los programas (software)				
[E21] Errores de mantenimiento/actualiza de prog				
[I6] Cortes de Suministro eléctrico	2	25%		
[A5] Suplantación de la identidad del usuario				
[A6] Abuso de privilegios de acceso				
[A7] Uso no previsto				
[A8] Difusión de software dañino	2	25%	25%	25%
[A9] [Re-] encaminamiento de mensajes				
[A10] Alteración de secuencia				
[A11] Acceso no autorizado	4		25%	25%
[A14] Interceptación de información (escucha)				
[A22] Manipulación de programas	4		25%	25%

Tabla 142

Amenazas del [SBD_SYT] Servidor de Datos

AMENAZA	FRECUENCIA	[D]	[I]	[C]
[N1] Fuego				
[N2] Daños por Agua				
[N*] Desastres Naturales				
[I1] Fuego	1	50%		
[I2] Daños por agua				
[I*] Desastres industriales	2	50%		
[I3] Contaminación mecánica	12	50%		
[I4] Contaminación electromagnética	4	50%		
[I5] Avería de origen físico o lógico	4	50%		
[I6] Corte del suministro eléctrico				
[I7] Condiciones inadecuadas de temperatura y/o humedad	4	50%		
[E2] Errores del administrador				
[E4] Errores de configuración				
[E23] Errores de mantenimiento/actualiz progr				
[E24] Caída del sistema por agotamiento de recursos	4	50%		
[A4] Manipulación de la configuración				
[A6] Abuso de privilegios de acceso				
[A7] Uso no previsto				
[A11] Acceso no autorizado	4			50%
[A24] Denegación de servicio				
[A25] Robo				
[A26] Ataque destructivo				
[A27] Ocupación enemiga				

Tabla 143

Amenazas del [FIREWALL] Firewall

AMENAZA	FRECUENCIA	[D]	[I]	[C]
[N1] Fuego				
[N2] Daños por Agua				
[N*] Desastres Naturales				
[I1] Fuego				
[I2] Daños por agua				
[I*] Desastres industriales	2	50%		
[I3] Contaminación mecánica	12	50%		
[I4] Contaminación electromagnética	4	50%		
[I5] Avería de origen físico o lógico	4	50%		
[I6] Corte del suministro eléctrico				
[I7] Condiciones inadecuadas de temperatura y/o humedad	4	50%		
[E2] Errores del administrador				
[E4] Errores de configuración				
[E23] Errores de mantenimiento/actualiz progr	2	25%		
[E24] Caída del sistema por agotamiento de recursos	2	25%		
[A4] Manipulación de la configuración				
[A6] Abuso de privilegios de acceso				
[A7] Uso no previsto				
[A11] Acceso no autorizado				
[A24] Denegación de servicio	1	50%		
[A25] Robo				
[A26] Ataque destructivo				
[A27] Ocupación enemiga				

Tabla 144

Amenazas de [DESKTOP_SYT] Computadoras de Escritorio

AMENAZA	FRECUENCIA	[D]	[I]	[C]
[N1] Fuego				
[N2] Daños por Agua				
[N*] Desastres Naturales				
[I1] Fuego	2	25%		
[I2] Daños por agua	2	25%		
[I*] Desastres industriales				
[I3] Contaminación mecánica	4	50%		
[I4] Contaminación electromagnética	4	50%		
[I5] Avería de origen físico o lógico	4	50%		
[I6] Corte del suministro eléctrico	2	25%		
[I7] Condiciones inadecuadas de temperatura y/o humedad				
[E2] Errores del administrador				
[E4] Errores de configuración				
[E23] Errores de mantenimiento/actualiz progr				
[E24] Caída del sistema por agotamiento de recursos				
[A4] Manipulación de la configuración	2	25%	25%	25%
[A6] Abuso de privilegios de acceso				
[A7] Uso no previsto				
[A11] Acceso no autorizado				
[A24] Denegación de servicio				
[A25] Robo	1	100%		100%
[A26] Ataque destructivo	1	25%		
[A27] Ocupación enemiga				

Tabla 145

Amenazas de las [LAPTOPS_SYT] Computadoras Portátiles

AMENAZA	FRECUENCIA	[D]	[I]	[C]
[N1] Fuego				
[N2] Daños por Agua				
[N*] Desastres Naturales				
[I1] Fuego				
[I2] Daños por agua	2	50%		
[I*] Desastres industriales				
[I3] Contaminación mecánica				
[I4] Contaminación electromagnética				
[I5] Avería de origen físico o lógico	2	50%		
[I6] Corte del suministro eléctrico				
[I7] Condiciones inadecuadas de temperatura y/o humedad	4	50%		
[E1] Errores del usuario	4	25%		
[E4] Errores de configuración				
[E8] Difusión de software dañino	4	25%		
[E23] Errores de mantenimiento/actualiz progr				
[E24] Caída del sistema por agotamiento de recursos				
[A4] Manipulación de la configuración	4	25%		
[A6] Abuso de privilegios de acceso				
[A7] Uso no previsto				
[A11] Acceso no autorizado				
[A24] Denegación de servicio				
[A25] Robo	4	80%		80%
[A26] Ataque destructivo				
[A27] Ocupación enemiga				

Tabla 146

Amenazas del [SCAN_SYT] Scanner

AMENAZA	FRECUENCIA	[D]	[I]	[C]
[N1] Fuego				
[N2] Daños por Agua				
[N*] Desastres Naturales				
[I1] Fuego				
[I2] Daños por agua				
[I*] Desastres industriales				
[I3] Contaminación mecánica				
[I4] Contaminación electromagnética				
[I5] Avería de origen físico o lógico	4	25%		
[I6] Corte del suministro eléctrico	4	25%		
[I7] Condiciones inadecuadas de temperatura y/o humedad				
[E2] Errores del administrador				
[E4] Errores de configuración	2	25%		
[E23] Errores de mantenimiento/actualiz progr				
[E24] Caída del sistema por agotamiento de recursos				
[A4] Manipulación de la configuración	2	25%	25%	25%
[A6] Abuso de privilegios de acceso				
[A7] Uso no previsto				
[A11] Acceso no autorizado				
[A24] Denegación de servicio				
[A25] Robo				
[A26] Ataque destructivo				
[A27] Ocupación enemiga				

Tabla 147

Amenazas de las [PRINT1_SYT] Impresoras Matriciales

AMENAZA	FRECUENCIA	[D]	[I]	[C]
[N1] Fuego				
[N2] Daños por Agua				
[N*] Desastres Naturales				
[I1] Fuego				
[I2] Daños por agua				
[I*] Desastres industriales				
[I3] Contaminación mecánica				
[I4] Contaminación electromagnética				
[I5] Avería de origen físico o lógico	4	25%		
[I6] Corte del suministro eléctrico	4	25%		
[I7] Condiciones inadecuadas de temperatura y/o humedad				
[E2] Errores del administrador				
[E4] Errores de configuración	8	25%		
[E23] Errores de mantenimiento/actualiz progr	2	25%		
[E24] Caída del sistema por agotamiento de recursos				
[A4] Manipulación de la configuración	8	25%		
[A6] Abuso de privilegios de acceso				
[A7] Uso no previsto				
[A11] Acceso no autorizado				
[A24] Denegación de servicio				
[A25] Robo				
[A26] Ataque destructivo				
[A27] Ocupación enemiga				

Tabla 148

Amenazas de la [PRINT2_SYT] Impresora Laser

AMENAZA	FRECUENCIA	[D]	[I]	[C]
[N1] Fuego				
[N2] Daños por Agua				
[N*] Desastres Naturales				
[I1] Fuego				
[I2] Daños por agua				
[I*] Desastres industriales				
[I3] Contaminación mecánica				
[I4] Contaminación electromagnética				
[I5] Avería de origen físico o lógico	4	25%		
[I6] Corte del suministro eléctrico	4	25%		
[I7] Condiciones inadecuadas de temperatura y/o humedad				
[E2] Errores del administrador				
[E4] Errores de configuración	4	25%		
[E23] Errores de mantenimiento/actualiz progr	2	25%		
[E24] Caída del sistema por agotamiento de recursos				
[A4] Manipulación de la configuración	4	25%		
[A6] Abuso de privilegios de acceso				
[A7] Uso no previsto				
[A11] Acceso no autorizado				
[A24] Denegación de servicio				
[A25] Robo				
[A26] Ataque destructivo				
[A27] Ocupación enemiga				

Tabla 149

Amenazas del [SWITCH_SYT] Switch

AMENAZA	FRECUENCIA	[D]	[I]	[C]
[N1] Fuego				
[N2] Daños por Agua				
[N*] Desastres Naturales				
[I1] Fuego				
[I2] Daños por agua	4	25%		
[I*] Desastres industriales				
[I3] Contaminación mecánica				
[I4] Contaminación electromagnética				
[I5] Avería de origen físico o lógico	4	25%		
[I6] Corte del suministro eléctrico	4	25%		
[I7] Condiciones inadecuadas de temperatura y/o humedad	4	25%		
[E2] Errores del administrador				
[E4] Errores de configuración				
[E23] Errores de mantenimiento/actualiz progr				
[E24] Caída del sistema por agotamiento de recursos				
[A4] Manipulación de la configuración				
[A6] Abuso de privilegios de acceso				
[A7] Uso no previsto				
[A11] Acceso no autorizado				
[A24] Denegación de servicio				
[A25] Robo				
[A26] Ataque destructivo				
[A27] Ocupación enemiga				

Tabla 150

Amenazas del [ROUTER_SYT] Router

AMENAZA	FRECUENCIA	[D]	[I]	[C]
[N1] Fuego				
[N2] Daños por Agua				
[N*] Desastres Naturales				
[I1] Fuego				
[I2] Daños por agua	4	25%		
[I*] Desastres industriales				
[I3] Contaminación mecánica				
[I4] Contaminación electromagnética				
[I5] Avería de origen físico o lógico	4	25%		
[I6] Corte del suministro eléctrico	4	25%		
[I7] Condiciones inadecuadas de temperatura y/o humedad				
[E2] Errores del administrador				
[E4] Errores de configuración	1	25%	25%	25%
[E23] Errores de mantenimiento/actualiz progr				
[E24] Caída del sistema por agotamiento de recursos				
[A4] Manipulación de la configuración				
[A6] Abuso de privilegios de acceso				
[A7] Uso no previsto				
[A11] Acceso no autorizado				
[A24] Denegación de servicio				
[A25] Robo				
[A26] Ataque destructivo				
[A27] Ocupación enemiga				

Tabla 151

Amenazas del [GTWY_SYT] Gateway

AMENAZA	FRECUENCIA	[D]	[I]	[C]
[N1] Fuego				
[N2] Daños por Agua				
[N*] Desastres Naturales				
[I1] Fuego				
[I2] Daños por agua				
[I*] Desastres industriales	2	50%		
[I3] Contaminación mecánica	12	50%		
[I4] Contaminación electromagnética	4	50%		
[I5] Avería de origen físico o lógico	4	50%		
[I6] Corte del suministro eléctrico				
[I7] Condiciones inadecuadas de temperatura y/o humedad	4	50%		
[E2] Errores del administrador				
[E4] Errores de configuración				
[E23] Errores de mantenimiento/actualiz progr	2	25%		
[E24] Caída del sistema por agotamiento de recursos	2	25%		
[A4] Manipulación de la configuración				
[A6] Abuso de privilegios de acceso				
[A7] Uso no previsto				
[A11] Acceso no autorizado				
[A24] Denegación de servicio	1	50%		
[A25] Robo				
[A26] Ataque destructivo				
[A27] Ocupación enemiga				

Tabla 152

Amenazas de los [WIFI_SYT] Puntos de Acceso Wireless

AMENAZA	FRECUENCIA	[D]	[I]	[C]
[N1] Fuego				
[N2] Daños por Agua				
[N*] Desastres Naturales				
[I1] Fuego				
[I2] Daños por agua	2	25%		
[I*] Desastres industriales				
[I3] Contaminación mecánica				
[I4] Contaminación electromagnética				
[I5] Avería de origen físico o lógico	2	25%		
[I6] Corte del suministro eléctrico	4	25%		
[I7] Condiciones inadecuadas de temperatura y/o humedad	2	25%		
[E2] Errores del administrador				
[E4] Errores de configuración	2	25%		
[E23] Errores de mantenimiento/actualiz progr				
[E24] Caída del sistema por agotamiento de recursos				
[A4] Manipulación de la configuración	2	25%		
[A6] Abuso de privilegios de acceso				
[A7] Uso no previsto				
[A11] Acceso no autorizado				
[A24] Denegación de servicio				
[A25] Robo				
[A26] Ataque destructivo				
[A27] Ocupación enemiga				

Tabla 153

Amenazas de la [PABX_SYTS] Central Telefónica

AMENAZA	FRECUENCIA	[D]	[I]	[C]
[N1] Fuego				
[N2] Daños por Agua				
[N*] Desastres Naturales				
[I1] Fuego				
[I2] Daños por agua				
[I*] Desastres industriales				
[I3] Contaminación mecánica				
[I4] Contaminación electromagnética				
[I5] Avería de origen físico o lógico	2	25%		
[I6] Corte del suministro eléctrico	4	25%		
[I7] Condiciones inadecuadas de temperatura y/o humedad	2	25%		
[E2] Errores del administrador				
[E4] Errores de configuración	2	25%		
[E23] Errores de mantenimiento/actualiz progr				
[E24] Caída del sistema por agotamiento de recursos				
[A4] Manipulación de la configuración	2	25%		
[A6] Abuso de privilegios de acceso				
[A7] Uso no previsto				
[A11] Acceso no autorizado				
[A24] Denegación de servicio				
[A25] Robo				
[A26] Ataque destructivo				
[A27] Ocupación enemiga				

Tabla 154

Amenazas de la [PSTN_SYT] Red Telefónica

AMENAZA	FRECUENCIA	[D]	[I]	[C]
[N1] Fuego				
[N2] Daños por Agua				
[N*] Desastres Naturales				
[I1] Fuego				
[I2] Daños por agua	2	25%		
[I*] Desastres industriales				
[I3] Contaminación mecánica				
[I4] Contaminación electromagnética				
[I5] Avería de origen físico o lógico	2	25%		
[I6] Corte del suministro eléctrico	4	25%		
[I7] Condiciones inadecuadas de temperatura y/o humedad				
[I8]				
[E2] Errores del administrador				
[E4] Errores de configuración				
[E9] Errores de [re-] encaminamiento				
[E10] Errores de secuencia				
[E14] Escapes de información				
[E24] Caída del sistema por agotamiento de recursos				
[A4] Manipulación de la configuración	2	25%		
[A5] Suplantación de la identidad del usuario				
[A6] Abuso de privilegios de acceso				
[A7] Uso no previsto				
[A9] [Re-] encaminamiento de mensajes				
[A10] Alteración de secuencia				
[A11] Acceso no autorizado				
[A12] Análisis de tráfico				

Tabla 155

Amenazas de la [RADIO_SYT] RED WIFI

AMENAZA	FRECUENCIA	[D]	[I]	[C]
[N1] Fuego				
[N2] Daños por Agua				
[N*] Desastres Naturales				
[I1] Fuego				
[I2] Daños por agua	2	25%		
[I*] Desastres industriales				
[I3] Contaminación mecánica				
[I4] Contaminación electromagnética				
[I5] Avería de origen físico o lógico	2	25%		
[I6] Corte del suministro eléctrico	4	25%		
[I7] Condiciones inadecuadas de temperatura y/o humedad				
[I8]				
[E2] Errores del administrador				
[E4] Errores de configuración				
[E9] Errores de [re-] encaminamiento				
[E10] Errores de secuencia				
[E14] Escapes de información				
[E24] Caída del sistema por agotamiento de recursos				
[A4] Manipulación de la configuración	2	25%		
[A5] Suplantación de la identidad del usuario				
[A6] Abuso de privilegios de acceso				
[A7] Uso no previsto				
[A9] [Re-] encaminamiento de mensajes				
[A10] Alteración de secuencia				
[A11] Acceso no autorizado				
[A12] Análisis de tráfico				

Tabla 156

Amenazas de la [LAN_SYT] Red LAN

AMENAZA	FRECUENCIA	[D]	[I]	[C]
[N1] Fuego				
[N2] Daños por Agua				
[N*] Desastres Naturales				
[I1] Fuego				
[I2] Daños por agua	4	25%		
[I*] Desastres industriales				
[I3] Contaminación mecánica				
[I4] Contaminación electromagnética	4	25%		
[I5] Avería de origen físico o lógico	4	25%		
[I6] Corte del suministro eléctrico	4	25%		
[I7] Condiciones inadecuadas de temperatura y/o humedad	4	25%		
[I8]				
[E2] Errores del administrador				
[E4] Errores de configuración	2	25%	25%	25%
[E9] Errores de [re-] encaminamiento				
[E10] Errores de secuencia	2		25%	
[E14] Escapes de información				
[E24] Caída del sistema por agotamiento de recursos				
[A4] Manipulación de la configuración				
[A5] Suplantación de la identidad del usuario				
[A6] Abuso de privilegios de acceso				
[A7] Uso no previsto				
[A9] [Re-] encaminamiento de mensajes				
[A10] Alteración de secuencia				
[A11] Acceso no autorizado				
[A12] Análisis de tráfico				

Tabla 157

Amenazas de la [WAN_SYT] Red WAN

AMENAZA	FRECUENCIA	[D]	[I]	[C]
[N1] Fuego				
[N2] Daños por Agua				
[N*] Desastres Naturales				
[I1] Fuego				
[I2] Daños por agua	4	25%		
[I*] Desastres industriales				
[I3] Contaminación mecánica				
[I4] Contaminación electromagnética				
[I5] Avería de origen físico o lógico	2	25%		
[I6] Corte del suministro eléctrico	4	25%		
[I7] Condiciones inadecuadas de temperatura y/o humedad				
[I8]				
[E2] Errores del administrador				
[E4] Errores de configuración	4	25%		
[E9] Errores de [re-] encaminamiento				
[E10] Errores de secuencia	4	25%		
[E14] Escapes de información				
[E24] Caída del sistema por agotamiento de recursos				
[A4] Manipulación de la configuración				
[A5] Suplantación de la identidad del usuario				
[A6] Abuso de privilegios de acceso				
[A7] Uso no previsto				
[A9] [Re-] encaminamiento de mensajes				
[A10] Alteración de secuencia				
[A11] Acceso no autorizado				

Tabla 158

Amenazas de los [DISK_SYT] Discos

AMENAZA	FRECUENCIA	[D]	[I]	[C]
[N1] Fuego				
[N2] Daños por Agua				
[N*] Desastres Naturales				
[I1] Fuego				
[I2] Daños por agua				
[I*] Desastres industriales				
[I3] Contaminación mecánica				
[I4] Contaminación electromagnética				
[I5] Avería de origen físico o lógico	1	25%		
[I6] Corte del suministro eléctrico				
[I7] Condiciones inadecuadas de temperatura y/o humedad				
[I10] Degradación de los soportes de almacenamiento de la información	1	25%		
[A7] Uso no previsto				
[A11] Acceso no autorizado				
[A25] Robo de equipos				
[A26] Ataque destructivo				
[A27] Ocupación enemiga				

Tabla 159

Amenazas de los [USB_SYT] Dispositivos USB

AMENAZA	FRECUENCIA	[D]	[I]	[C]
[N1] Fuego				
[N2] Daños por Agua				
[N*] Desastres Naturales				
[I1] Fuego				
[I2] Daños por agua				
[I*] Desastres industriales				
[I3] Contaminación mecánica				
[I4] Contaminación electromagnética				
[I5] Avería de origen físico o lógico	1	25%		
[I6] Corte del suministro eléctrico				
[I7] Condiciones inadecuadas de temperatura y/o humedad				
[I10] Degradación de los soportes de almacenamiento de la información	1	25%		
[A7] Uso no previsto				
[A11] Acceso no autorizado				
[A25] Robo de equipos				
[A26] Ataque destructivo				
[A27] Ocupación enemiga				

Tabla 160

Amenazas de los [UPS_SYT] Sistemas de Alimentación Ininterrumpida

AMENAZA	FRECUENCIA	[D]	[I]	[C]
[N1] Fuego				
[N2] Daños por Agua				
[N*] Desastres Naturales				
[I1] Fuego				
[I2] Daños por agua	2	25%		
[I*] Desastres industriales				
[I3] Contaminación mecánica				
[I4] Contaminación electromagnética	4	25%		
[I5] Avería de origen físico o lógico	4	25%		
[I6] Corte del suministro eléctrico	4	25%		
[I7] Condiciones inadecuadas de temperatura y/o humedad	4	25%		
[I9] Interrupción de otros servicios y suministros esenciales				
[A7] Uso no previsto				
[A11] Acceso no autorizado				
[A25] Robo de equipos				
[A26] Ataque destructivo				
[A27] Ocupación enemiga				

Tabla 161

Amenazas del [CCTV_SYT] Circuito Cerrado de Televisión

AMENAZA	FRECUENCIA	[D]	[I]	[C]
[N1] Fuego				
[N2] Daños por Agua	2	25%		
[N*] Desastres Naturales				
[I1] Fuego				
[I2] Daños por agua				
[I*] Desastres industriales				
[I3] Contaminación mecánica	2	25%		
[I4] Contaminación electromagnética				
[I5] Avería de origen físico o lógico	4	25%		
[I6] Corte del suministro eléctrico	4	25%		
[I7] Condiciones inadecuadas de temperatura y/o humedad	2	25%		
[I9] Interrupción de otros servicios y suministros esenciales				
[A7] Uso no previsto				
[A11] Acceso no autorizado	1		25%	25%
[A25] Robo de equipos				
[A26] Ataque destructivo				
[A27] Ocupación enemiga				

Tabla 162

Amenazas del [RASTREO_SYT] Sistema de Rastreo

AMENAZA	FRECUENCIA	[D]	[I]	[C]
[N1] Fuego				
[N2] Daños por Agua				
[N*] Desastres Naturales				
[I1] Fuego				
[I2] Daños por agua	4	25%		
[I*] Desastres industriales				
[I3] Contaminación mecánica				
[I4] Contaminación electromagnética				
[I5] Avería de origen físico o lógico	4	25%		
[I6] Corte del suministro eléctrico	4	255		
[I7] Condiciones inadecuadas de temperatura y/o humedad	4	25%		
[I9] Interrupción de otros servicios y suministros esenciales	4	25%		
[A7] Uso no previsto	4	25%		
[A11] Acceso no autorizado	4		25%	25%
[A25] Robo de equipos				
[A26] Ataque destructivo	4	25%		
[A27] Ocupación enemiga				

Tabla 163

Amenazas de la [L_SYT] Unidad de Sistema de Redes y Comunicaciones

AMENAZA	FRECUENCIA	[D]	[I]	[C]
[N1] Fuego				
[N2] Daños por Agua				
[N*] Desastres Naturales				
[I1] Fuego				
[I2] Daños por agua	4	25%		
[I*] Desastres industriales				
[A7] Uso no previsto	12	25%		
[A11] Acceso no autorizado	12		25%	25%
[A26] Ataque destructivo				
[A27] Ocupación enemiga				

Tabla 164

Amenazas del [GER_SYT] Responsable del Área de Sistemas

AMENAZA	FRECUENCIA	[D]	[I]	[C]
[E7] Deficiencia en la organización				
[E28] Indisponibilidad del personal	12	25%		
[A28] Indisponibilidad del personal				
[A29] Extorsión				
[A30] Ingeniería social				

Tabla 165

Amenazas del [UI_SYT] Responsable de Soporte a Usuarios

AMENAZA	FRECUENCIA	[D]	[I]	[C]
[E7] Deficiencia en la organización				
[E28] Indisponibilidad del personal	12	25%		
[A28] Indisponibilidad del personal				
[A29] Extorsión				
[A30] Ingeniería social				

Tabla 166

Amenazas de la [ITL_SYT] Infraestructura y Telecomunicaciones

AMENAZA	FRECUENCIA	[D]	[I]	[C]
[E7] Deficiencia en la organización				
[E28] Indisponibilidad del personal	12	25%		
[A28] Indisponibilidad del personal				
[A29] Extorsión				
[A30] Ingeniería social				

Tabla 167

Amenazas del [DBA_SYT] Administrador de la Base de Datos

AMENAZA	FRECUENCIA	[D]	[I]	[C]
[E7] Deficiencia en la organización				
[E28] Indisponibilidad del personal	12	25%		
[A28] Indisponibilidad del personal				
[A29] Extorsión				
[A30] Ingeniería social				

Tabla 168

Amenazas del [SEG_SYT] Responsable de Seguridad y Calidad

AMENAZA	FRECUENCIA	[D]	[I]	[C]
[E7] Deficiencia en la organización				
[E28] Indisponibilidad del personal	4	25%		
[A28] Indisponibilidad del personal				
[A29] Extorsión				
[A30] Ingeniería social				

Tabla 169

[RASTREO_SYT] Responsable de Monitoreo y Sopor te de Rastreo

AMENAZA	FRECUENCIA	[D]	[I]	[C]
[E7] Deficiencia en la organización				
[E28] Indisponibilidad del personal	4	25%		
[A28] Indisponibilidad del personal				
[A29] Extorsión				
[A30] Ingeniería social				

4.4 ACTIVOS POR AMENAZA

Tabla 170

Amenaza: Daños por agua [N2]

[N2] DAÑOS POR AGUA				
ACTIVO	**FRECUENCIA**	**[D]**	**[I]**	**[C]**
[CCTV] CIRCUITO CERRADO DE TELEVISIÓN	2	25%		

Tabla 171

Amenaza: Fuego [I1]

[I1] FUEGO				
ACTIVO	**FRECUENCIA**	**[D]**	**[I]**	**[C]**
[SBD] SERVIDOR DE DATOS	1	50%		
[DESKTOP] COMPUTADORAS DE ESCRITORIO	2	25%		

Tabla 172

Amenaza: Daños por Agua [I2]

[I2] DAÑOS POR AGUA				
ACTIVO	**FRECUENCIA**	**[D]**	**[I]**	**[C]**
[LAPTOPS] COMPUTADORAS PORTÁTILES	2	50%		
[DESKTOP] COMPUTADORAS DE ESCRITORIO	2	25%		
[SWITCH] SWITCH	4	25%		
[ROUTER] ROUTER	4	25%		
[RADIO] RED INHALÁMBRICA	2	25%		
[LAN] RED LAN	4	25%		
[WAN] RED WAN	4	25%		
[UPS] SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA	2	25%		
[RASTREO] SISTEMA DE RASTREO	4	25%		
[L] UNIDAD DE SISTEMAS DE REDES Y COMUNICACIONES	4	25%		
[WIFI] PUNTOS DE ACCESO WIRELESS	2	25%		
[PSTN] RED TELEFÓNICA	2	25%		

Tabla 173

Amenaza: Desastres Naturales: [I*]

[I*] DESASTRES INDUSTRIALES				
ACTIVO	**FRECUENCIA**	**[D]**	**[I]**	**[C]**
[SBD] SERVIDOR DE DATOS	2	50%		
[FIREWALL] FIREWALL	2	50%		
[GTWY] GATEWAY	2	50%		

Tabla 174

Amenaza: Contaminación Mecánica [I3]

[I3] CONTAMINACIÓN MECÁNICA				
ACTIVO	**FRECUENCIA**	**[D]**	**[I]**	**[C]**
[SBD] SERVIDOR DE DATOS	12	50%		
[FIREWALL] FIREWALL	12	50%		
[GTWY] GATEWAY	12	50%		
[DESKTOP] COMPUTADORAS DE ESCRITORIO	4	50%		
[CCTV] CIRCUITO CERRADO DE TELEVISIÓN	2	25%		

Tabla 175

Amenaza: Contaminación electromagnética

[I4] CONTAMINACIÓN ELECTROMAGNÉTICA				
AMENAZA	**FRECUENCIA**	**[D]**	**[I]**	**[C]**
[SBD] SERVIDOR DE DATOS	4	50%		
[FIREWALL] FIREWALL	4	50%		
[GTWY] GATEWAY	4	50%		
[DESKTOP] COMPUTADORAS DE ESCRITORIO	4	50%		
[LAN] RED LAN	4	25%		
[UPS] SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA	4	25%		

Tabla 176

Amenaza: Avería de origen físico o lógico

[I5] AVERÍA DE ORIGEN FISICO O LÓGICO				
ACTIVO	**FRECUENCIA**	**[D]**	**[I]**	**[C]**
[WEB] PORTAL WEB	2	25%		
[OFF] OFIMÁTICA	4	25%		
[AV] ANTIVIRUS	4	25%		
[SBD] SERVIDOR DE DATOS	4	50%		
[FIREWALL] FIREWALL	4	50%		
[DESKTOP] COMPUTADORAS DE ESCRITORIO	4	50%		
[LAPTOPS] COMPUTADORAS PORTÁTILES	2	50%		
[PRINT1] IMPRESORAS MATRICIALES	4	25%		
[PRINT2] IMPRESORA LASER	4	25%		
[SCAN] SCANNER	4	25%		
[SWITCH] SWITCH	4	25%		
[ROUTER]	4	25%		
[GTWY] GATEWAY	12	50%		
[WIFI] PUNTOS DE ACCESO WIRELESS	2	25%		
[PABX] CENTRAL TELEFÓNICA	2	25%		
[PSTN] RED TELEFÓNICA	2	25%		
[RADIO] RED INHALÁMBRICA	2	25%		
[LAN] RED LAN	4	25%		
[WAN] RED WAN	2	25%		
[DISK] DISCOS	1	25%		
[USB] DISPOSITIVO USB	1	25%		
[CCTV] CIRCUITO CERRADO DE TELEVISIÓN	4	25%		
[RASTREO] SISTEMA DE RASTREO	4	25%		
[UPS] SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA	4	25%		

Tabla 177

Amenaza: Corte del Suministro eléctrico

[I6] CORTE DEL SUMINISTRO ELÉCTRICO				
ACTIVO	**FRECUENCIA**	**[D]**	**[I]**	**[C]**
[CCTV] CIRCUITO CERRADO DE TELEVISIÓN	4	25%		
[DESKTOP] COMPUTADORAS DE ESCRITORIO	2	50%		
[SWITCH] SWITCH	4	25%		
[ROUTER]	4	25%		
[RADIO] RED INHALÁMBRICA	2	25%		
[LAN] RED LAN	4	25%		
[WAN] RED WAN	4	25%		
[UPS] SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA	4	25%		
[RASTREO] SISTEMA DE RASTREO	4	25%		
[WEB] PORTAL WEB	2	25%		
[ZM] SERVIDOR DE CORREO ELECTRÓNICO ZIMBRA	2	25%		
[OFF] OFIMÁTICA	4	25%		
[PRINT1] IMPRESORAS MATRICIALES	4	25%		
[PRINT2] IMPRESORA LASER	4	25%		
[SCAN] SCANNER	4	25%		
[WIFI] PUNTOS DE ACCESO WIRELESS	4	25%		
[PABX] CENTRAL TELEFÓNICA	2	25%		
[PSTN] RED TELEFÓNICA	4	25%		
[IEX] INTERNET	2	25%		
[NIGISU] SISTEMA FINANCIERO NIGISU	4		25%	

Tabla 178

Amenaza: Condiciones inadecuadas de temperatura y/o humedad

[I7] CONDICIONES INADECUADAS DE TEMPERATURA Y/O HUMEDAD				
ACTIVO	**FRECUENCIA**	**[D]**	**[I]**	**[C]**
[FIREWALL] FIREWALL	4	50%		
[LAPTOP] COMPUTADORAS LAPTOPS	4	50%		
[SWITCH] SWITCH	4	25%		
[GTWY] GATEWAY	12	50%		
[WIFI] PUNTOS DE ACCESO WIRELESS	2	25%		
[PABX] CENTRAL TELEFÓNICA	2	25%		
[LAN] RED LAN	4	25%		
[UPS] SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA	4	25%		
[CCTV] CIRCUITO CERRADO DE TELEVISIÓN	2	25%		
[RASTREO] SISTEMA DE RASTREO	4	25%		
[SBD] SERVIDOR DE DATOS	4	50%		

Tabla 179

Amenaza: Fallo de servicios de comunicaciones

[I8] FALLO DE SERVICIOS DE COMUNICACIONES				
ACTIVO	**FRECUENCIA**	**[D]**	**[I]**	**[C]**
[WEB] PORTAL WEB	2	25%		
[NIGISU] SISTEMA FINANCIERO NIGISU	4	50%		
[ZM] SERVIDOR DE CORREO ELECTRÓNICO ZIMBRA	2	25%		

Tabla 180

Amenaza: Interrupción de otros servicios y suministros esenciales

[I9] INTERRUPCIÓN DE OTROS SERVICIOS Y SUMINISTROS ESENCIALES				
ACTIVO	**FRECUENCIA**	**[D]**	**[I]**	**[C]**
[RASTREO] SISTEMA DE RASTREO	4	25%		

Tabla 181

Amenaza: Degradación de los soportes de almacenamiento de la información

[I10] DEGRADACIÓN DE LOS SOPORTES DE ALMACENAMIENTO DE LA INFORMACIÓN				
ACTIVO	**FRECUENCIA**	**[D]**	**[I]**	**[C]**
[DISK] DISCOS	1	25%		
[USB] DISPOSITIVOS USB	1	25%		

Tabla 182

Amenaza: Errores del administrador

[E2] ERRORES DEL ADMINISTRADOR				
ACTIVO	**FRECUENCIA**	**[D]**	**[I]**	**[C]**
[LOG] INFORMACIÓN DE REGISTROS DE INGRESOS SOBRE LOS SERVIDORES	12	25%	25%	25%

Tabla 183

Amenaza: Errores de los usuarios

[E1] ERRORES DE LOS USUARIOS				
ACTIVO	**FRECUENCI**	**[D]**	**[I]**	**[C]**
[ZM] SERVIDOR DE CORREO ELECTRÓNICO ZIMBRA	12	25%		
[IP] TELEFONÍA IP	2	25%	25%	25%
[BACKUP] SERVIDOR DE COPIAS DE RESPALDO	2	25%	25%	
[COM] INFORMACIÓN LOGÍSTICA	2	25%	25%	
[INT] INFORMACIÓN ÓR DEPARTAMENTO	4	50%	50%	
[NIGISU] SISTEMA FINANCIERO CONTABLE	4	25%	25%	
[OFF] OFIMÁTICA	4	25%	25%	
[AV] ANTIVIRUS	4	25%	25%	
[OTR] OTROS SOFWTARE	4	25%	25%	
[TC_SYT] TRANSPORTE DE CARGE REFRIGERADA O SECA	12	50%		
[AC_SYT] ALQUILER DE CONTENEDORES	12	50%		
[SMD] SERVICIO DE MONTAJE Y DESMONTAJE	12	50%		
[PER_M_SYT] INFORMACIÓN DE CADA USUARIO	4	10%	10%	10%
[LAPTOPS] COMPUTADORAS PORTÁTILES	4	25%		

Tabla 184

Amenaza: Errores de monitorización

[E3] ERRORES DE MONITORIZACIÓN				
ACTIVO	**FRECUENCIA**	**[D]**	**[I]**	**[C]**
[COM] INFORMACIÓN LOGÍSTICA	2	25%	25%	25%
[LOG] INFORMACIÓN DE REGISTROS DE INGRESOS SOBRE LOS SERVIDORES	12	50%	50%	50%

Tabla 185

Amenaza: Errores de configuración

[E4] ERRORES DE CONFIGURACIÓN				
ACTIVO	**FRECUENCIA**	**[D]**	**[I]**	**[C]**
[IP] TELEFONÍA IP	2	25%	25%	25%
[BACKUP] SERVIDOR DE COPIAS DE RESPALDO	2	25%	25%	25%
[IEX] INTERNET	2	25%	25%	25%
[SCAN] SCANNER	2	25%		
[PRINT1] IMPRESORAS MATRICIALES	8	25%		
[PRINT2] IMPRESORA LASER	4	25%		
[ROUTER]ROUTER	1	25%	25%	25%
[WIFI] PUNTOS DE ACCESO WIRELESS	2	25%		
[PABX] CENTRAL TELEFÓNICA	2	25%		
[LAN] RED LAN	2	25%	25%	25%
[WAN] RED WAN	4	25%		

Tabla 186

Amenaza: Difusión de software dañino

[E8] DIFUSIÓN DE SOFTWARE DAÑINO				
ACTIVO	**FRECUENCIA**	**[D]**	**[I]**	**[C]**
[LAPTOPS] COMPUTADORAS PORTÁTILES	4	25%		
[E9] ERRORES DE [RE-]ENCAMINAMIENTO				
[IP] TELEFONÍA IP	2		25%	25%

Tabla 187

Amenaza: Errores de secuencia

[E10] ERRORES DE SECUENCIA				
ACTIVO	**FRECUENCIA**	**[D]**	**[I]**	**[C]**
[LAN] RED LAN	2		25%	
[WAN] RED WAN	1		25%	

Tabla 188

Amenaza: Escapes de información

[E14] ESCAPES DE INFORMACIÓN				
ACTIVO	**FRECUENCIA**	**[D]**	**[I]**	**[C]**
[ZM] SERVIDOR DE CORREO ELECTRÓNICO	2			25%

Tabla 189

Amenaza: Alteración de la información

[E15] ALTERACIÓN DE LA INFORMACIÓN				
ACTIVO	**FRECUENCIA**	**[D]**	**[I]**	**[C]**
[BACKUP] SERVICIO DE COPIAS DE RESPALDO	2	25%		
[COM] INFORMACIÓN LOGÍSTICA	2		25%	
[INT] INFORMACIÓN POR DEPARTAMENTO	2		50%	

Tabla 190

Amenaza: Introducción de información incorrecta

[E16] INTRODUCCIÓN DE INFORMACIÓN INCORRECTA				
ACTIVO	**FRECUENCIA**	**[D]**	**[I]**	**[C]**
[COM] INFORMACIÓN LOGÍSTICA	12		50%	
[INT] INFORMACIÓN POR DEPARTAMENTO	12		50%	

Tabla 191

Amenaza: Degradación de la información

[E17] DEGRADACIÓN DE LA INFORMACIÓN				
ACTIVO	**FRECUENCIA**	**[D]**	**[I]**	**[C]**
[LOG] INFORMACIÓN DE REGISTROS DE INGRESOS SOBRE LOS SERVIDORES	2		25%	

Tabla 192

Amenaza: Destrucción de la información

[E18] DESTRUCCIÓN DE LA INFORMACIÓN				
ACTIVO	**FRECUENCIA**	**[D]**	**[I]**	**[C]**
[COM] INFORMACIÓN LOGÍSTICA	2	25%		
[LOG] INFORMACIÓN DE REGISTROS DE INGRESOS SOBRE LOS SERVIDORES	1	25%		

Tabla 193

Amenaza: Errores de mantenimiento/actualización de programas (software)

[E21] ERRORES DE MANTENIMIENTO/ACTUALIZACIÓN DE PROGRAMAS (SOTFWARE)				
ACTIVO	**FRECUENCIA**	**[D]**	**[I]**	**[C]**
[IP] TELEFONÍA IP	2	25%	25%	
[NIGISU] SISTEMA FINANCERO CONTABLE	4	25%	25%	
[OFF] OFIMÁTICA	4	25%	25%	
[AV] ANTIVIRUS	4	25%	25%	
[OTR] OTROS SOFTWARE	2	25%	25%	
[ZM] SERVIDOR DE CORREO ELECTRÓNICO	2			25 %

Tabla 194

Amenaza: Errores de mantenimiento/actualización de programas (hardware)

[E23] ERRORES DE MANTENIMIENTO/ACTUALIZACIÓN DE PROGRAMAS (HARDWARE)				
ACTIVO	**FRECUENCIA**	**[D]**	**[I]**	**[C]**
[FIREWALL] FIREWALL	2	25%		
[PRINT1] IMPRESORAS MATRICIALES	2	25%		
[PRINT2] IMPRESORA LASER	2	25%		
[GTWY] GATEWAY	2	25%		

Tabla 195

Amenaza: Caída del sistema por agotamiento de recursos

[E24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS				
ACTIVO	FRECUENCIA	[D]	[I]	[C]
[WEB] PORTAL WEB	2	25%	25%	25%
[FIREWALL] FIREWALL	2	25%		
[GTWY] GATEWAY	2	25%		
[SBD] SERVIDOR DE DATOS	4	50%		

Tabla 196

Amenaza: Indisponibilidad del personal

[E28] INDISPONIBILIDAD DEL PERSONAL				
ACTIVO	FRECUENCIA	[D]	[I]	[C]
[GER] RESPONSABLE DEL ÁREA DE SISTEMAS	12	25%		
[UI] RESPONSABLE DEL SOPORTE DE USUARIOS	12	25%		
[DBA] ADMINISTRADOR DE LA BASE DE DATOS	12	25%		
[SEG] RESPONSABLE DEL ÁREA DE SEGURIDAD Y CALIDAD	4	25%		
[RASTREO] RESPONSABLE DEL SISTEMA DE RASTREO	4	25%		

Tabla 197

Amenaza: Manipulación de la configuración

[A4] MANIPULACIÓN DE LA CONFIGURACIÓN				
ACTIVO	**FRECUENCIA**	**[D]**	**[I]**	**[C]**
[LOG] INFORMACIÓN DE REGISTROS DE INGRESOS SOBRE LOS SERVIDORES	12	25%	25%	25%
[AV] ANTIVIRUS	1	25%	25%	25%
[DESKTOP] COMPUTADORAS DE ESCRITORIIO	2	25%	25%	25%
[LAPTOPS] COMPUTADORAS PORTÁTILES	4	25%		
[SCAN] SCANNER	2	25%	25%	25%
[PRINT1] IMPRESORAS MATRICIALES	8	25%		
[PRINT2] IMPRESORAS LASER	4	25%		
[WIFI] PUNTOS DE ACCESO WIRELESS	2	25%		
[PABX] CENTRAL TELEFÓNICA	2	25%		
[PSTN] RED TELEFÓNICA	2	25%		
[OTR] OTROS SOFTWARE	2	25%		
[RADIO] RED INHALÁMBRICA	2	25%		

Tabla 198

Amenaza: Suplantación de la identidad del usuario

[A5] SUPLANTACIÓN DE LA IDENTIDAD DEL USUARIO				
ACTIVO	**FRECUENCIA**	**[D]**	**[I]**	**[C]**
[ZM] SERVIDOR DE CORREO ELECTRÓNICO ZIMBRA	2			25%

Tabla 199

Amenaza: Difusión de software dañino

[A8] DIFUSIÓN DE SOFTWARE DAÑINO				
ACTIVO	**FRECUENCIA**	**[D]**	**[I]**	**[C]**
[AV] ANTIVIRUS	4	25%	25%	25%
[IEX] INTERNET	2	25%	25%	25%

Tabla 200

Amenaza: Encaminamiento de mensajes

[A9] [RE-]ENCAMINAMIENTO DE MENSAJES				
ACTIVO	**FRECUENCIA**	**[D]**	**[I]**	**[C]**
[TC_SYT] TRANSPORTE DE CARGA REFRIGERADA Y SECA	4			50%
[AC_SYT] ALQUILER DE CONTENEDORES	4			50%
[SMD] SERVICIO DE MONTAJE Y DESMONTAJE	4			50%

Tabla 201

Amenaza: Acceso no autorizado

[A11] ACCESO NO AUTORIZADO				
ACTIVO	**FREC**	**[D]**	**[I]**	**[C]**
[IP] TELEFONÍA IP	2		25%	25%
[COM] INFORMACIÓN LOGÍSTICA	2		25%	25%
[INT] INFORMACIÓN POR DEPARTAMENTO	2		25%	25%
[IEX] INTERNET	4		25%	25%
[SBD] SERVIDOR DE DATOS	4			50%
[CCTV] CIRCUITO CERRADO DE TELEVISIÓN	1		25%	25%
[RASTREO] SISTEMA DE RASTREO	4		25%	25%
[L] UNIDAD DE REDES Y COMUNICACIONES	12		25%	25%

Tabla 202

Amenaza: Modificación de la información

[A15] MODIFICACIÓN DE LA INFORMACIÓN				
ACTIVO	**FRECUENCIA**	**[D]**	**[I]**	**[C]**
[COM] INFORMACIÓN LOGÍSTICA	2		50%	
[INT] INFORMACIÓN POR DEPARTAMENTO	2		50%	
[PER_M] INFORMACIÓN DE CADA USUARIO	4	10%	10%	10%
[NIGISU] SISTEMA FINANCIERO NIGISU	4		25%	

Tabla 203

Amenaza: Denegación del servicio

[A24] DENEGACION DE SERVICIO				
ACTIVO	**FRECUENCIA**	**[D]**	**[I]**	**[C]**
[BACKUP] SERVICIO DE COPIAS DE RESPALDO	2	25%		
[FIREWALL] FIREWALL	1	50%		
[GTWY] GATEWAY	1	50%		

Tabla 204

Amenaza: Robo

[A25] ROBO				
ACTIVO	**FRECUENCIA**	**[D]**	**[I]**	**[C]**
[DESKTOP] COMPUTADORAS DE ESCRITORIO	1	100%		100%
[LAPTOPS] COMPUTADORAS PORTÁTILES	4	80%		80%

ANEXO 5

EVALUACIÓN DE SALVAGUARDAS

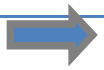
Tabla 205

Marco de Gestión

MARCO DE GESTIÓN	20%	82%
SALVAGUARDA	**HOY**	**SOLUC**
Organización	9%	48%
Comité de gestión de seguridad de la información (fórum)	10%	40%
Coordinación de la seguridad de la información	10%	60%
Asignación de responsabilidades para la seguridad de la información	5%	50%
Se dispone de asesoramiento especializado en seguridad	10%	30&
Cooperación entre organizaciones	10%	40%
Normativa de seguridad	21%	75%
Marco legal	20%	40%
Política de Seguridad (documento)	28%	68%
Política derivada de la Política de Seguridad Global de la Organización	10%	30%
Está aprobado y respaldado por el responsable de la organización	40%	80%
Todo el personal de la organización tiene acceso al documento	40%	80%
Conocido y aceptado por los afectados	20%	80%
Referencia normativa y procedimientos específicos	0%	50%
Revisión periódica del documento de política	0%	60%
Documentación de seguridad del sistema	10%	80%
Procedimientos operativos	10%	80%
Criterios de aceptación para versiones o sistemas nuevos	40%	100%
Acreditación de sistemas	20%	80%

Continua

MARCO DE GESTIÓN	20%	82%
SALVAGUARDA	**HOY**	**SOLUC**
Identificación y autenticación	40%	100%
Identificación de usuario	40%	100%
Herramientas de Identificación y Autenticación de usuario	40%	100%
Control de acceso lógico	34%	91%
Norma para el control de accesos	20%	80%
Restricción de acceso a la información	30%	100%
Segregación de tareas	10%	80%
Registro de usuario	50%	100%
Gestión de privilegios	50%	100%
Revisión de los derechos de acceso de los usuarios	20%	80%
Control de acceso discrecional	10%	80%
Control de acceso obligatorio	40%	100%
Uso de las utilidades del sistema	40%	80%
Conexión en terminales (logon)	50%	100%
Identificación automática de terminales	60%	100%
Limitación del tiempo de conexión	20%	80%
Desconexión automática de terminales	40%	100%
Gestión de incidencias	10%	80%
Procedimientos de gestión de incidentes	0%	80%
Frente a código dañino	10%	80%
Comunicación de las incidencias de seguridad	10%	80%
Comunicación de las deficiencias de seguridad	10%	80%
Comunicación de los fallos del software	10%	80%
Registro de fallos y revisión de las medidas correctoras	10%	80%
Se aprende de los incidentes y se proponen mejoras	10%	80%
Revisión de la seguridad de los sistemas de información	10%	80%
Continuidad del negocio (contingencia)	13%	100%

Continua 

MARCO DE GESTIÓN	20%	82%
SALVAGUARDA	**HOY**	**SOLUC**
Proceso de gestión de la continuidad	10%	100%
Plan de gestión de crisis	10%	100%
Seguros contra interrupciones en el negocio	20%	100%

Tabla 206

Relaciones con Terceros

RELACIONES CON TERCEROS	33%	100%
SALVAGUARDA	**HOY**	**SOLUC**
Seguridad en los accesos de terceras partes	50%	100%
Establecimiento de acuerdos para intercambio de información y software	20%	100%
Inclusión de cláusulas de confidencialidad en los contratos con otras empresas	30%	100%

Tabla 207

Servicios

SERVICIOS	41%	83%
SALVAGUARDA	**HOY**	**SOLUC**
Inventario de servicios	60%	100%
Disponibilidad	50%	100%
Protección frente a Dos	50%	100%
Desarrollo	40%	60%
Despliegue	35%	65%
Procedimiento de puesta en pre-producción	40%	60%
Pruebas de aceptación	40%	60%

Continua

Tabla 208

Servicios

SERVICIOS	41%	83%
SALVAGUARDA	**HOY**	**SOLUC**
Procedimiento de paso a producción	40%	60%
Campaña de ejecución de pruebas de regresión (no afecta a los demás servicios)	20%	80%
Aplicación de perfiles de seguridad	20%	80%
Explotación	43%	95%
Norma de condiciones de uso	20%	80%
No repudio	20%	80%
Seguridad en comercio electrónico	50%	100%
Seguridad del correo electrónico	70%	100%
Protección de la integridad de la información publicada electrónicamente	60%	100%
Infraestructura de clave pública	20%	100%
Protección del directorio	40%	100%
Telefonía móvil	60%	100%
Gestión de servicios externos	40%	80%

Tabla 209

Datos/Información

DATOS/INFORMACIÓN	28%	88%
SALVAGUARDA	**HOY**	**SOLUC**
Inventario de activos de información	10%	100%
Clasificación de la información	20%	100%
Disponibilidad	40%	50%
Integridad	40%	100%

Tabla 210

Aplicaciones Informáticas (SW)

APLICACIONES INFORMÁTICAS (SW)	27%	78%
SALVAGUARDA	**HOY**	**SOLUC**
Inventario de aplicaciones	10%	80%
Copias de seguridad	40%	100%
Adquisición	20%	60%
Desarrollo	20%	60%
Aplicación de perfiles de seguridad	20%	60%
Explotación	36%	96%
Procedimiento para el control de software en producción	10%	50%
Seguridad de las aplicaciones	20%	80%
Seguridad de los ficheros del sistema	40%	100%
Seguridad de los ficheros de datos de la aplicación	40%	100%
Seguridad de los ficheros de configuración	40%	100%
Seguridad de los mecanismos de comunicación entre procesos	40%	100%
Cambios (Actualizaciones y mantenimiento)	40%	90%
Seguimiento permanente de actualizaciones y parches	40%	80%
Evaluación del impacto potencial del cambio	0%	20%
Definición del proceso de cambio de forma que minimice la interrupción del servicio	40%	100%
Retención de versiones anteriores de software como medida de precaución para contingencias	0%	0%
Pruebas de regresión	0%	0%
Procedimientos de control de cambios	0%	0%
Registro de toda actualización de SW	0%	0%
Documentación	0%	0%
Control de versiones de toda actualización del software	0%	0%
Actualización de todos los procedimientos de explotación afectados	0%	0%
Actualización de los planes de contingencia	0%	0%

Tabla 211

Equipos Informáticos (HW)

EQUIPOS INFORMÁTICOS (HW)	39%	81%
SALVAGUARDA	**HOY**	**SOLUC**
Inventario de equipos	60%	100%
Adquisición de HW	40%	80%
Desarrollo de HW	40%	80%
Instalación	40%	80%
Operación	26%	75%
Cambios (actualizaciones y mantenimiento)	30%	70%

Tabla 212

Comunicaciones

COMUNICACIONES	34%	64%
SALVAGUARDA	**HOY**	**SOLUC**
Inventario de servicios de comunicación	50%	80%
Adquisición o contratación	35%	80%
Planificación	20%	80%
Aceptación de nuevos servicios	50%	80%
Instalación	50%	80%
Aplicación de perfiles de seguridad	10%	10%
Operación	43%	73%
Control de acceso a la red	40%	60%
Acceso remoto	60%	100%
Norma de uso de los servicios de red	60%	100%
Protección de puertos de diagnóstico remoto	60%	100%
Segregación de las redes en dominios	80%	100%

Continua

COMUNICACIONES	34%	64%
SALVAGUARDA	**HOY**	**SOLUC**
Autenticación de nodos de la red	0%	0%
Control del encaminamiento	0%	0%
Criptografía	45%	85%
Seguridad de los servicios de red	60%	100%
Protección de las comunicaciones Internet	60%	100%
Red privada virtual (VPN)	60%	100%
Protección emanaciones electromagnéticas	0%	40%
Cambios (actualizaciones y mantenimiento)	18%	60%
Seguimiento permanente de Actualizaciones	10%	50%
Procedimientos de control de cambios	10%	40%
Documentación	10%	50%
Actualización de todos los procedimientos de operación afectados	30%	80%
Actualización de los planes de contingencia	30%	80%

Tabla 213

Soportes de Información

SOPORTES DE INFORMACIÓN	10%	50%
SALVAGUARDA	**HOY**	**SOLUC**
Inventario de soportes	10%	50%
Disponibilidad	10%	50%
Adquisición de soportes	10%	50%
Gestión de soportes	10%	50%
Terminación	10%	50%
Herramientas para destrucción segura de información en soportes	10%	50%

Tabla 214

Elementos Auxiliares

ELEMENTOS AUXILIARES	50%	83%
SALVAGUARDA	**HOY**	**SOLUC**
Inventario de equipamiento auxiliar	50%	100%
Disponibilidad	50%	80%
Instalaciones	50%	80%
Suministro eléctrico	50%	80%
Climatización	50%	80%
Protección del cableado	50%	80%
Otros suministros	50%	80%

Tabla 215

Seguridad Física

SEGURIDAD FÍSICA	15%	56%
SALVAGUARDA	**HOY**	**SOLUC**
Inventario de instalaciones	40%	80%
Normativa	20%	60%
Procedimientos	10%	50%
Diseño	0%	40%
Control de los accesos físicos	10%	50%
Protección del perímetro	10%	50%
Vigilancia	30%	100%
Iluminación de seguridad	10%	40%
Protección frente a desastres	5%	30%

Tabla 216

Personal

PERSONAL	48%	92%
SALVAGUARDA	**HOY**	**SOLUC**
Relación de personal	60%	80%
Puestos de trabajo	60%	80%
Formación	40%	100%
Política del puesto de trabajo despejado y bloqueo de pantalla	40%	100%
Evaluación y revisión del plan de formación	40%	100%

ANEXO 6

ESTADO DE RIESGO

6.1 IMPACTO ACUMULADO

Tabla 217

Impacto acumulado del Transporte de mercancía refrigerada

[TC_SYT] TRANSPORTE DE MERCANCÍA REFRIGERADA			
IMPACTO ACUMULADO			
[E1] ERRORES DE LOS USUARIOS	[6]	[6]	[6]
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	[7]	[7]	[7]
[E18] DESTRUCCIÓN DE LA INFORMACIÓN	[3]	[3]	[3]
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	[3]	[3]	[3]
[A18] DESTRUCCIÓN DE LA INFORMACIÓN	[8]	[8]	[8]

Tabla 218

Impacto acumulado del Alquiler de contenedores

[AC_SYT] ALQUILER DE CONTENEDORES			
IMPACTO ACUMULADO			
[E1] ERRORES DE LOS USUARIOS	[6]	[6]	[6]
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	[4]	[4]	[4]
[E18] DESTRUCCIÓN DE LA INFORMACIÓN	[0]	[0]	[0]
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	[0]	[0]	[0]
[A18] DESTRUCCIÓN DE LA INFORMACIÓN	[5]	[5]	[5]

Tabla 219

Impacto acumulado del Servicios de montaje y desmontaje

[SMD_SYT] SERVICIO DE MONTAJE Y DESMONTAJE			
IMPACTO ACUMULADO			
[E1] ERRORES DE LOS USUARIOS	[3]	[3]	[3]
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	[4]	[4]	[4]
[E18] DESTRUCCIÓN DE LA INFORMACIÓN	[0]	[0]	[0]
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	[0]	[0]	[0]
[A18] DESTRUCCIÓN DE LA INFORMACIÓN	[5]	[5]	[5]

Tabla 220

Impacto acumulado del Portal Web

[WEB_SYT] PORTAL WEB			
IMPACTO ACUMULADO			
[I9] INTERRUPCION DE OTROS SERVICIOS O SUMINISTROS ESENCIALES	[0]	[0]	[0]
[E1] ERRORES DE LOS USUARIOS	[0]	[0]	[0]
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	[0]	[0]	[0]
[E18] DESTRUCCIÓN DE LA INFORMACIÓN	[0]	[0]	[0]
[E24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	[0]	[0]	[0]
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	[0]	[0]	[0]
[A7] USO NO PREVISTO	[0]	[0]	[0]
[A18] DESTRUCCIÓN DE LA INFORMACIÓN	[0]	[0]	[0]
[A24] DENEGACIÓN DEL SERVICIO	[0]	[0]	[0]

Tabla 221

Impacto acumulado del Servidor de Correo Electrónico Zimbra

[ZM_SYT] SERVIDOR DE CORREO ELECTRÓNICO ZIMBRA			
IMPACTO ACUMULADO			
[E1] ERRORES DE LOS USUARIOS	[7]	[7]	[7]
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	[8]	[8]	[8]
[E15] ALTERACIÓN DE LA INFORMACIÓN			
[E18] DESTRUCCIÓN DE LA INFORMACIÓN	[7]	[7]	[7]
[E24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	[9]	[9]	[9]
[A5] SUPLANTACIÓN DE LA IDENTIDAD			
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	[4]	[4]	[4]
[A7] USO NO PREVISTO	[4]	[4]	[4]
[A11] ACCESO NO AUTORIZADO			
[A15] MODIFICACIÓN DE LA INFORMACIÓN			
[A18] DESTRUCCIÓN DE LA INFORMACIÓN	[9]	[9]	[9]
[A24] DENEGACIÓN DEL SERVICIO	[9]	[9]	[9]

Tabla 222

Impacto acumulado de la Telefonía IP

[IP_SYT] TELEFONÍA IP			
IMPACTO ACUMULADO			
[E1] ERRORES DE LOS USUARIOS	[4]	[4]	[4]
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	[5]	[5]	[5]
[E15] ALTERACIÓN DE LA INFORMACIÓN			

Continua

[IP_SYT] TELEFONÍA IP			
IMPACTO ACUMULADO			
[E18] DESTRUCCIÓN DE LA INFORMACIÓN	[4]	[4]	[4]
[E24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	[6]	[6]	[6]
[A5] SUPLANTACIÓN DE LA IDENTIDAD			
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	[1]	[1]	[1]
[A7] USO NO PREVISTO	[1]	[1]	[1]
[A11] ACCESO NO AUTORIZADO			
[A15] MODIFICACIÓN DE LA INFORMACIÓN			
[A18] DESTRUCCIÓN DE LA INFORMACIÓN	[6]	[6]	[6]
[A24] DENEGACIÓN DEL SERVICIO	[6]	[6]	[6]

Tabla 223

Impacto acumulado del Servicio de copias de respaldo

[BACKUP_SYT] SERVICIO DE COPIAS DE RESPALDO			
IMPACTO ACUMULADO			
[E1] ERRORES DE LOS USUARIOS	[0]	[0]	[0]
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	[1]	[1]	[1]
[E15] ALTERACIÓN DE LA INFORMACIÓN			
[E18] DESTRUCCIÓN DE LA INFORMACIÓN	[0]	[0]	[0]
[E19] FUGAS DE INFORMACIÓN			
[E24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	[2]	[2]	[2]
[A5] SUPLANTACIÓN DE LA IDENTIDAD			
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	[0]	[0]	[0]
[A7] USO NO PREVISTO	[0]	[0]	[0]

Continua

[BACKUP_SYT] SERVICIO DE COPIAS DE RESPALDO			
IMPACTO ACUMULADO			
[A11] ACCESO NO AUTORIZADO			
[A15] MODIFICACIÓN DE LA INFORMACIÓN			
[A18] DESTRUCCIÓN DE LA INFORMACIÓN	[2]	[2]	[2]
[A19] REVELACIÓN DE INFORMACIÓN			
[A24] DENEGACIÓN DEL SERVICIO	[2]	[2]	[2]

Tabla 224

Impacto Acumulado dela Información logística

[INF_SYT] INFORMACIÓN LOGÍSTICA			
IMPACTO ACUMULADO			
[E1] ERRORES DE LOS USUARIOS	[7]	[7]	[7]
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	[8]	[8]	[8]
[E15] ALTERACIÓN DE LA INFORMACIÓN			
[E18] DESTRUCCIÓN DE LA INFORMACIÓN	[4]	[4]	[4]
[E19] FUGAS DE INFORMACIÓN			
[A5] SUPLANTACIÓN DE LA IDENTIDAD			
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	[4]	[4]	[4]
[A11] ACCESO NO AUTORIZADO			
[A15] MODIFICACIÓN DE LA INFORMACIÓN			
[A18] DESTRUCCIÓN DE LA INFORMACIÓN	[9]	[9]	[9]
[A19] REVELACIÓN DE INFORMACIÓN			

Tabla 225

Impacto acumulado de la Información por cada departamento

[INT_SYT] INFORMACIÓN POR CADA DEPARTAMENTO			
IMPACTO ACUMULADO			
[E1] ERRORES DE LOS USUARIOS	[7]	[7]	[7]
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	[8]	[8]	[8]
[E15] ALTERACIÓN DE LA INFORMACIÓN			
[E18] DESTRUCCIÓN DE LA INFORMACIÓN	[4]	[4]	[4]
[A5] SUPLANTACIÓN DE LA IDENTIDAD			
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	[4]	[4]	[4]
[A11] ACCESO NO AUTORIZADO			
[A15] MODIFICACIÓN DE LA INFORMACIÓN			
[A18] DESTRUCCIÓN DE LA INFORMACIÓN	[9]	[9]	[9]

Tabla 226

Impacto acumulado de la Información de Logs

[LOG_SYT] INFORMACIÓN DE REGISTROS DE INGRESOS SOBRE LOS SERVIDORES			
IMPACTO ACUMULADO			
[E1] ERRORES DE LOS USUARIOS	[6]	[6]	[6]
[E2] ERRORES DE ADMIN. DE SIST/DE SEG	[7]	[7]	[7]
[E3] ERRORES DE MONITORIZACION (LOG)			
[E15] ALTERACIÓN DE LA INFORMACIÓN			
[E18] DESTRUCCIÓN DE LA INFORMACIÓN	[3]	[3]	[3]
[E19] FUGAS DE INFORMACIÓN			
[A3] MANIPULACIÓN DE LOS REGISTROS DE ACTIVIDAD (LOG)			
[A5] SUPLANTACIÓN DE LA IDENTIDAD			

Continua

[LOG_SYT] INFORMACIÓN DE REGISTROS DE INGRESOS SOBRE LOS SERVIDORES			
IMPACTO ACUMULADO			
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	[3]	[3]	[3]
[A11] ACCESO NO AUTORIZADO			
[A13] REPUDIO (NEGACIÓN DE ACTUACIONES)			
[A15] MODIFICACIÓN DE LA INFORMACIÓN			
[A18] DESTRUCCIÓN DE LA INFORMACIÓN	[8]	[8]	[8]
[A19] REVELACIÓN DE LA INFORMACIÓN			

Tabla 227

Impacto Acumulado de la Información de cada usuario

[PER_SYT] INFORMACIÓN PERSONAL DE CADA USUARIO			
IMPACTO ACUMULADO			
[E1] ERRORES DE LOS USUARIOS	[0]	[0]	[0]
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	[1]	[1]	[1]
[E15] ALTERACIÓN DE LA INFORMACIÓN			
[E18] DESTRUCCIÓN DE LA INFORMACIÓN	[0]	[0]	[0]
[E19] FUGAS DE INFORMACIÓN			
[A5] SUPLANTACIÓN DE LA IDENTIDAD			
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	[0]	[0]	[0]
[A11] ACCESO NO AUTORIZADO			
[A15] MODIFICACIÓN DE LA INFORMACIÓN			
[A18] DESTRUCCIÓN DE LA INFORMACIÓN	[2]	[2]	[2]
[A19] REVELACIÓN DE LA INFORMACIÓN			

Tabla 228

Impacto acumulado del Sistema Financiero contable

[NIGISU_SYT] SISTEMA FINANCIERO CONTABLE			
IMPACTO ACUMULADO			
[I5] AVERÍA DE ORIGEN FISICO O LÓGICO	[9]	[9]	[9]
[E1] ERRORES DE LOS USUARIOS	[7]	[7]	[7]
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	[8]	[8]	[8]
[E3] ERRORES DE MONITORIZACIÓN (LOG)			
[E8] DIFUSIÓN DE SOFTWARE DAÑINO	[7]	[7]	[7]
[E15] ALTERACIÓN DE LA INFORMACIÓN			
[E18] DESTRUCCIÓN DE LA INFORMACIÓN	[9]	[9]	[9]
[E19] FUGAS DE INFORMACIÓN			
[E20] VULNERABILIDADES DE LOS PROGRAMAS DE SW	[4]	[4]	[4]
[E21] ERRORES DE MANTENIMIENTO/ACTUALIZACIÓN DE PROGRAMAS (SOFTWARE)	[4]	[4]	[4]
[A3] MANIPULACIÓN DE LOS REGISTROS DE ACTIVIDAD (LOG)			
[A5] SUPLANTACIÓN DE LA IDENTIDAD			
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	[4]	[4]	[4]
[A7] USO NO PREVISTO	[4]	[4]	[4]
[A8] DIFUSIÓN DE SOFTWARE DAÑINO			
[A11] ACCESO NO AUTORIZADO			
[A13] REPUDIO NEGACIÓN DE LAS ACTUACIONES			
[A15] MODIFICACIÓN DE LA INFORMACIÓN			
[A18] DESTRUCCIÓN DE LA INFORMACIÓN	[9]	[9]	[9]
[A19] REVELACIÓN DE LA INFORMACIÓN			
[A22] MANIPULACIÓN DE PROGRAMAS	[9]	[9]	[9]

Tabla 229

Impacto acumulado de la Ofimática

[OFF_SYT] OFIMÁTICA			
IMPACTO ACUMULADO			
[I5] AVERÍA DE ORIGEN FISICO O LÓGICO	[9]	[9]	[9]
[E1] ERRORES DE LOS USUARIOS	[4]	[4]	[4]
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	[8]	[8]	[8]
[E8] DIFUSIÓN DE SOFTWARE DAÑINO	[7]	[7]	[7]
[E15] ALTERACIÓN DE LA INFORMACIÓN			
[E18] DESTRUCCIÓN DE LA INFORMACIÓN	[9]	[9]	[9]
[E19] FUGAS DE INFORMACIÓN			
[E20] VULNERABILIDADES DE LOS PROGRAMAS DE SW	[4]	[4]	[4]
[E21] ERRORES DE MANTENIMIENTO/ACTUALIZACIÓN DE PROGRAMAS (SOFTWARE)	[4]	[4]	[4]
[A5] SUPLANTACIÓN DE LA IDENTIDAD			
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	[4]	[4]	[4]
[A7] USO NO PREVISTO	[4]	[4]	[4]
[A8] DIFUSIÓN DE SOFTWARE DAÑINO	[10]	[10]	[10]
[A11] ACCESO NO AUTORIZADO			
[A15] MODIFICACIÓN DE LA INFORMACIÓN			
[A18] DESTRUCCIÓN DE LA INFORMACIÓN	[9]	[9]	[9]
[A19] REVELACIÓN DE LA INFORMACIÓN			
[A22] MANIPULACIÓN DE PROGRAMAS	[9]	[9]	[9]

Tabla 230

Impacto acumulado del antivirus

[AV_SYT] ANTIVIRUS
IMPACTO ACUMULADO
[E1] ERRORES DE LOS USUARIOS
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD
[E8] DIFUSIÓN DE SOFTWARE DAÑINO
[E19] FUGAS DE INFORMACIÓN
[E20] VULNERABILIDADES DE LOS PROGRAMAS DE SW
[A5] SUPLANTACIÓN DE LA IDENTIDAD
[A6] ABUSO DE PRIVILEGIOS DE ACCESO
[A7] USO NO PREVISTO
[A8] DIFUSIÓN DE SOFTWARE DAÑINO
[A11] ACCESO NO AUTORIZADO
[A19] REVELACIÓN DE LA INFORMACIÓN
[A22] MANIPULACIÓN DE PROGRAMAS

Tabla 231

Impacto acumulado de Otros software

[OTR_SYT] OTROS SOFTWARE
IMPACTO ACUMULADO
[I5] AVERÍA DE ORIGEN FÍSICO O LÓGICO
[E1] ERRORES DE LOS USUARIOS
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD
[E8] DIFUSIÓN DE SOFTWARE DAÑINO
[E18] DESTRUCCIÓN DE LA INFORMACIÓN

Continua

[OTR_SYT] OTROS SOFTWARE			
IMPACTO ACUMULADO			
[E20] VULNERABILIDADES DE LOS PROGRAMAS DE SW			
[E21] ERRORES DE MANTENIMIENTO/ACTUALIZACIÓN DE PROGRAMAS (SOFTWARE)			
[A6] ABUSO DE PRIVILEGIOS DE ACCESO			
[A7] USO NO PREVISTO			
[A8] DIFUSIÓN DE SOFTWARE DAÑINO	[1]	[1]	[1]
[A18] DESTRUCCIÓN DE LA INFORMACIÓN			
[A22] MANIPULACIÓN DE PROGRAMAS			

Tabla 232

Impacto acumulado del Internet

[IEX_SYT] INTERNET			
IMPACTO ACUMULADO			
[I5] AVERÍA DE ORIGEN FÍSICO O LÓGICO	[9]	[9]	[9]
[E1] ERRORES DE LOS USUARIOS	[4]	[4]	[4]
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	[8]	[8]	[8]
[E8] DIFUSIÓN DE SOFTWARE DAÑINO	[7]	[7]	[7]
[E15] ALTERACION DE LA INFORMACIÓN			
[E18] DESTRUCCIÓN DE LA INFORMACIÓN	[9]	[9]	[9]
[E20] VULNERABILIDADES DE LOS PROGRAMAS DE SW	[4]	[4]	[4]
[E21] ERRORES DE MANTENIMIENTO/ACTUALIZACIÓN DE PROGRAMAS (SOFTWARE)	[4]	[4]	[4]
[A5] SUPLANTACIÓN DE LA IDENTIDAD			
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	[4]	[4]	[4]
[A7] USO NO PREVISTO	[4]	[4]	[4]

Continua

[IEX_SYT] INTERNET			
IMPACTO ACUMULADO			
[A8] DIFUSIÓN DE SOFTWARE DAÑINO	[10]	[10]	[10]
[A11] ACCESO NO AUTORIZADO			
[A15] MODIFICACIÓN DE LA INFORMACIÓN			
[A18] DESTRUCCIÓN DE LA INFORMACIÓN	[9]	[9]	[9]
[A22] MANIPULACIÓN DE PROGRAMAS	[9]	[9]	[9]

Tabla 233

Impacto acumulado del Servidor de datos

[SBD_SYT] SERVIDOR DE BASE DE DATOS			
IMPACTO ACUMULADO			
[N1] FUEGO	[10]	[10]	[10]
[N2] DAÑOS POR AGUA	[9]	[9]	[9]
[N*] DESASTRES NATURALES	[10]	[10]	[10]
[I1] FUEGO	[10]	[10]	[10]
[I2] DAÑOS POR AGUA	[9]	[9]	[9]
[I*] DESASTRES INDUSTRIALES	[10]	[10]	[10]
[I3] CONTAMINACIÓN MEDIOAMBIENTAL	[9]	[9]	[9]
[I4] CONTAMINACIÓN ELECTROMAGNÉTICA	[7]	[7]	[7]
[I5] AVERÍA DE ORIGEN FÍSICO O LÓGICO	[9]	[9]	[9]
[I6] CORTE DEL SUMINISTRO ELÉCTRICO	[10]	[10]	[10]
[I7] CONDICIONES INADECUADAS DE TEMPERATURA O HUMEDAD	[10]	[10]	[10]
[I11] EMANACIONES ELECTROMAGNÉTICAS			
[E1] ERRORES DE LOS USUARIOS	[7]	[7]	[7]
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	[8]	[8]	[8]

Continua

[SBD_SYT] SERVIDOR DE BASE DE DATOS			
IMPACTO ACUMULADO			
[E8] DIFUSIÓN DE SOFTWARE DAÑINO	[7]	[7]	[7]
[E15] ALTERACIÓN DE LA INFORMACIÓN			
[E18] DESTRUCCIÓN DE LA INFORMACIÓN	[9]	[9]	[9]
[E19] FUGAS DE INFORMACIÓN			
[E20] VULNERABILIDADES DE LOS PROGRAMAS	[4]	[4]	[4]
[E21] ERRORES DE MANTENIMIENTO/ACTUALIZACIÓN DE PROGRAMAS (SOFTWARE)	[4]	[4]	[4]
[E23] ERRORES DE MANTENIMIENTO/ACTUALIZACIÓN DE PROGRAMAS (HARDWARE)	[7]	[7]	[7]
[E24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	[9]	[9]	[9]
[E25] PÉRDIDA DE EQUIPOS	[10]	[10]	[10]
[A5] SUPLANTACIÓN DE LA IDENTIDAD			
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	[7]	[7]	[7]
[A7] USO NO PREVISTO	[7]	[7]	[7]
[A8] DIFUSIÓN DE SOFTWARE DAÑINO	[10]	[10]	[10]
[A11] ACCESO NO AUTORIZADO	[7]	[7]	[7]
[A15] MODIFICACIÓN DE LA INFORMACIÓN			
[A18] DESTRUCCIÓN DE LA INFORMACIÓN	[9]	[9]	[9]
[A19] REVELACIÓN DE LA INFORMACIÓN			
[A22] MANIPULACIÓN DE PROGRAMAS	[9]	[9]	[9]
[A23] MANIPULACIÓN DE HARDWARE	[9]	[9]	[9]
[A24] DENEGACIÓN DEL SERVICIO	[10]	[10]	[10]
[A25] ROBO DE EQUIPOS	[10]	[10]	[10]
[A26] ATAQUE DESTRUCTIVO	[10]	[10]	[10]

Tabla 234

Impacto acumulado del Firewall

[FIREWALL_SYT] FIREWALL			
IMPACTO ACUMULADO			
[N1] FUEGO	[10]	[10]	[10]
[N2] DAÑOS POR AGUA	[9]	[9]	[9]
[N*] DESASTRES NATURALES	[10]	[10]	[10]
[I1] FUEGO	[10]	[10]	[10]
[I2] DAÑOS POR AGUA	[9]	[9]	[9]
[I*] DESASTRES INDUSTRIALES	[10]	[10]	[10]
[I3] CONTAMINACIÓN MEDIOAMBIENTAL	[9]	[9]	[9]
[I4] CONTAMINACIÓN ELECTROMAGNÉTICA	[7]	[7]	[7]
[I5] AVERÍA DE ORIGEN FÍSICO O LÓGICO	[9]	[9]	[9]
[I6] CORTE DEL SUMINISTRO ELÉCTRICO	[10]	[10]	[10]
[I7] CONDICIONES INADECUADAS DE TEMPERATURA O HUMEDAD	[10]	[10]	[10]
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	[8]	[8]	[8]
[E23] ERRORES DE MANTENIMIENTO/ACTUALIZACIÓN DE PROGRAMAS (HARDWARE)	[7]	[7]	[7]
[E24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	[9]	[9]	[9]
[E25] PÉRDIDA DE EQUIPOS	[10]	[10]	[10]
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	[7]	[7]	[7]
[A7] USO NO PREVISTO	[7]	[7]	[7]
[A11] ACCESO NO AUTORIZADO	[7]	[7]	[7]
[A23] MANIPULACIÓN DE HARDWARE	[10]	[10]	[10]
[A24] DENEGACIÓN DEL SERVICIO	[10]	[10]	[10]
[A25] ROBO DE EQUIPOS	[10]	[10]	[10]

Tabla 235

Impacto acumulado de las Computadoras de escritorio

[DESKTOP_SYT] COMPUTADORAS DE ESCRITORIO			
IMPACTO ACUMULADO			
[N1] FUEGO	[3]	[3]	[3]
[N2] DAÑOS POR AGUA	[2]	[2]	[2]
[N*] DESASTRES NATURALES	[3]	[3]	[3]
[I1] FUEGO	[3]	[3]	[3]
[I2] DAÑOS POR AGUA	[2]	[2]	[2]
[I*] DESASTRES INDUSTRIALES	[3]	[3]	[3]
[I3] CONTAMINACIÓN MEDIOAMBIENTAL	[2]	[2]	[2]
[I4] CONTAMINACIÓN ELECTROMAGNÉTICA	[0]	[0]	[0]
[I5] AVERÍA DE ORIGEN FÍSICO O LÓGICO	[2]	[2]	[2]
[I6] CORTE DEL SUMINISTRO ELÉCTRICO	[3]	[3]	[3]
[I7] CONDICIONES INADECUADAS DE TEMPERATURA O HUMEDAD	[3]	[3]	[3]
[I11] EMANACIONES ELECTROMAGNÉTICAS			
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	[1]	[1]	[1]
[E23] ERRORES DE MANTENIMIENTO/ACTUALIZACIÓN DE PROGRAMAS (HARDWARE)	[0]	[0]	[0]
[E24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	[2]	[2]	[2]
[E25] PÉRDIDA DE EQUIPOS	[3]	[3]	[3]
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	[0]	[0]	[0]
[A7] USO NO PREVISTO	[0]	[0]	[0]
[A11] ACCESO NO AUTORIZADO	[0]	[0]	[0]
[A23] MANIPULACIÓN DE HARDWARE	[2]	[2]	[2]
[A24] DENEGACIÓN DEL SERVICIO	[3]	[3]	[3]

Tabla 236

Impacto acumulado de las computadoras portátiles

[LAPTOPS_SYT] COMPUTADORAS PORTÁTILES			
IMPACTO ACUMULADO			
[N1] FUEGO	[3]	[3]	[3]
[N2] DAÑOS POR AGUA	[2]	[2]	[2]
[N*] DESASTRES NATURALES	[3]	[3]	[3]
[I1] FUEGO	[3]	[3]	[3]
[I2] DAÑOS POR AGUA	[2]	[2]	[2]
[I*] DESASTRES INDUSTRIALES	[3]	[3]	[3]
[I3] CONTAMINACIÓN MEDIOAMBIENTAL	[2]	[2]	[2]
[I4] CONTAMINACIÓN ELECTROMAGNÉTICA	[0]	[0]	[0]
[I5] AVERÍA DE ORIGEN FÍSICO O LÓGICO	[2]	[2]	[2]
[I6] CORTE DEL SUMINISTRO ELÉCTRICO	[3]	[3]	[3]
[I7] CONDICIONES INADECUADAS DE TEMPERATURA O HUMEDAD	[3]	[3]	[3]
[I11] EMANACIONES ELECTROMAGNÉTICAS			
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	[1]	[1]	[1]
[E23] ERRORES DE MANTENIMIENTO/ACTUALIZACIÓN DE PROGRAMAS (HARDWARE)	[0]	[0]	[0]
[E24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	[2]	[2]	[2]
[E25] PÉRDIDA DE EQUIPOS	[3]	[3]	[3]
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	[0]	[0]	[0]
[A7] USO NO PREVISTO	[0]	[0]	[0]
[A11] ACCESO NO AUTORIZADO	[0]	[0]	[0]
[A23] MANIPULACIÓN DE HARDWARE	[2]	[2]	[2]
[A24] DENEGACIÓN DEL SERVICIO	[3]	[3]	[3]

Tabla 237

Impacto acumulado del Scanner

[SCAN_SYT] SCANNER			
IMPACTO ACUMULADO			
[N1] FUEGO	[0]	[0]	[0]
[N2] DAÑOS POR AGUA	[0]	[0]	[0]
[N*] DESASTRES NATURALES	[0]	[0]	[0]
[I1] FUEGO	[0]	[0]	[0]
[I2] DAÑOS POR AGUA	[0]	[0]	[0]
[I*] DESASTRES INDUSTRIALES	[0]	[0]	[0]
[I3] CONTAMINACIÓN MEDIOAMBIENTAL	[0]	[0]	[0]
[I4] CONTAMINACIÓN ELECTROMAGNÉTICA	[0]	[0]	[0]
[I5] AVERÍA DE ORIGEN FÍSICO O LÓGICO	[0]	[0]	[0]
[I6] CORTE DEL SUMINISTRO ELÉCTRICO	[0]	[0]	[0]
[I7] CONDICIONES INADECUADAS DE TEMPERATURA O HUMEDAD	[0]	[0]	[0]
[I11] EMANACIONES ELECTROMAGNÉTICAS			
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	[0]	[0]	[0]
[E23] ERRORES DE MANTENIMIENTO/ACTUALIZACIÓN DE PROGRAMAS (HARDWARE)	[0]	[0]	[0]
[E24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	[0]	[0]	[0]
[A7] USO NO PREVISTO	[0]	[0]	[0]
[A11] ACCESO NO AUTORIZADO	[0]	[0]	[0]
[A23] MANIPULACIÓN DE HARDWARE	[0]	[0]	[0]
[A24] DENEGACIÓN DEL SERVICIO	[0]	[0]	[0]
[A25] ROBO DE EQUIPOS	[0]	[0]	[0]
[A26] ATAQUE DESTRUCTIVO	[0]	[0]	[0]

Tabla 238

Impacto acumulado de las Impresoras matriciales

[PRINT1_SYT] IMPRESORAS MATRICIALES			
IMPACTO ACUMULADO			
[N1] FUEGO	[1]	[1]	[1]
[N2] DAÑOS POR AGUA	[0]	[0]	[0]
[N*] DESASTRES NATURALES	[1]	[1]	[1]
[I1] FUEGO	[1]	[1]	[1]
[I2] DAÑOS POR AGUA	[0]	[0]	[0]
[I*] DESASTRES INDUSTRIALES	[1]	[1]	[1]
[I3] CONTAMINACIÓN MEDIOAMBIENTAL	[0]	[0]	[0]
[I4] CONTAMINACIÓN ELECTROMAGNÉTICA	[0]	[0]	[0]
[I5] AVERÍA DE ORIGEN FÍSICO O LÓGICO	[0]	[0]	[0]
[I6] CORTE DEL SUMINISTRO ELÉCTRICO	[1]	[1]	[1]
[I7] CONDICIONES INADECUADAS DE TEMPERATURA O HUMEDAD	[1]	[1]	[1]
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	[0]	[0]	[0]
[E23] ERRORES DE MANTENIMIENTO/ACTUALIZACIÓN DE PROGRAMAS (HARDWARE)	[0]	[0]	[0]
[E24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	[0]	[0]	[0]
[E25] PÉRDIDA DE EQUIPOS	[1]	[1]	[1]
[A11] ACCESO NO AUTORIZADO	[0]	[0]	[0]
[A23] MANIPULACIÓN DE HARDWARE	[0]	[0]	[0]
[A24] DENEGACIÓN DEL SERVICIO	[1]	[1]	[1]
[A25] ROBO DE EQUIPOS	[1]	[1]	[1]
[A26] ATAQUE DESTRUCTIVO	[1]	[1]	[1]

Tabla 239

Impacto acumulado de la Impresora Laser

[PRINT2_SYT] IMPRESORA LASER			
IMPACTO ACUMULADO			
[N1] FUEGO	[1]	[1]	[1]
[N2] DAÑOS POR AGUA	[0]	[0]	[0]
[N*] DESASTRES NATURALES	[1]	[1]	[1]
[I1] FUEGO	[1]	[1]	[1]
[I2] DAÑOS POR AGUA	[0]	[0]	[0]
[I*] DESASTRES INDUSTRIALES	[1]	[1]	[1]
[I3] CONTAMINACIÓN MEDIOAMBIENTAL	[0]	[0]	[0]
[I4] CONTAMINACIÓN ELECTROMAGNÉTICA	[0]	[0]	[0]
[I5] AVERÍA DE ORIGEN FÍSICO O LÓGICO	[0]	[0]	[0]
[I6] CORTE DEL SUMINISTRO ELÉCTRICO	[1]	[1]	[1]
[I7] CONDICIONES INADECUADAS DE TEMPERATURA O HUMEDAD	[1]	[1]	[1]
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	[0]	[0]	[0]
[E23] ERRORES DE MANTENIMIENTO/ACTUALIZACIÓN DE PROGRAMAS (HARDWARE)	[0]	[0]	[0]
[E24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	[0]	[0]	[0]
[E25] PÉRDIDA DE EQUIPOS	[1]	[1]	[1]
[A7] USO NO PREVISTO	[0]	[0]	[0]
[A11] ACCESO NO AUTORIZADO	[0]	[0]	[0]
[A23] MANIPULACIÓN DE HARDWARE	[0]	[0]	[0]
[A24] DENEGACIÓN DEL SERVICIO	[1]	[1]	[1]
[A25] ROBO DE EQUIPOS	[1]	[1]	[1]
[A26] ATAQUE DESTRUCTIVO	[1]	[1]	[1]

Tabla 240

Impacto acumulado del Switch

[SWITCH_SYT] SWITCH			
IMPACTO ACUMULADO			
[N1] FUEGO	[10]	[10]	[10]
[N2] DAÑOS POR AGUA	[9]	[9]	[9]
[N*] DESASTRES NATURALES	[10]	[10]	[10]
[I1] FUEGO	[10]	[10]	[10]
[I2] DAÑOS POR AGUA	[9]	[9]	[9]
[I*] DESASTRES INDUSTRIALES	[10]	[10]	[10]
[I3] CONTAMINACIÓN MEDIOAMBIENTAL	[9]	[9]	[9]
[I4] CONTAMINACIÓN ELECTROMAGNÉTICA	[7]	[7]	[7]
[I5] AVERÍA DE ORIGEN FÍSICO O LÓGICO	[9]	[9]	[9]
[I6] CORTE DEL SUMINISTRO ELÉCTRICO	[10]	[10]	[10]
[I7] CONDICIONES INADECUADAS DE TEMPERATURA O HUMEDAD	[10]	[10]	[10]
[I11] EMANACIONES ELECTROMAGNÉTICAS			
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	[8]	[8]	[8]
[E23] ERRORES DE MANT/ACT DE PROG (HARD)	[7]	[7]	[7]
[E24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	[9]	[9]	[9]
[E25] PÉRDIDA DE EQUIPOS	[10]	[10]	[10]
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	[7]	[7]	[7]
[A7] USO NO PREVISTO	[7]	[7]	[7]
[A11] ACCESO NO AUTORIZADO	[7]	[7]	[7]
[A23] MANIPULACIÓN DE HARDWARE	[10]	[10]	[10]
[A24] DENEGACIÓN DEL SERVICIO	[10]	[10]	[10]
[A25] ROBO DE EQUIPOS	[10]	[10]	[10]
[A26] ATAQUE DESTRUCTIVO	[10]	[10]	[10]

Tabla 241

Impacto acumulado del Router

[ROUTER_SYT] ROUTER			
IMPACTO ACUMULADO			
[N1] FUEGO	[10]	[10]	[10]
[N2] DAÑOS POR AGUA	[9]	[9]	[9]
[N*] DESASTRES NATURALES	[10]	[10]	[10]
[I1] FUEGO	[10]	[10]	[10]
[I2] DAÑOS POR AGUA	[9]	[9]	[9]
[I*] DESASTRES INDUSTRIALES	[10]	[10]	[10]
[I3] CONTAMINACIÓN MEDIOAMBIENTAL	[9]	[9]	[9]
[I4] CONTAMINACIÓN ELECTROMAGNÉTICA	[7]	[7]	[7]
[I5] AVERÍA DE ORIGEN FÍSICO O LÓGICO	[9]	[9]	[9]
[I6] CORTE DEL SUMINISTRO ELÉCTRICO	[10]	[10]	[10]
[I7] CONDICIONES INADECUADAS DE TEMPERATURA O HUMEDAD	[10]	[10]	[10]
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	[8]	[8]	[8]
[E23] ERRORES DE MANT/ACT DE PROG (HARD)	[7]	[7]	[7]
[E24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	[9]	[9]	[9]
[E25] PÉRDIDA DE EQUIPOS	[10]	[10]	[10]
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	[7]	[7]	[7]
[A7] USO NO PREVISTO	[7]	[7]	[7]
[A11] ACCESO NO AUTORIZADO	[7]	[7]	[7]
[A23] MANIPULACIÓN DE HARDWARE	[10]	[10]	[10]
[A24] DENEGACIÓN DEL SERVICIO	[10]	[10]	[10]
[A25] ROBO DE EQUIPOS	[10]	[10]	[10]
[A26] ATAQUE DESTRUCTIVO	[10]	[10]	[10]

Tabla 242

Impacto acumulado del Gateway

[GTWY_SYT] GATEWAY			
IMPACTO ACUMULADO			
[N1] FUEGO	[10]	[10]	[10]
[N2] DAÑOS POR AGUA	[9]	[9]	[9]
[N*] DESASTRES NATURALES	[10]	[10]	[10]
[I1] FUEGO	[10]	[10]	[10]
[I2] DAÑOS POR AGUA	[9]	[9]	[9]
[I*] DESASTRES INDUSTRIALES	[10]	[10]	[10]
[I3] CONTAMINACIÓN MEDIOAMBIENTAL	[9]	[9]	[9]
[I4] CONTAMINACIÓN ELECTROMAGNÉTICA	[7]	[7]	[7]
[I5] AVERÍA DE ORIGEN FÍSICO O LÓGICO	[9]	[9]	[9]
[I6] CORTE DEL SUMINISTRO ELÉCTRICO	[10]	[10]	[10]
[I7] CONDICIONES INADECUADAS DE TEMPERATURA O HUMEDAD	[10]	[10]	[10]
[I11] EMANACIONES ELECTROMAGNÉTICAS			
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	[8]	[8]	[8]
[E23] ERRORES DE MANT/ACT DE PROG (HARD)	[7]	[7]	[7]
[E24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	[9]	[9]	[9]
[E25] PÉRDIDA DE EQUIPOS	[10]	[10]	[10]
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	[7]	[7]	[7]
[A7] USO NO PREVISTO	[7]	[7]	[7]
[A11] ACCESO NO AUTORIZADO	[7]	[7]	[7]
[A23] MANIPULACIÓN DE HARDWARE	[10]	[10]	[10]
[A24] DENEGACIÓN DEL SERVICIO	[10]	[10]	[10]
[A25] ROBO DE EQUIPOS	[10]	[10]	[10]
[A26] ATAQUE DESTRUCTIVO	[10]	[10]	[10]

Tabla 243

Impacto acumulado de los puntos de acceso Wireless

[WIFI_SYT] PUNTOS DE ACCESO WIRELESS			
IMPACTO ACUMULADO			
[N1] FUEGO	[10]	[10]	[10]
[N2] DAÑOS POR AGUA	[9]	[9]	[9]
[N*] DESASTRES NATURALES	[10]	[10]	[10]
[I1] FUEGO	[10]	[10]	[10]
[I2] DAÑOS POR AGUA	[9]	[9]	[9]
[I*] DESASTRES INDUSTRIALES	[10]	[10]	[10]
[I3] CONTAMINACIÓN MEDIOAMBIENTAL	[9]	[9]	[9]
[I4] CONTAMINACIÓN ELECTROMAGNÉTICA	[7]	[7]	[7]
[I5] AVERÍA DE ORIGEN FÍSICO O LÓGICO	[9]	[9]	[9]
[I6] CORTE DEL SUMINISTRO ELÉCTRICO	[10]	[10]	[10]
[I7] CONDICIONES INADECUADAS DE TEMPERATURA O HUMEDAD	[10]	[10]	[10]
[I11] EMANACIONES ELECTROMAGNÉTICAS			
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	[8]	[8]	[8]
[E23] ERRORES DE MANT/ACT DE PROG (HARD)	[7]	[7]	[7]
[E24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	[9]	[9]	[9]
[E25] PÉRDIDA DE EQUIPOS	[10]	[10]	[10]
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	[7]	[7]	[7]
[A7] USO NO PREVISTO	[7]	[7]	[7]
[A11] ACCESO NO AUTORIZADO	[7]	[7]	[7]
[A23] MANIPULACIÓN DE HARDWARE	[10]	[10]	[10]
[A24] DENEGACIÓN DEL SERVICIO	[10]	[10]	[10]
[A25] ROBO DE EQUIPOS	[10]	[10]	[10]
[A26] ATAQUE DESTRUCTIVO	[10]	[10]	[10]

Tabla 244

Impacto acumulado de la Central Telefónica

[PABX_SYT] CENTRAL TELEFÓNICA			
IMPACTO ACUMULADO			
[N1] FUEGO	[7]	[7]	[7]
[N2] DAÑOS POR AGUA	[6]	[6]	[6]
[N*] DESASTRES NATURALES	[7]	[7]	[7]
[I1] FUEGO	[7]	[7]	[7]
[I2] DAÑOS POR AGUA	[6]	[6]	[6]
[I*] DESASTRES INDUSTRIALES	[7]	[7]	[7]
[I3] CONTAMINACIÓN MEDIOAMBIENTAL	[6]	[6]	[6]
[I4] CONTAMINACIÓN ELECTROMAGNÉTICA	[4]	[4]	[4]
[I5] AVERÍA DE ORIGEN FÍSICO O LÓGICO	[6]	[6]	[6]
[I6] CORTE DEL SUMINISTRO ELÉCTRICO	[7]	[7]	[7]
[I7] CONDICIONES INADECUADAS DE TEMPERATURA O HUMEDAD	[7]	[7]	[7]
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	[5]	[5]	[5]
[E23] ERRORES DE MANT/ACT DE PROG (HARD)	[4]	[4]	[4]
[E24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	[6]	[6]	[6]
[E25] PÉRDIDA DE EQUIPOS	[7]	[7]	[7]
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	[4]	[4]	[4]
[A7] USO NO PREVISTO	[4]	[4]	[4]
[A11] ACCESO NO AUTORIZADO	[4]	[4]	[4]
[A23] MANIPULACIÓN DE HARDWARE	[6]	[6]	[6]
[A24] DENEGACIÓN DEL SERVICIO	[7]	[7]	[7]
[A25] ROBO DE EQUIPOS	[7]	[7]	[7]
[A26] ATAQUE DESTRUCTIVO	[7]	[7]	[7]

Tabla 245

Impacto acumulado de la Red Telefónica

[PSTN_SYT] RED TELEFÓNICA			
IMPACTO ACUMULADO			
[I8] FALLO DE SERVICIOS DE COMUNICACIONES	[6]	[6]	[6]
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	[5]	[5]	[5]
[E10] ERRORES DE SECUENCIA			
[E15] ALTERACIÓN DE LA INFORMACIÓN			
[E24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	[6]	[6]	[6]
[A5] SUPLANTACIÓN DE LA IDENTIDAD			
[A6] ABUSO DE PRIVILEGIOS DE ACCESO			
[A7] USO NO PREVISTO	[4]	[4]	[4]
[A10] ALTERACIÓN DE LA SECUENCIA			
[A11] ACCESO NO AUTORIZADO			
[A15] MODIFICACIÓN DE LA INFORMACIÓN			
[A18] DESTRUCCIÓN DE LA INFORMACIÓN	[6]	[6]	[6]
[A24] DENEGACIÓN DEL SERVICIO	[6]	[6]	[6]

Tabla 246

Impacto acumulado de la red inalámbrica

[RADIO_SYT] RED INALÁMBRICA			
IMPACTO ACUMULADO			
[I8] FALLO DE SERVICIOS DE COMUNICACIONES	[9]	[9]	[9]
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	[8]	[8]	[8]

Continua

[RADIO_SYT] RED INALÁMBRICA			
IMPACTO ACUMULADO			
[E9] ERRORES DE [RE-]ENCAMINAMIENTO			
[E10] ERRORES DE SECUENCIA			
[E15] ALTERACIÓN DE LA INFORMACIÓN			
[E19] FUGAS DE INFORMACIÓN			
[E24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	[9]	[9]	[9]
[A5] SUPLANTACIÓN DE LA IDENTIDAD			
[A6] ABUSO DE PRIVILEGIOS DE ACCESO			
[A7] USO NO PREVISTO	[7]	[7]	[7]
[A9] [RE-]ECAMINAMIENTO DE MENSAJES			
[A10] ALTERACIÓN DE LA SECUENCIA			
[A11] ACCESO NO AUTORIZADO			
[A12] ANÁLISIS DE TRÁFICO			
[A14] INTERCEPTACIÓN DE INFORMACIÓN (ESCUCHA)			
[A15] MODIFICACIÓN DE LA INFORMACIÓN			
[A18] DESTRUCCIÓN DE LA INFORMACIÓN	[9]	[9]	[9]
[A19] REVELACIÓN DE LA INFORMACIÓN			
[A24] DENEGACIÓN DEL SERVICIO	[9]	[9]	[9]

Tabla 247

Impacto de la Red Lan

[LAN_SYT] RED LAN			
IMPACTO ACUMULADO			
[I8] FALLO DE SERVICIOS DE COMUNICACIONES	[9]	[9]	[9]
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	[8]	[8]	[8]
[E9] ERRORES DE [RE-]ENCAMINAMIENTO			

Continua

[LAN_SYT] RED LAN			
IMPACTO ACUMULADO			
[E10] ERRORES DE SECUENCIA			
[E15] ALTERACIÓN DE LA INFORMACIÓN			
[E19] FUGAS DE INFORMACIÓN			
[E24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	[9]	[9]	[9]
[A5] SUPLANTACIÓN DE LA IDENTIDAD			
[A6] ABUSO DE PRIVILEGIOS DE ACCESO			
[A7] USO NO PREVISTO	[7]	[7]	[7]
[A9] [RE-]ECAMINAMIENTO DE MENSAJES			
[A10] ALTERACIÓN DE LA SECUENCIA			
[A11] ACCESO NO AUTORIZADO			
[A12] ANÁLISIS DE TRÁFICO			
[A14] INTERCEPTACIÓN DE INFORMACIÓN (ESCUCHA)			
[A15] MODIFICACIÓN DE LA INFORMACIÓN			
[A18] DESTRUCCIÓN DE LA INFORMACIÓN	[9]	[9]	[9]
[A19] REVELACIÓN DE LA INFORMACIÓN			
[A24] DENEGACIÓN DEL SERVICIO	[9]	[9]	[9]

Tabla 248

Impacto acumulado de la Red Wan

[WAN_SYT] RED WAN			
IMPACTO ACUMULADO			
[I8] FALLO DE SERVICIOS DE COMUNICACIONES	[9]	[9]	[9]
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	[8]	[8]	[8]
[E9] ERRORES DE [RE-]ENCAMINAMIENTO			
[E10] ERRORES DE SECUENCIA			

Continua

[WAN_SYT] RED WAN			
IMPACTO ACUMULADO			
[E15] ALTERACIÓN DE LA INFORMACIÓN			
[E19] FUGAS DE INFORMACIÓN			
[E24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	[9]	[9]	[9]
[A5] SUPLANTACIÓN DE LA IDENTIDAD			
[A6] ABUSO DE PRIVILEGIOS DE ACCESO			
[A7] USO NO PREVISTO	[7]	[7]	[7]
[A9] [RE-]ECAMINAMIENTO DE MENSAJES			
[A10] ALTERACIÓN DE LA SECUENCIA			
[A11] ACCESO NO AUTORIZADO			
[A12] ANÁLISIS DE TRÁFICO			
[A14] INTERCEPTACIÓN DE INFORMACIÓN (ESCUCHA)			
[A15] MODIFICACIÓN DE LA INFORMACIÓN			
[A18] DESTRUCCIÓN DE LA INFORMACIÓN	[9]	[9]	[9]
[A19] REVELACIÓN DE LA INFORMACIÓN			
[A24] DENEGACIÓN DEL SERVICIO	[9]	[9]	[9]

Tabla 249

Impacto acumulado del Sistemas de alimentación ininterrumpida

[UPS_SYT] SISTEMAS DE ALIMENTACIÓN ININTERRUMPIDA			
IMPACTO ACUMULADO			
[N1] FUEGO	[10]	[10]	[10]
[N2] DAÑOS POR AGUA	[9]	[9]	[9]
[N*] DESASTRES NATURALES	[10]	[10]	[10]
[I1] FUEGO	[10]	[10]	[10]
[I2] DAÑOS POR AGUA	[9]	[9]	[9]
[I*] DESASTRES INDUSTRIALES	[10]	[10]	[10]

Continua

[UPS_SYT] SISTEMAS DE ALIMENTACIÓN ININTERRUMPIDA			
IMPACTO ACUMULADO			
[I3] CONTAMINACIÓN MEDIOAMBIENTAL	[9]	[9]	[9]
[E23] ERRORES DE MANTENIMIENTO/ACTUALIZACIÓN DE PROGRAMAS (HARDWARE)	[7]	[7]	[7]
[A7] USO NO PREVISTO	[9]	[9]	[9]
[A23] MANIPULACIÓN DE HARDWARE	[9]	[9]	[9]
[A25] ROBO DE EQUIPOS	[7]	[7]	[7]
[A26] ATAQUE DESTRUCTIVO	[7]	[7]	[7]

Tabla 250

Impacto acumulado del Circuito cerrado de televisión

[CCTV_SYT] CIRCUITO CERRADO DE TELEVISIÓN			
IMPACTO ACUMULADO			
[N1] FUEGO	[10]	[10]	[10]
[N2] DAÑOS POR AGUA	[9]	[9]	[9]
[N*] DESASTRES NATURALES	[10]	[10]	[10]
[I1] FUEGO	[10]	[10]	[10]
[I2] DAÑOS POR AGUA	[9]	[9]	[9]
[I*] DESASTRES INDUSTRIALES	[10]	[10]	[10]
[I3] CONTAMINACIÓN MEDIOAMBIENTAL	[9]	[9]	[9]
[E23] ERRORES DE MANTENIMIENTO/ACTUALIZACIÓN DE PROGRAMAS (HARDWARE)	[7]	[7]	[7]
[A7] USO NO PREVISTO	[9]	[9]	[9]
[A23] MANIPULACIÓN DE HARDWARE	[9]	[9]	[9]
[A25] ROBO DE EQUIPOS	[7]	[7]	[7]
[A26] ATAQUE DESTRUCTIVO	[7]	[7]	[7]

Tabla 251

Impacto acumulado del Sistema de rastreo

[RASTREO_SYT] SISTEMA DE RASTREO			
IMPACTO ACUMULADO			
[N1] FUEGO	[10]	[10]	[10]
[N2] DAÑOS POR AGUA	[9]	[9]	[9]
[N*] DESASTRES NATURALES	[10]	[10]	[10]
[I1] FUEGO	[10]	[10]	[10]
[I2] DAÑOS POR AGUA	[9]	[9]	[9]
[I*] DESASTRES INDUSTRIALES	[10]	[10]	[10]
[I3] CONTAMINACIÓN MEDIOAMBIENTAL	[9]	[9]	[9]
[E23] ERRORES DE MANTENIMIENTO/ACTUALIZACIÓN DE PROGRAMAS (HARDWARE)	[7]	[7]	[7]
[A7] USO NO PREVISTO	[9]	[9]	[9]
[A23] MANIPULACIÓN DE HARDWARE	[9]	[9]	[9]
[A25] ROBO DE EQUIPOS	[7]	[7]	[7]
[A26] ATAQUE DESTRUCTIVO	[7]	[7]	[7]

Tabla 252

Impacto acumulado del Sistema de redes y comunicaciones

[L_SYT] UNIDAD DE SISTEMA DE REDES Y COMUNICACIONES			
IMPACTO ACUMULADO			
[N1] FUEGO	[10]	[10]	[10]
[N2] DAÑOS POR AGUA	[10]	[10]	[10]
[N*] DESASTRES NATURALES	[10]	[10]	[10]
[I1] FUEGO	[10]	[10]	[10]
[I2] DAÑOS POR AGUA	[10]	[10]	[10]

[L_SYT] UNIDAD DE SISTEMA DE REDES Y COMUNICACIONES			
IMPACTO ACUMULADO			
[I*] DESASTRES INDUSTRIALES	[10]	[10]	[10]
[I3] CONTAMINACIÓN MEDIOAMBIENTAL	[7]	[7]	[7]
[I4] CONTAMINACIÓN ELECTROMAGNÉTICA	[7]	[7]	[7]
[I11] EMANACIONES ELECTROMAGNÉTICAS			
[A5] SUPLANTACIÓN DE LA IDENTIDAD			
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	[7]	[7]	[7]
[A7] USO NO PREVISTO	[7]	[7]	[7]
[A11] ACCESO NO AUTORIZADO			
[A26] ATAQUE DESTRUCTIVO	[10]	[10]	[10]
[A27] OCUPACION ENEMIGA	[10]	[10]	[10]

Tabla 253

Impacto acumulado del Responsable del área de sistemas

[GER_SYT] RESPONSABLE DEL ÁREA DE SISTEMAS
IMPACTO ACUMULADO
[E19] FUGAS DE INFORMACIÓN
[A19] REVELACIÓN DE INFORMACIÓN
[A29] EXTORSIÓN
[A30] INGENIERÍA SOCIAL

6.2 RIESGO ACUMULADO

Tabla 254

Riesgo del Transporte de mercancía refrigerada

[TC_SYT] TRANSPORTE DE MERCANCIA REFRIGERADA			
RIESGO ACUMULADO			
[E1] ERRORES DE LOS USUARIOS	{5,4}	{5,4}	{5,4}
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	{5,0}	{5,0}	{5,0}
[E18] DESTRUCCIÓN DE LA INFORMACIÓN	{2,7}	{2,7}	{2,7}
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	{3,6}	{3,6}	{3,6}
[A18] DESTRUCCIÓN DE LA INFORMACIÓN	{6,6}	{6,6}	{6,6}

Tabla 255

Riesgo del alquiler de contenedores

[AC_SYT] ALQUILER DE CONTENEDORES			
RIESGO ACUMULADO			
[E1] ERRORES DE LOS USUARIOS	{3,6}	{3,6}	{3,6}
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	{3,2}	{3,2}	{3,2}
[E18] DESTRUCCIÓN DE LA INFORMACIÓN	{0,98}	{0,98}	{0,98}
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	{1,8}	{1,8}	{1,8}
[A18] DESTRUCCIÓN DE LA INFORMACIÓN	{4,8}	{4,8}	{4,8}

Tabla 256

Riesgo del servicio de montaje y desmontaje

[SMD_SYT] SERVICIO DE MONTAJE Y DESMONTAJE			
RIESGO ACUMULADO			
[E1] ERRORES DE LOS USUARIOS	{3,6}	{3,6}	{3,6}
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	{3,2}	{3,2}	{3,2}
[E18] DESTRUCCIÓN DE LA INFORMACIÓN	{0,98}	{0,98}	{0,98}
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	{1,8}	{1,8}	{1,8}
[A18] DESTRUCCIÓN DE LA INFORMACIÓN	{4,8}	{4,8}	{4,8}

Tabla 257

Riesgo del Portal Web

[WEB_SYT] PORTAL WEB			
RIESGO ACUMULADO			
[I9] INTERRUPCIÓN DE OTROS SERVICIOS O SUMINISTROS ESENCIALES	{1,0}	{1,0}	{1,0}
[E1] ERRORES DE LOS USUARIOS	{0,75}	{0,75}	{0,75}
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	{1,0}	{1,0}	{1,0}
[E18] DESTRUCCIÓN DE LA INFORMACIÓN	{0.75}	{0.75}	{0.75}
[E24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	{1,9}	{1,9}	{1,9}
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	{0.40}	{0.40}	{0.40}
[A7] USO NO PREVISTO	{0.40}	{0.40}	{0.40}
[A18] DESTRUCCIÓN DE LA INFORMACIÓN	{1,0}	{1,0}	{1,0}
[A24] DENEGACIÓN DEL SERVICIO	{1,9}	{1,9}	{1,9}

Tabla 258

Riesgo del Servidor de correo electrónico Zimbra

[ZM_SYT] SERVIDOR DE CORREO ELECTRÓNICO ZIMBRA			
RIESGO ACUMULADO			
[E1] ERRORES DE LOS USUARIOS	{5,1}	{5,1}	{5,1}
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	{5,6}	{5,6}	{5,6}
[E15] ALTERACIÓN DE LA INFORMACIÓN			
[E18] DESTRUCCIÓN DE LA INFORMACIÓN	{5,1}	{5,1}	{5,1}
[E24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	{7,2}	{7,2}	{7,2}
[A5] SUPLANTACIÓN DE LA IDENTIDAD			
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	{3,3}	{3,3}	{3,3}
[A7] USO NO PREVISTO	{3,3}	{3,3}	{3,3}
[A11] ACCESO NO AUTORIZADO			
[A15] MODIFICACIÓN DE LA INFORMACIÓN			
[A18] DESTRUCCIÓN DE LA INFORMACIÓN	{6,3}	{6,3}	{6,3}
[A24] DENEGACIÓN DEL SERVICIO	{7,2}	{7,2}	{7,2}

Tabla 259

Riesgo de la Telefonía IP

[IP_SYT] TELEFONÍA IP			
RIESGO ACUMULADO			
[E1] ERRORES DE LOS USUARIOS	{3,3}	{3,3}	{3,3}
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	{3,8}	{3,8}	{3,8}
[E15] ALTERACIÓN DE LA INFORMACIÓN			

Continua

[IP_SYT] TELEFONÍA IP			
RIESGO ACUMULADO			
[E18] DESTRUCCIÓN DE LA INFORMACIÓN	{3,3}	{3,3}	{3,3}
[E24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	{5,4}	{5,4}	{5,4}
[A5] SUPLANTACIÓN DE LA IDENTIDAD			
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	{1,5}	{1,5}	{1,5}
[A7] USO NO PREVISTO	{1,5}	{1,5}	{1,5}
[A11] ACCESO NO AUTORIZADO			
[A15] MODIFICACIÓN DE LA INFORMACIÓN			
[A18] DESTRUCCIÓN DE LA INFORMACIÓN	{4,5}	{4,5}	{4,5}
[A24] DENEGACIÓN DEL SERVICIO	{5,4}	{5,4}	{5,4}

Tabla 260

Riesgo del Servicio de copias de respaldo

[BACKUP_SYT] SERVICIO DE COPIAS DE RESPALDO			
RIESGO ACUMULADO			
[E1] ERRORES DE LOS USUARIOS	{0,98}	{0,98}	{0,98}
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	{1,5}	{1,5}	{1,5}
[E15] ALTERACIÓN DE LA INFORMACIÓN			
[E18] DESTRUCCIÓN DE LA INFORMACIÓN	{0,98}	{0,98}	{0,98}
[E19] FUGAS DE INFORMACIÓN			
[E24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	{3,1}	{3,1}	{3,1}
[A5] SUPLANTACIÓN DE LA IDENTIDAD			
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	{0,63}	{0,63}	{0,63}
[A7] USO NO PREVISTO	{0,63}	{0,63}	{0,63}

Continua

[BACKUP_SYT] SERVICIO DE COPIAS DE RESPALDO			
RIESGO ACUMULADO			
[A11] ACCESO NO AUTORIZADO			
[A15] MODIFICACIÓN DE LA INFORMACIÓN			
[A18] DESTRUCCIÓN DE LA INFORMACIÓN	{2,2}	{2,2}	{2,2}
[A19] REVELACIÓN DE INFORMACIÓN			
[A24] DENEGACIÓN DEL SERVICIO	{3,1}	{3,1}	{3,1}

Tabla 261

Riesgo de la Información logística

[INF_SYT] INFORMACIÓN LOGÍSTICA			
RIESGO ACUMULADO			
[E1] ERRORES DE LOS USUARIOS	{5,9}	{5,9}	{5,9}
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	{5,6}	{5,6}	{5,6}
[E15] ALTERACION DELA INFORMACIÓN			
[E18] DESTRUCCIÓN DE LA INFORMACIÓN	{3,3}	{3,3}	{3,3}
[E19] FUGAS DE INFORMACIÓN			
[A5] SUPLANTACIÓN DE IDENTIDAD			
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	{4,2}	{4,2}	{4,2}
[A11] ACCESO NO AUTORIZADO			
[A15] MODIFICACIÓN DE LA INFORMACIÓN			
[A18] DESTRUCCIÓN DE LA INFORMACIÓN	{7,2}	{7,2}	{7,2}
[A19] REVELACIÓN DELA INFORMACIÓN			

Tabla 262

Riesgo de la Información por cada departamento

[INT_SYT] INFORMACIÓN POR CADA DEPARTAMENTO			
RIESGO ACUMULADO			
[E1] ERRORES DE LOS USUARIOS	{5,9}	{5,9}	{5,9}
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	{5,6}	{5,6}	{5,6}
[E15] ALTERACIÓN DE LA INFORMACIÓN			
[E18] DESTRUCCIÓN DE LA INFORMACIÓN	{3,3}	{3,3}	{3,3}
[A5] SUPLANTACIÓN DE LA IDENTIDAD			
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	{4,2}	{4,2}	{4,2}
[A11] ACCESO NO AUTORIZADO			
[A15] MODIFICACIÓN DE LA INFORMACIÓN			
[A18] DESTRUCCIÓN DE LA INFORMACIÓN	{7,2}	{7,2}	{7,2}

Tabla 263

Riesgo de la información de Logs

[LOG_SYT] INFORMACIÓN DE REGISTROS DE INGRESOS SOBRE LOS SERVIDORES			
RIESGO ACUMULADO			
[E1] ERRORES DE LOS USUARIOS	{5,4}	{5,4}	{5,4}
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	{5,0}	{5,0}	{5,0}
[E3] ERRORES DE MONITORIZACION (LOG)			
[E15] ALTERACIÓN DE LA INFORMACIÓN			
[E18] DESTRUCCIÓN DE LA INFORMACIÓN	{2,7}	{2,7}	{2,7}
[E19] FUGAS DE INFORMACIÓN			
[A3] MANIPULACIÓN DE LOS REGISTROS DE ACTIVIDAD (LOG)			

[LOG_SYT] INFORMACIÓN DE REGISTROS DE INGRESOS SOBRE LOS SERVIDORES			
RIESGO ACUMULADO			
[A5] SUPLANTACIÓN DE LA IDENTIDAD			
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	{3,6}	{3,6}	{3,6}
[A11] ACCESO NO AUTORIZADO			
[A13] REPUDIO (NEGACIÓN DE ACTUACIONES)			
[A15] MODIFICACIÓN DE LA INFORMACIÓN			
[A18] DESTRUCCIÓN DE LA INFORMACIÓN	{6,6}	{6,6}	{6,6}
[A19] REVELACIÓN DE LA INFORMACIÓN			

Tabla 264

Riesgo de la información personal de cada usuario

[PER_SYT] INFORMACIÓN PERSONAL DE CADA USUARIO			
RIESGO ACUMULADO			
[E1] ERRORES DE LOS USUARIOS	{1,8}	{1,8}	{1,8}
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	{1,5}	{1,5}	{1,5}
[E15] ALTERACIÓN DE LA INFORMACIÓN			
[E18] DESTRUCCIÓN DE LA INFORMACIÓN	{0,63}	{0,63}	{0,63}
[E19] FUGAS DE INFORMACIÓN			
[A5] SUPLANTACIÓN DE LA IDENTIDAD			
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	{0,81}	{0,81}	{0,81}
[A11] ACCESO NO AUTORIZADO			
[A15] MODIFICACIÓN DE LA INFORMACIÓN			
[A18] DESTRUCCIÓN DE LA INFORMACIÓN	{3,1}	{3,1}	{3,1}
[A19] REVELACIÓN DE LA INFORMACIÓN			

Tabla 265

Riesgo del Sistema financiero Nigisu

[NIGISU_SYT] SISTEMA FINANCIERO CONTABLE			
RIESGO ACUMULADO			
[I5] AVERÍA DE ORIGEN FISICO O LÓGICO	{6,3}	{6,3}	{6,3}
[E1] ERRORES DE LOS USUARIOS	{5,9}	{5,9}	{5,9}
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	{5,6}	{5,6}	{5,6}
[E3] ERRORES DE MONITORIZACIÓN (LOG)			
[E8] DIFUSIÓN DE SOFTWARE DAÑINO	{5,1}	{5,1}	{5,1}
[E15] ALTERACIÓN DE LA INFORMACIÓN			
[E18] DESTRUCCIÓN DE LA INFORMACIÓN	{6,3}	{6,3}	{6,3}
[E19] FUGAS DE INFORMACIÓN			
[E20] VULNERABILIDADES DE LOS PROGRAMAS DE SW	{3,3}	{3,3}	{3,3}
[E21] ERRORES DE MANTENIMIENTO/ACTUALIZACIÓN DE PROGRAMAS (SOFTWARE)	{4,2}	{4,2}	{4,2}
[A3] MANIPULACIÓN DE LOS REGISTROS DE ACTIVIDAD (LOG)			
[A5] SUPLANTACIÓN DE LA IDENTIDAD			
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	{4,2}	{4,2}	{4,2}
[A7] USO NO PREVISTO	{3,3}	{3,3}	{3,3}
[A8] DIFUSIÓN DE SOFTWARE DAÑINO	{6,8}	{6,8}	{6,8}
[A11] ACCESO NO AUTORIZADO			
[A13] REPUDIO NEGACIÓN DE LAS ACTUACIONES			
[A15] MODIFICACIÓN DE LA INFORMACIÓN			
[A18] DESTRUCCIÓN DE LA INFORMACIÓN	{7,2}	{7,2}	{7,2}
[A19] REVELACIÓN DE LA INFORMACIÓN			
[A22] MANIPULACIÓN DE PROGRAMAS	{6,3}	{6,3}	{6,3}

Tabla 266

Riesgo de la Ofimática

[OFF_SYT] OFIMÁTICA			
RIESGO ACUMULADO			
[I5] AVERÍA DE ORIGEN FÍSICO O LÓGICO	{6,3}	{6,3}	{6,3}
[E1] ERRORES DE LOS USUARIOS	{3,3}	{3,3}	{3,3}
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	{5,6}	{5,6}	{5,6}
[E8] DIFUSIÓN DE SOFTWARE DAÑINO	{5,1}	{5,1}	{5,1}
[E15] ALTERACIÓN DE LA INFORMACIÓN			
[E18] DESTRUCCIÓN DE LA INFORMACIÓN	{6,3}	{6,3}	{6,3}
[E19] FUGAS DE INFORMACIÓN			
[E20] VULNERABILIDADES DE LOS PROGRAMAS DE SW	{3,3}	{3,3}	{3,3}
[E21] ERRORES DE MANTENIMIENTO/ACTUALIZACIÓN DE PROGRAMAS (SOFTWARE)	{4,2}	{4,2}	{4,2}
[A5] SUPLANTACIÓN DE LA IDENTIDAD			
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	{3,3}	{3,3}	{3,3}
[A7] USO NO PREVISTO	{3,3}	{3,3}	{3,3}
[A8] DIFUSIÓN DE SOFTWARE DAÑINO	{6,8}	{6,8}	{6,8}
[A11] ACCESO NO AUTORIZADO			
[A15] MODIFICACIÓN DE LA INFORMACIÓN	{6,3}	{6,3}	{6,3}
[A18] DESTRUCCIÓN DE LA INFORMACIÓN			
[A19] REVELACIÓN DE LA INFORMACIÓN	{6,3}	{6,3}	{6,3}
[A22] MANIPULACIÓN DE PROGRAMAS			

Tabla 267

Riesgo del Antivirus

[AV_SYT] ANTIVIRUS
RIESGO ACUMULADO
[E1] ERRORES DE LOS USUARIOS
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD
[E8] DIFUSIÓN DE SOFTWARE DAÑINO
[E19] FUGAS DE INFORMACIÓN
[E20] VULNERABILIDADES DE LOS PROGRAMAS DE SW
[A5] SUPLANTACIÓN DE LA IDENTIDAD
[A6] ABUSO DE PRIVILEGIOS DE ACCESO
[A7] USO NO PREVISTO
[A8] DIFUSIÓN DE SOFTWARE DAÑINO
[A11] ACCESO NO AUTORIZADO
[A19] REVELACIÓN DE LA INFORMACIÓN
[A22] MANIPULACIÓN DE PROGRAMAS

Tabla 268

Riesgo de Otros Software

[OTR_SYT] OTROS SOFTWARE			
RIESGO ACUMULADO			
[I5] AVERÍA DE ORIGEN FÍSICO O LÓGICO	{1,0}	{1,0}	{1,0}
[E1] ERRORES DE LOS USUARIOS	{0,40}	{0,40}	{0,40}
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	{0,86}	{0,86}	{0,86}
[E8] DIFUSIÓN DE SOFTWARE DAÑINO	{0,75}	{0,75}	{0,75}
[E18] DESTRUCCIÓN DE LA INFORMACIÓN	{1,0}	{1,0}	{1,0}

Continua

[OTR_SYT] OTROS SOFTWARE			
RIESGO ACUMULADO			
[E20] VULNERABILIDADES DE LOS PROGRAMAS DE SW	{0,40}	{0,40}	{0,40}
[E21] ERRORES DE MANTENIMIENTO/ACTUALIZACIÓN DE PROGRAMAS (SOFTWARE)	{0,57}	{0,57}	{0,57}
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	{0,40}	{0,40}	{0,40}
[A7] USO NO PREVISTO	{0,40}	{0,40}	{0,40}
[A8] DIFUSIÓN DE SOFTWARE DAÑINO	{1,5	{1,5	{1,5
[A18] DESTRUCCIÓN DE LA INFORMACIÓN	{1,0}	{1,0}	{1,0}
[A22] MANIPULACIÓN DE PROGRAMAS	{1,0}	{1,0}	{1,0}

Tabla 269

Riesgo del Internet

[IEX_SYT] INTERNET			
RIESGO ACUMULADO			
[I5] AVERÍA DE ORIGEN FÍSICO O LÓGICO	{6,3}	{6,3}	{6,3}
[E1] ERRORES DE LOS USUARIOS	{3,3}	{3,3}	{3,3}
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	{5,6}	{5,6}	{5,6}
[E8] DIFUSIÓN DE SOFTWARE DAÑINO	{5,1}	{5,1}	{5,1}
[E15] ALTERACION DE LA INFORMACIÓN			
[E18] DESTRUCCIÓN DE LA INFORMACIÓN	{6,3}	{6,3}	{6,3}
[E20] VULNERABILIDADES DE LOS PROGRAMAS DE SW	{3,3}	{3,3}	{3,3}
[E21] ERRORES DE MANT/ACT DE PROG (SW	{4,2}	{4,2}	{4,2}
[A5] SUPLANTACIÓN DE LA IDENTIDAD			
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	{3,3}	{3,3}	{3,3}
[A7] USO NO PREVISTO	{3,3}	{3,3}	{3,3}
[A8] DIFUSIÓN DE SOFTWARE DAÑINO	{6,8}	{6,8}	{6,8}
[A18] DESTRUCCIÓN DE LA INFORMACIÓN	{6,3}	{6,3}	{6,3}
[A22] MANIPULACIÓN DE PROGRAMAS	{6,3}	{6,3}	{6,3}

Tabla 270

Riesgo del Servidor de Base de datos

[SBD_SYT] SERVIDOR DE BASE DE DATOS			
RIESGO ACUMULADO			
[N1] FUEGO	{5,9}	{5,9}	{5,9}
[N2] DAÑOS POR AGUA	{5,4}	{5,4}	{5,4}
[N*] DESASTRES NATURALES	{5,9}	{5,9}	{5,9}
[I1] FUEGO	{6,6}	{6,6}	{6,6}
[I2] DAÑOS POR AGUA	{6,0}	{6,0}	{6,0}
[I*] DESASTRES INDUSTRIALES	{6,6}	{6,6}	{6,6}
[I3] CONTAMINACIÓN MEDIO AMBIENTAL	{5,4}	{5,4}	{5,4}
[I4] CONTAMINACIÓN ELECTROMAGNÉTICA	{5,1}	{5,1}	{5,1}
[I5] AVERÍA DE ORIGEN FÍSICO O LÓGICO	{6,3}	{6,3}	{6,3}
[I6] CORTE DEL SUMINISTRO ELÉCTRICO	{6,8}	{6,8}	{6,8}
[I7] CONDICIONES INADECUADAS DE TEMPERATURA O HUMEDAD	{6,8}	{6,8}	{6,8}
[I11] EMANACIONES ELECTROMAGNÉTICAS			
[E1] ERRORES DE LOS USUARIOS	{5,9}	{5,9}	{5,9}
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	{5,6}	{5,6}	{5,6}
[E8] DIFUSIÓN DE SOFTWARE DAÑINO	{5,1}	{5,1}	{5,1}
[E15] ALTERACIÓN DE LA INFORMACIÓN			
[E18] DESTRUCCIÓN DE LA INFORMACIÓN	{6,3}	{6,3}	{6,3}
[E19] FUGAS DE INFORMACIÓN			
[E20] VULNERABILIDADES DE LOS PROGRAMAS	{3,3}	{3,3}	{3,3}
[E21] ERRORES DE MANTENIMIENTO/ACTUALIZACIÓN DE PROGRAMAS (SOFTWARE)	{4,2}	{4,2}	{4,2}

Continua

[SBD_SYT] SERVIDOR DE BASE DE DATOS			
RIESGO ACUMULADO			
[E23] ERRORES DE MANTENIMIENTO/ACTUALIZACIÓN DE PROGRAMAS (HARDWARE)	{5,1}	{5,1}	{5,1}
[E24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	{7,2}	{7,2}	{7,2}
[E25] PÉRDIDA DE EQUIPOS	{6,8}	{6,8}	{6,8}
[A5] SUPLANTACIÓN DE LA IDENTIDAD			
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	{5,9}	{5,9}	{5,9}
[A7] USO NO PREVISTO	{5,1}	{5,1}	{5,1}
[A8] DIFUSIÓN DE SOFTWARE DAÑINO	{6,8}	{6,8}	{6,8}
[A11] ACCESO NO AUTORIZADO	{6,8}	{6,8}	{6,8}
[A15] MODIFICACIÓN DE LA INFORMACIÓN			
[A18] DESTRUCCIÓN DE LA INFORMACIÓN	{7,2}	{7,2}	{7,2}
[A19] REVELACIÓN DE LA INFORMACIÓN			
[A22] MANIPULACIÓN DE PROGRAMAS	{6,3}	{6,3}	{6,3}
[A23] MANIPULACIÓN DE HARDWARE	{6,0}	{6,0}	{6,0}
[A24] DENEGACIÓN DEL SERVICIO	{7,1}	{7,1}	{7,1}
[A25] ROBO DE EQUIPOS	{6,6}	{6,6}	{6,6}
[A26] ATAQUE DESTRUCTIVO	{6,8}	{6,8}	{6,8}

Tabla 271

Riesgo del Firewall

[FIREWALL_SYT] FIREWALL			
RIESGO ACUMULADO			
[N1] FUEGO	{5,9}	{5,9}	{5,9}
[N2] DAÑOS POR AGUA	{5,4}	{5,4}	{5,4}
[N*] DESASTRES NATURALES	{5,9}	{5,9}	{5,9}

Continua

[FIREWALL_SYT] FIREWALL			
RIESGO ACUMULADO			
[I1] FUEGO	{6,6}	{6,6}	{6,6}
[I2] DAÑOS POR AGUA	{6,0}	{6,0}	{6,0}
[I*] DESASTRES INDUSTRIALES	{6,6}	{6,6}	{6,6}
[I3] CONTAMINACIÓN MEDIOAMBIENTAL	{5,4}	{5,4}	{5,4}
[I4] CONTAMINACIÓN ELECTROMAGNÉTICA	{5,1}	{5,1}	{5,1}
[I5] AVERÍA DE ORIGEN FÍSICO O LÓGICO	{6,3}	{6,3}	{6,3}
[I6] CORTE DEL SUMINISTRO ELÉCTRICO	{6,8}	{6,8}	{6,8}
[I7] CONDICIONES INADECUADAS DE TEMPERATURA O HUMEDAD	{6,8}	{6,8}	{6,8}
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	{5,6}	{5,6}	{5,6}
[E23] ERRORES DE MANTENIMIENTO/ACTUALIZACIÓN DE PROGRAMAS (HARDWARE)	{5,1}	{5,1}	{5,1}
[E24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	{7,2}	{7,2}	{7,2}
[E25] PÉRDIDA DE EQUIPOS	{6,8}	{6,8}	{6,8}
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	{5,1}	{5,1}	{5,1}
[A7] USO NO PREVISTO	{5,1}	{5,1}	{5,1}
[A11] ACCESO NO AUTORIZADO	{5,1}	{5,1}	{5,1}
[A23] MANIPULACIÓN DE HARDWARE	{6,6}	{6,6}	{6,6}
[A24] DENEGACIÓN DEL SERVICIO	{7,1}	{7,1}	{7,1}
[A25] ROBO DE EQUIPOS	{6,6}	{6,6}	{6,6}
[A26] ATAQUE DESTRUCTIVO	{6,8}	{6,8}	{6,8}

Tabla 272

Riesgo de las Computadoras de escritorio

[DESKTOP_SYT] COMPUTADORAS DE ESCRITORIO			
RIESGO ACUMULADO			
[N1] FUEGO	{1,8}	{1,8}	{1,8}
[N2] DAÑOS POR AGUA	{1,3}	{1,3}	{1,3}
[N*] DESASTRES NATURALES	{1,8}	{1,8}	{1,8}
[I1] FUEGO	{2,4}	{2,4}	{2,4}
[I2] DAÑOS POR AGUA	{1,9}	{1,9}	{1,9}
[I*] DESASTRES INDUSTRIALES	{2,4}	{2,4}	{2,4}
[I3] CONTAMINACIÓN MEDIOAMBIENTAL	{1,3}	{1,3}	{1,3}
[I4] CONTAMINACIÓN ELECTROMAGNÉTICA			
[I5] AVERÍA DE ORIGEN FÍSICO O LÓGICO	{0,98}	{0,98}	{0,98}
[I6] CORTE DEL SUMINISTRO ELÉCTRICO	{2,2}	{2,2}	{2,2}
[I7] CONDICIONES INADECUADAS DE TEMPERATURA O HUMEDAD	{2,7}	{2,7}	{2,7}
[I11] EMANACIONES ELECTROMAGNÉTICAS	{2,7}	{2,7}	{2,7}
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD			
[E23] ERRORES DE MANT/ACT DE PROG (HW)	{1,5}	{1,5}	{1,5}
[E24] CAÍDA DEL SIST POR AGOTAM DE RECURSOS	{0,98}	{0,98}	{0,98}
[E25] PÉRDIDA DE EQUIPOS	{3,1}	{3,1}	{3,1}
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	{2,7}	{2,7}	{2,7}
[A7] USO NO PREVISTO	{0,98}	{0,98}	{0,98}
[A11] ACCESO NO AUTORIZADO	{0,98}	{0,98}	{0,98}
[A23] MANIPULACIÓN DE HARDWARE	{0,98}	{0,98}	{0,98}
[A24] DENEGACIÓN DEL SERVICIO	{1,9}	{1,9}	{1,9}
[A25] ROBO DE EQUIPOS	{3,0}	{3,0}	{3,0}
[A26] ATAQUE DESTRUCTIVO	{2,4}	{2,4}	{2,4}

Tabla 273

Riesgo de Computadoras portátiles

[LAPTOPS_SYT] COMPUTADORAS PORTÁTILES			
RIESGO ACUMULADO			
[N1] FUEGO	{1,8}	{1,8}	{1,8}
[N2] DAÑOS POR AGUA	{1,3}	{1,3}	{1,3}
[N*] DESASTRES NATURALES	{1,8}	{1,8}	{1,8}
[I1] FUEGO	{2,4}	{2,4}	{2,4}
[I2] DAÑOS POR AGUA	{1,9}	{1,9}	{1,9}
[I*] DESASTRES INDUSTRIALES	{2,4}	{2,4}	{2,4}
[I3] CONTAMINACIÓN MEDIO AMBIENTAL	{1,3}	{1,3}	{1,3}
[I4] CONTAMINACIÓN ELECTROMAGNÉTICA	{0,98}	{0,98}	{0,98}
[I5] AVERÍA DE ORIGEN FÍSICO O LÓGICO	{2,2}	{2,2}	{2,2}
[I6] CORTE DEL SUMINISTRO ELÉCTRICO	{2,7}	{2,7}	{2,7}
[I7] CONDICIONES INADECUADAS DE TEMPERATURA O HUMEDAD	{2,7}	{2,7}	{2,7}
[I11] EMANACIONES ELECTROMAGNÉTICAS			
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	{1,5}	{1,5}	{1,5}
[[E23] ERRORES DE MANT/ACT DE PROG (HW)	{0,98}	{0,98}	{0,98}
[E24] CAÍDA DEL SIST POR AGOT DE RECURSOS	{3,1}	{3,1}	{3,1}
[E25] PÉRDIDA DE EQUIPOS	{2,7}	{2,7}	{2,7}
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	{0,98}	{0,98}	{0,98}
[A7] USO NO PREVISTO	{0,98}	{0,98}	{0,98}
[A11] ACCESO NO AUTORIZADO	{0,98}	{0,98}	{0,98}
[A23] MANIPULACIÓN DE HARDWARE	{1,9}	{1,9}	{1,9}
[A24] DENEGACIÓN DEL SERVICIO	{3,0}	{3,0}	{3,0}
[A25] ROBO DE EQUIPOS	{2,4}	{2,4}	{2,4}
[A26] ATAQUE DESTRUCTIVO	{2,7	{2,7	{2,7

Tabla 274

Riesgo del Scanner

[SCAN_SYT] SCANNER			
RIESGO ACUMULADO			
[N1] FUEGO	{0,81}	{0,81}	{0,81}
[N2] DAÑOS POR AGUA	{0,70}	{0,70}	{0,70}
[N*] DESASTRES NATURALES	{0,81}	{0,81}	{0,81}
[I1] FUEGO	{0,93}	{0,93}	{0,93}
[I2] DAÑOS POR AGUA	{0,83}	{0,83}	{0,83}
[I*] DESASTRES INDUSTRIALES	{0,93}	{0,93}	{0,93}
[I3] CONTAMINACIÓN MEDIOAMBIENTAL	{0,70}	{0,70}	{0,70}
[I4] CONTAMINACIÓN ELECTROMAGNÉTICA	{0.63}	{0.63}	{0.63}
[I5] AVERÍA DE ORIGEN FÍSICO O LÓGICO	{0.88}	{0.88}	{0.88}
[I6] CORTE DEL SUMINISTRO ELÉCTRICO	{0.98}	{0.98}	{0.98}
[I7] CONDICIONES INADECUADAS DE TEMPERATURA O HUMEDAD	{0,98}	{0,98}	{0,98}
[I11] EMANACIONES ELECTROMAGNÉTICAS			
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	{0,74}	{0,74}	{0,74}
[E23] ERRORES DE MANT/ACT DE PROG (HW)	{0,63}	{0,63}	{0,63}
[E24] CAÍDA DEL SIST POR AGOT DE RECURSOS	{1,30}	{1,30}	{1,30}
[E25] PÉRDIDA DE EQUIPOS	{0,98}	{0,98}	{0,98}
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	{0,63}	{0,63}	{0,63}
[A7] USO NO PREVISTO	{0,63}	{0,63}	{0,63}
[A11] ACCESO NO AUTORIZADO	{0,63}	{0,63}	{0,63}
[A23] MANIPULACIÓN DE HARDWARE	{0,83}	{0,83}	{0,83}
[A24] DENEGACIÓN DEL SERVICIO	{1,20}	{1,20}	{1,20}
[A25] ROBO DE EQUIPOS	{0,93}	{0,93}	{0,93}
[A26] ATAQUE DESTRUCTIVO	{0,98}	{0,98}	{0,98}

Tabla 275

Riesgo de las Impresoras matriciales

[PRINT1_SYT] IMPRESORAS MATRICIALES			
RIESGO ACUMULADO			
[N1] FUEGO	{0,93}	{0,93}	{0,93}
[N2] DAÑOS POR AGUA	{0,82}	{0,82}	{0,82}
[N*] DESASTRES NATURALES	{0,93}	{0,93}	{0,93}
[I1] FUEGO	{1,30}	{1,30}	{1,30}
[I2] DAÑOS POR AGUA	{0,94}	{0,94}	{0,94}
[I*] DESASTRES INDUSTRIALES	{1,30}	{1,30}	{1,30}
[I3] CONTAMINACIÓN MEDIOAMBIENTAL	{0,82}	{0,82}	{0,82}
[I4] CONTAMINACIÓN ELECTROMAGNÉTICA	{0.75}	{0.75}	{0.75}
[I5] AVERÍA DE ORIGEN FÍSICO O LÓGICO	{1,0}	{1,0}	{1,0}
[I6] CORTE DEL SUMINISTRO ELÉCTRICO	{1,5}	{1,5}	{1,5}
[I7] CONDICIONES INADECUADAS DE TEMPERATURA O HUMEDAD	{1,5}	{1,5}	{1,5}
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	{0,86}	{0,86}	{0,86}
[E23] ERRORES DE MANT/ACT DE PROG (HW)	{0,75}	{0,75}	{0,75}
[E24] CAÍDA DEL SIST POR AGOT DE RECURSOS	{1,90}	{1,90}	{1,90}
[E25] PÉRDIDA DE EQUIPOS	{1,50}	{1,50}	{1,50}
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	{0,75}	{0,75}	{0,75}
[A7] USO NO PREVISTO	{0,75}	{0,75}	{0,75}
[A11] ACCESO NO AUTORIZADO	{0,75}	{0,75}	{0,75}
[A23] MANIPULACIÓN DE HARDWARE	{0,94}	{0,94}	{0,94}
[A24] DENEGACIÓN DEL SERVICIO	{1,80}	{1,80}	{1,80}
[A25] ROBO DE EQUIPOS	{1,30}	{1,30}	{1,30}
[A26] ATAQUE DESTRUCTIVO	{1,50}	{1,50}	{1,50}

Tabla 276

Riesgo de Impresora Laser

[PRINT2_SYT] IMPRESORA LASER			
RIESGO ACUMULADO			
[N1] FUEGO	{0,93}	{0,93}	{0,93}
[N2] DAÑOS POR AGUA	{0,82}	{0,82}	{0,82}
[N*] DESASTRES NATURALES	{0,93}	{0,93}	{0,93}
[I1] FUEGO	{1,30}	{1,30}	{1,30}
[I2] DAÑOS POR AGUA	{0.94}	{0.94}	{0.94}
[I*] DESASTRES INDUSTRIALES	{1,30}	{1,30}	{1,30}
[I3] CONTAMINACIÓN MEDIO AMBIENTAL	{0,82}	{0,82}	{0,82}
[I4] CONTAMINACIÓN ELECTROMAGNÉTICA	{0,75}	{0,75}	{0,75}
[I5] AVERÍA DE ORIGEN FÍSICO O LÓGICO	{1,0}	{1,0}	{1,0}
[I6] CORTE DEL SUMINISTRO ELÉCTRICO	{1,5}	{1,5}	{1,5}
[I7] CONDICIONES INADECUADAS DE TEMPERATURA O HUMEDAD	{1,5}	{1,5}	{1,5}
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	{0,86}	{0,86}	{0,86}
[E23] ERRORES DE MANT/ACT DE PROG (HW)	{0,75}	{0,75}	{0,75}
[E24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	{1,9}	{1,9}	{1,9}
[E25] PÉRDIDA DE EQUIPOS	{1,5}	{1,5}	{1,5}
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	{0,75}	{0,75}	{0,75}
[A7] USO NO PREVISTO	{0,75}	{0,75}	{0,75}
[A11] ACCESO NO AUTORIZADO	{0,75}	{0,75}	{0,75}
[A23] MANIPULACIÓN DE HARDWARE	{0,94}	{0,94}	{0,94}
[A24] DENEGACIÓN DEL SERVICIO	{1,80}	{1,80}	{1,80}
[A25] ROBO DE EQUIPOS	{1,30}	{1,30}	{1,30}
[A26] ATAQUE DESTRUCTIVO	{1,5}	{1,5}	{1,5}

Tabla 277

Riesgo del Switch

[SWITCH_SYT] SWITCH			
RIESGO ACUMULADO			
[N1] FUEGO	{5,9}	{5,9}	{5,9}
[N2] DAÑOS POR AGUA	{5,4}	{5,4}	{5,4}
[N*] DESASTRES NATURALES	{5,9}	{5,9}	{5,9}
[I1] FUEGO	{6,6}	{6,6}	{6,6}
[I2] DAÑOS POR AGUA	{6,0}	{6,0}	{6,0}
[I*] DESASTRES INDUSTRIALES	{6,6}	{6,6}	{6,6}
[I3] CONTAMINACIÓN MEDIOAMBIENTAL	{5,4}	{5,4}	{5,4}
[I4] CONTAMINACIÓN ELECTROMAGNÉTICA	{5,1}	{5,1}	{5,1}
[I5] AVERÍA DE ORIGEN FÍSICO O LÓGICO	{6,3}	{6,3}	{6,3}
[I6] CORTE DEL SUMINISTRO ELÉCTRICO	{6,8}	{6,8}	{6,8}
[I7] CONDICIONES INADECUADAS DE TEMPERATURA O HUMEDAD	{6,8}	{6,8}	{6,8}
[I11] EMANACIONES ELECTROMAGNÉTICAS			
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	{5,6}	{5,6}	{5,6}
[E23] ERRORES DE MANT/ACT DE PROG (HW)	{5,1}	{5,1}	{5,1}
[E24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	{7,2}	{7,2}	{7,2}
[E25] PÉRDIDA DE EQUIPOS	{6,8}	{6,8}	{6,8}
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	{5,1}	{5,1}	{5,1}
[A7] USO NO PREVISTO	{5,1}	{5,1}	{5,1}
[A11] ACCESO NO AUTORIZADO	{5,1}	{5,1}	{5,1}
[A23] MANIPULACIÓN DE HARDWARE	{6,6}	{6,6}	{6,6}
[A24] DENEGACIÓN DEL SERVICIO	{7,1}	{7,1}	{7,1}
[A25] ROBO DE EQUIPOS	{6,6}	{6,6}	{6,6}
[A26] ATAQUE DESTRUCTIVO	{6,8}	{6,8}	{6,8}

Tabla 278

Riesgo del Router

[ROUTER_SYT] ROUTER			
RIESGO ACUMULADO			
[N1] FUEGO	{5,9}	{5,9}	{5,9}
[N2] DAÑOS POR AGUA	{5,4}	{5,4}	{5,4}
[N*] DESASTRES NATURALES	{5,9}	{5,9}	{5,9}
[I1] FUEGO	{6,6}	{6,6}	{6,6}
[I2] DAÑOS POR AGUA	{6,0}	{6,0}	{6,0}
[I*] DESASTRES INDUSTRIALES	{6,6}	{6,6}	{6,6}
[I3] CONTAMINACIÓN MEDIOAMBIENTAL	{5,4}	{5,4}	{5,4}
[I4] CONTAMINACIÓN ELECTROMAGNÉTICA	{5,1}	{5,1}	{5,1}
[I5] AVERÍA DE ORIGEN FÍSICO O LÓGICO	{6,3}	{6,3}	{6,3}
[I6] CORTE DEL SUMINISTRO ELÉCTRICO	{6,8}	{6,8}	{6,8}
[I7] CONDICIONES INADECUADAS DE TEMPERATURA O HUMEDAD	{6,8}	{6,8}	{6,8}
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	{5,6}	{5,6}	{5,6}
[E23] ERRORES DE MANT/ACT DE PROG (HW)	{5,1}	{5,1}	{5,1}
[E24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	{7,2}	{7,2}	{7,2}
[E25] PÉRDIDA DE EQUIPOS	{6,8}	{6,8}	{6,8}
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	{5,1}	{5,1}	{5,1}
[A7] USO NO PREVISTO	{5,1}	{5,1}	{5,1}
[A11] ACCESO NO AUTORIZADO	{5,1}	{5,1}	{5,1}
[A23] MANIPULACIÓN DE HARDWARE	{6,6}	{6,6}	{6,6}
[A24] DENEGACIÓN DEL SERVICIO	{7,1}	{7,1}	{7,1}
[A25] ROBO DE EQUIPOS	{6,6}	{6,6}	{6,6}
[A26] ATAQUE DESTRUCTIVO	{6,8}	{6,8}	{6,8}

[GTWY_SYT] GATEWAY

RIESGO ACUMULADO			
[N1] FUEGO	{5,9}	{5,9}	{5,9}
[N2] DAÑOS POR AGUA	{5,4}	{5,4}	{5,4}
[N*] DESASTRES NATURALES	{5,9}	{5,9}	{5,9}
[I1] FUEGO	{6,6}	{6,6}	{6,6}
[I2] DAÑOS POR AGUA	{6,0}	{6,0}	{6,0}
[I*] DESASTRES INDUSTRIALES	{6,6}	{6,6}	{6,6}
[I3] CONTAMINACIÓN MEDIOAMBIENTAL	{5,4}	{5,4}	{5,4}
[I4] CONTAMINACIÓN ELECTROMAGNÉTICA	{5,1}	{5,1}	{5,1}
[I5] AVERÍA DE ORIGEN FÍSICO O LÓGICO	{6,3}	{6,3}	{6,3}
[I6] CORTE DEL SUMINISTRO ELÉCTRICO	{6,8}	{6,8}	{6,8}
[I7] CONDICIONES INADECUADAS DE TEMPERATURA O HUMEDAD	{6,8}	{6,8}	{6,8}
[I11] EMANACIONES ELECTROMAGNÉTICAS			
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	{5,6}	{5,6}	{5,6}
[E23] ERRORES DE MANTENIMIENTO/ACTUALIZACIÓN DE PROGRAMAS (HARDWARE)	{5,1}	{5,1}	{5,1}
[E24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	{7,2}	{7,2}	{7,2}
[E25] PÉRDIDA DE EQUIPOS	{6,8}	{6,8}	{6,8}
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	{5,1}	{5,1}	{5,1}
[A7] USO NO PREVISTO	{5,1}	{5,1}	{5,1}
[A11] ACCESO NO AUTORIZADO	{5,1}	{5,1}	{5,1}
[A23] MANIPULACIÓN DE HARDWARE	{6,6}	{6,6}	{6,6}
[A24] DENEGACIÓN DEL SERVICIO	{7,1}	{7,1}	{7,1}
[A25] ROBO DE EQUIPOS	{6,6}	{6,6}	{6,6}
[A26] ATAQUE DESTRUCTIVO	{6,8}	{6,8}	{6,8}

Tabla 279

Riesgo de los Puntos de acceso Wireless

[WIFI_SYT] PUNTOS DE ACCESO WIRELESS			
RIESGO ACUMULADO			
[N1] FUEGO	{5,9}	{5,9}	{5,9}
[N2] DAÑOS POR AGUA	{5,4}	{5,4}	{5,4}
[N*] DESASTRES NATURALES	{5,9}	{5,9}	{5,9}
[I1] FUEGO	{6,6}	{6,6}	{6,6}
[I2] DAÑOS POR AGUA	{6,0}	{6,0}	{6,0}
[I*] DESASTRES INDUSTRIALES	{6,6}	{6,6}	{6,6}
[I3] CONTAMINACIÓN MEDIOAMBIENTAL	{5,4}	{5,4}	{5,4}
[I4] CONTAMINACIÓN ELECTROMAGNÉTICA	{5,1}	{5,1}	{5,1}
[I5] AVERÍA DE ORIGEN FÍSICO O LÓGICO	{6,3}	{6,3}	{6,3}
[I6] CORTE DEL SUMINISTRO ELÉCTRICO	{6,8}	{6,8}	{6,8}
[I7] CONDICIONES INADECUADAS DE TEMPERATURA O HUMEDAD	{6,8}	{6,8}	{6,8}
[I11] EMANACIONES ELECTROMAGNÉTICAS			
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	{5,6}	{5,6}	{5,6}
[E23] ERRORES DE MANT/ACT DE PROG (HW)	{5,1}	{5,1}	{5,1}
[E24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	{7,2}	{7,2}	{7,2}
[E25] PÉRDIDA DE EQUIPOS	{6,8}	{6,8}	{6,8}
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	{5,1}	{5,1}	{5,1}
[A7] USO NO PREVISTO	{5,1}	{5,1}	{5,1}
[A11] ACCESO NO AUTORIZADO	{5,1}	{5,1}	{5,1}
[A23] MANIPULACIÓN DE HARDWARE	{6,6}	{6,6}	{6,6}
[A24] DENEGACIÓN DEL SERVICIO	{7,1}	{7,1}	{7,1}
[A25] ROBO DE EQUIPOS	{6,6}	{6,6}	{6,6}
[A26] ATAQUE DESTRUCTIVO	{6,8}	{6,8}	{6,8}

Tabla 280

Riesgo de la Central Telefónica

[PABX_SYT] CENTRAL TELEFÓNICA			
RIESGO ACUMULADO			
[N1] FUEGO	[4,2}	[4,2}	[4,2}
[N2] DAÑOS POR AGUA	{3,7}	{3,7}	{3,7}
[N*] DESASTRES NATURALES	[4,2}	[4,2}	[4,2}
[I1] FUEGO	{4,8}	{4,8}	{4,8}
[I2] DAÑOS POR AGUA	{4,3}	{4,3}	{4,3}
[I*] DESASTRES INDUSTRIALES	{4,8}	{4,8}	{4,8}
[I3] CONTAMINACIÓN MEDIO AMBIENTAL	{3,7}	{3,7}	{3,7}
[I4] CONTAMINACIÓN ELECTROMAGNÉTICA	{3,3}	{3,3}	{3,3}
[I5] AVERÍA DE ORIGEN FÍSICO O LÓGICO	{4,5}	{4,5}	{4,5}
[I6] CORTE DEL SUMINISTRO ELÉCTRICO	{5,1}	{5,1}	{5,1}
[I7] CONDICIONES INADECUADAS DE TEMPERATURA O HUMEDAD	{5,1}	{5,1}	{5,1}
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	{3,8}	{3,8}	{3,8}
[E23] ERRORES DE MANT/ACT DE PROG (HW)	{3,3}	{3,3}	{3,3}
[E24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	{5,4}	{5,4}	{5,4}
[E25] PÉRDIDA DE EQUIPOS	{5,1}	{5,1}	{5,1}
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	{3,3}	{3,3}	{3,3}
[A7] USO NO PREVISTO	{3,3}	{3,3}	{3,3}
[A11] ACCESO NO AUTORIZADO	{3,3}	{3,3}	{3,3}
[A23] MANIPULACIÓN DE HARDWARE	{4,3}	{4,3}	{4,3}
[A24] DENEGACIÓN DEL SERVICIO	{5,3}	{5,3}	{5,3}
[A25] ROBO DE EQUIPOS	{4,8}	{4,8}	{4,8}
[A26] ATAQUE DESTRUCTIVO	{5,1}	{5,1}	{5,1}

Tabla 281

Riesgo de la Red Telefónica

[PSTN_SYT] RED TELEFÓNICA			
RIESGO ACUMULADO			
[I8] FALLO DE SERVICIOS DE COMUNICACIONES	{4,5}	{4,5}	{4,5}
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	{3,8}	{3,8}	{3,8}
[E10] ERRORES DE SECUENCIA			
[E15] ALTERACIÓN DE LA INFORMACIÓN			
[E24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	{4,5}	{4,5}	{4,5}
[A5] SUPLANTACIÓN DE LA IDENTIDAD			
[A6] ABUSO DE PRIVILEGIOS DE ACCESO			
[A7] USO NO PREVISTO	{3,3}	{3,3}	{3,3}
[A10] ALTERACIÓN DE LA SECUENCIA			
[A11] ACCESO NO AUTORIZADO			
[A15] MODIFICACIÓN DE LA INFORMACIÓN			
[A18] DESTRUCCIÓN DE LA INFORMACIÓN	{4,5}	{4,5}	{4,5}
[A24] DENEGACIÓN DEL SERVICIO	{5,4}	{5,4}	{5,4}

Tabla 282

Riesgo de la Red inalámbrica

[RADIO_SYT] RED INHALÁMBRICA			
RIESGO ACUMULADO			
[I8] FALLO DE SERVICIOS DE COMUNICACIONES	{6,3}	{6,3}	{6,3}
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	{5,6}	{5,6}	{5,6}
[E9] ERRORES DE [RE-]ENCAMINAMIENTO			

Continua

[RADIO_SYT] RED INHALÁMBRICA			
RIESGO ACUMULADO			
[E10] ERRORES DE SECUENCIA			
[E15] ALTERACIÓN DE LA INFORMACIÓN			
[E19] FUGAS DE INFORMACIÓN			
[E24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	{6,3}	{6,3}	{6,3}
[A5] SUPLANTACIÓN DE LA IDENTIDAD			
[A6] ABUSO DE PRIVILEGIOS DE ACCESO			
[A7] USO NO PREVISTO	{5,1}	{5,1}	{5,1}
[A9] [RE-]ECAMINAMIENTO DE MENSAJES			
[A10] ALTERACIÓN DE LA SECUENCIA			
[A11] ACCESO NO AUTORIZADO			
[A12] ANÁLISIS DE TRÁFICO			
[A14] INTERCEPTACIÓN DE INFORMACIÓN (ESCUCHA)			
[A15] MODIFICACIÓN DE LA INFORMACIÓN			
[A18] DESTRUCCIÓN DE LA INFORMACIÓN	{6,3}	{6,3}	{6,3}
[A19] REVELACIÓN DE LA INFORMACIÓN			
[A24] DENEGACIÓN DEL SERVICIO	{7,2}	{7,2}	{7,2}

Tabla 283

Riesgo de la Red Lan

[LAN_SYT] RED LAN			
RIESGO ACUMULADO			
[I8] FALLO DE SERVICIOS DE COMUNICACIONES	{6,3}	{6,3}	
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	{5,6}	{5,6}	
[E9] ERRORES DE [RE-]ENCAMINAMIENTO			
[E10] ERRORES DE SECUENCIA			

Continua

[LAN_SYT] RED LAN			
RIESGO ACUMULADO			
[E15] ALTERACIÓN DE LA INFORMACIÓN			
[E19] FUGAS DE INFORMACIÓN			
[E24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	{6,3}	{6,3}	
[A5] SUPLANTACIÓN DE LA IDENTIDAD			
[A6] ABUSO DE PRIVILEGIOS DE ACCESO			
[A7] USO NO PREVISTO	{5,1}	{5,1}	
[A9] [RE-]ECAMINAMIENTO DE MENSAJES			
[A10] ALTERACIÓN DE LA SECUENCIA			
[A11] ACCESO NO AUTORIZADO			
[A12] ANÁLISIS DE TRÁFICO			
[A14] INTERCEPTACIÓN DE INFORMACIÓN (ESCUCHA)			
[A15] MODIFICACIÓN DE LA INFORMACIÓN			
[A18] DESTRUCCIÓN DE LA INFORMACIÓN	{6,3}	{6,3}	
[A19] REVELACIÓN DE LA INFORMACIÓN			
[A24] DENEGACIÓN DEL SERVICIO	{7,2}	{7,2}	

Tabla 284

Riesgo de la Red Wan

[WAN_SYT] RED WAN			
RIESGO ACUMULADO			
[I8] FALLO DE SERVICIOS DE COMUNICACIONES	{6,3}	{6,3}	{6,3}
[E2] ERRORES DE ADMINISTRADOR DE SISTEMA/DE LA SEGURIDAD	{5,6}	{5,6}	{5,6}
[E9] ERRORES DE [RE-]ENCAMINAMIENTO			
[E10] ERRORES DE SECUENCIA			
[E15] ALTERACIÓN DE LA INFORMACIÓN			

Continua

[WAN_SYT] RED WAN			
RIESGO ACUMULADO			
[E19] FUGAS DE INFORMACIÓN			
[E24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	{6,3}	{6,3}	{6,3}
[A5] SUPLANTACIÓN DE LA IDENTIDAD			
[A6] ABUSO DE PRIVILEGIOS DE ACCESO			
[A7] USO NO PREVISTO	{5,1}	{5,1}	{5,1}
[A9] [RE-]ECAMINAMIENTO DE MENSAJES			
[A10] ALTERACIÓN DE LA SECUENCIA			
[A11] ACCESO NO AUTORIZADO			
[A12] ANÁLISIS DE TRÁFICO			
[A14] INTERCEPTACIÓN DE INFORMACIÓN (ESCUCHA)			
[A15] MODIFICACIÓN DE LA INFORMACIÓN			
[A18] DESTRUCCIÓN DE LA INFORMACIÓN	{6,3}	{6,3}	{6,3}
[A19] REVELACIÓN DE LA INFORMACIÓN			
[A24] DENEGACIÓN DEL SERVICIO	{7,2}	{7,2}	{7,2}

Tabla 285

Riesgo de los Sistemas de alimentación ininterrumpida

[UPS_SYT] SISTEMAS DE ALIMENTACIÓN ININTERRUMPIDA			
RIESGO ACUMULADO			
[N1] FUEGO	{5,9}	{5,9}	{5,9}
[N2] DAÑOS POR AGUA	{5,4}	{5,4}	{5,4}
[N*] DESASTRES NATURALES	{5,9}	{5,9}	{5,9}
[I1] FUEGO	{6,6}	{6,6}	{6,6}
[I2] DAÑOS POR AGUA	{6,0}	{6,0}	{6,0}
[I*] DESASTRES INDUSTRIALES	{6,6}	{6,6}	{6,6}

Continua

[UPS_SYT] SISTEMAS DE ALIMENTACIÓN ININTERRUMPIDA			
RIESGO ACUMULADO			
[I3] CONTAMINACIÓN MEDIOAMBIENTAL	{5,4}	{5,4}	{5,4}
[E23] ERRORES DE MANTENIMIENTO/ACTUALIZACIÓN DE PROGRAMAS (HARDWARE)	{5,1}	{5,1}	{5,1}
[A7] USO NO PREVISTO	{6,3}	{6,3}	{6,3}
[A23] MANIPULACIÓN DE HARDWARE	{6,3}	{6,3}	{6,3}
[A25] ROBO DE EQUIPOS	{4,8}	{4,8}	{4,8}
[A26] ATAQUE DESTRUCTIVO	{5,1}	{5,1}	{5,1}

Tabla 286

Riesgo del Circuito cerrado de televisión

[CCTV_SYT] CIRCUITO CERRADO DE TELEVISIÓN			
RIESGO ACUMULADO			
[N1] FUEGO	{5,9}	{5,9}	{5,9}
[N2] DAÑOS POR AGUA	{5,4}	{5,4}	{5,4}
[N*] DESASTRES NATURALES	{5,9}	{5,9}	{5,9}
[I1] FUEGO	{6,6}	{6,6}	{6,6}
[I2] DAÑOS POR AGUA	{6,0}	{6,0}	{6,0}
[I*] DESASTRES INDUSTRIALES	{6,6}	{6,6}	{6,6}
[I3] CONTAMINACIÓN MEDIOAMBIENTAL	{5,4}	{5,4}	{5,4}
[E23] ERRORES DE MANTENIMIENTO/ACTUALIZACIÓN DE PROGRAMAS (HARDWARE)	{5,1}	{5,1}	{5,1}
[A7] USO NO PREVISTO	{6,3}	{6,3}	{6,3}
[A23] MANIPULACIÓN DE HARDWARE	{6,3}	{6,3}	{6,3}
[A25] ROBO DE EQUIPOS	{4,8}	{4,8}	{4,8}
[A26] ATAQUE DESTRUCTIVO	{5,1}	{5,1}	{5,1}

Tabla 287

Riesgo del Sistema de rastreo

[RASTREO_SYT] SISTEMA DE RASTREO			
RIESGO ACUMULADO			
[N1] FUEGO	{5,9}	{5,9}	{5,9}
[N2] DAÑOS POR AGUA	{5,4}	{5,4}	{5,4}
[N*] DESASTRES NATURALES	{5,9}	{5,9}	{5,9}
[I1] FUEGO	{6,6}	{6,6}	{6,6}
[I2] DAÑOS POR AGUA	{6,0}	{6,0}	{6,0}
[I*] DESASTRES INDUSTRIALES	{6,6}	{6,6}	{6,6}
[I3] CONTAMINACIÓN MEDIOAMBIENTAL	[5,4}	[5,4}	[5,4}
[E23] ERRORES DE MANTENIMIENTO/ACTUALIZACIÓN DE PROGRAMAS (HARDWARE)	{5,1}	{5,1}	{5,1}
[A7] USO NO PREVISTO	{6,3}	{6,3}	{6,3}
[A23] MANIPULACIÓN DE HARDWARE	{6,3}	{6,3}	{6,3}
[A25] ROBO DE EQUIPOS	{4,8}	{4,8}	{4,8}
[A26] ATAQUE DESTRUCTIVO	{5,1}	{5,1}	{5,1}

Tabla 288

Riesgo de la Unidad de Sistemas de Redes y comunicaciones

[L_SYT] UNIDAD DE SISTEMA DE REDES Y COMUNICACIONES			
RIESGO ACUMULADO			
[N1] FUEGO	{6,8}	{6,8}	{6,8}
[N2] DAÑOS POR AGUA	{6,8}	{6,8}	{6,8}
[N*] DESASTRES NATURALES	{6,6}	{6,6}	{6,6}
[I1] FUEGO	{6,8}	{6,8}	{6,8}
[I2] DAÑOS POR AGUA	{6,8}	{6,8}	{6,8}

Continua

[L_SYT] UNIDAD DE SISTEMA DE REDES Y COMUNICACIONES			
RIESGO ACUMULADO			
[I*] DESASTRES INDUSTRIALES	{6,8}	{6,8}	{6,8}
[I3] CONTAMINACIÓN MEDIO AMBIENTAL	{5,1}	{5,1}	{5,1}
[I4] CONTAMINACIÓN ELECTROMAGNÉTICA	{4,2}	{4,2}	{4,2}
[I11] EMANACIONES ELECTROMAGNÉTICAS			
[A5] SUPLANTACIÓN DE LA IDENTIDAD			
[A6] ABUSO DE PRIVILEGIOS DE ACCESO	{5,1}	{5,1}	{5,1}
[A7] USO NO PREVISTO	{5,1}	{5,1}	{5,1}
[A11] ACCESO NO AUTORIZADO			
[A26] ATAQUE DESTRUCTIVO	{5,9}	{5,9}	{5,9}
[A27] OCUPACION ENEMIGA	{6,8}	{6,8}	{6,8}

Tabla 289

Riesgo del Responsable del área de sistemas

[GER_SYT] RESPONSABLE DEL ÁREA DE SISTEMAS
RIESGO ACUMULADO
[E19] FUGAS DE INFORMACIÓN
[A19] REVELACIÓN DE INFORMACIÓN
[A29] EXTORSIÓN
[A30] INGENIERÍA SOCIAL

6.3 IMPACTO RESIDUAL

Tabla 290

Impacto Residual de cada Activo

IMPACTO RESIDUAL

ACTIVOS	IMPACTO	PRESENTE	SOLUCIÓN
[INF_SYT] INFORMACIÓN LOGÍSTICA	[10]	[10]	[10]
[INT_SYT] INFORMACIÓN POR DEPARTAMENTO	[7]	[7]	[7]
[LOG] INFORMACIÓN DE REGISTROS DE INGRESOS SOBRE LOS SERVIDORES	[9]	[9]	[9]
[PER_SYT] INFORMACIÓN DE CADA USUARIO	[0]	[0]	[0]
[TC_SYT] TRASNPORTE DE MERCADERÍA REFRIGERADA	[9]	[9]	[9]
[AC_SYT] ALQUILER DE CONTENEDORES	[6]	[6]	[6]
[SMD_SYT] SERVICIO DE MONTAJE Y DESMONTAJE	[6]	[6]	[6]
[WEB_SYT] PORTAL WEB	[1]	[1]	[1]
[ZM_SYT] SERVIDOR DE CORREO ELECTRÓNICO	[10]	[10]	[10]
[IP_SYT] TELEFONÍA IP	[7]	[7]	[7]
[BACKUP_SYT] SERVICIO DE COPIAS DE RESPALDO	[3]	[3]	[3]
[OTR_SYT] OTROS SOFTWARE	[1]	[1]	[1]
[SBD_SYT] SERVIDOR DE DATOS			
[LAPTOP_SYT] COMPUTADORAS PORTÁTILES			
[SCAN_SYT] SCANNER	[0]	[0]	[0]
[PRINT1_SYT] IMPRESORAS MATRICIALES	[1]	[1]	[1]
[PRINT2_SYT] IMPRESORA LASER	[1]	[1]	[1]
[UPS_SYT] SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA	[4]	[4]	[4]
[CCTV_SYT] CIRCUITO CERRADO DE TELEVISIÓN	[4]	[4]	[4]
[RASTREO_SYT] SISTEMA DE RASTREO	[4]	[4]	[4]
[GER_SYT] RESPONSABLE DEL ÁREA DE SISTEMAS			

6.4 RIESGO RESIDUAL

Tabla 291

Riesgo Residual de cada Activo

RIESGO RESIDUAL

ACTIVOS	IMPACTO	PRESENTE	SOLUCIÓN
[INF_SYT] INFORMACIÓN LOGÍSTICA	{7,2}	{7,2}	{7,2}
[INT_SYT] INFORMACIÓN POR DEPARTAMENTO	{5,4}	{5,4}	{5,4}
[LOG] INFORMACIÓN DE REGISTROS DE INGRESOS SOBRE LOS SERVIDORES	{6,6}	{6,6}	{6,6}
[PER_SYT] INFORMACIÓN DE CADA USUARIO	{2,1}	{2,1}	{2,1}
[TC_SYT] TRASNPORTE DE MERCADERÍA REFRIGERADA	{6,6}	{6,6}	{6,6}
[AC_SYT] ALQUILER DE CONTENEDORES	{4,8}	{4,8}	{4,8}
[SMD_SYT] SERVICIO DE MONTAJE Y DESMONTAJE	{4,8}	{4,8}	{4,8}
[WEB_SYT] PORTAL WEB	{1,9}	{1,9}	{1,9}
[ZM_SYT] SERVIDOR DE CORREO ELECTR ZIMBRA	{7,2}	{7,2}	{7,2}
[IP_SYT] TELEFONÍA IP	{5,4}	{5,4}	{5,4}
[BACKUP_SYT] SERVICIO DE COPIAS DE RESPALDO	{3,9}	{3,9}	{3,9}
[AV_SYT] ANTIVIRUS			
[OTR_SYT] OTROS SOFTWARE	{1,9}	{1,9}	{1,9}
[SBD_SYT] SERVIDOR DE DATOS			
[SCAN_SYT] SCANNER	{1,3}	{1,3}	{1,3}
[PRINT1_SYT] IMPRESORAS MATRICIALES	{1,9}	{1,9}	{1,9}
[PRINT2_SYT] IMPRESORA LASER	{1,9}	{1,9}	{1,9}
[UPS_SYT] SISTEMA DE ALIMENTACIÓN ININTER	{3,3}	{3,3}	{3,3}
[CCTV_SYT] CIRCUITO CERRADO DE TELEVISIÓN	{3,3}	{3,3}	{3,3}
[RASTREO_SYT] SISTEMA DE RASTREO	{3,3}	{3,3}	{3,3}
[GER_SYT] RESPONSABLE DEL ÁREA DE SISTEMAS			

BIBLIOGRAFÍA

[1] El Portal de ISO 27000, E. P. (s.f.). *GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN*. Obtenido de http://www.iso27000.es/sgsi.html

[2] BASC. (22 de 03 de 2011). *BUSINESS ALLIANCE FOR SECURE COMMERCE*. Obtenido de http://www.wbasco.org/

[3] EAR PILAR. (14 de 02 de 2014). *ANÁLISIS Y GESTIÓN DE RIESGOS*. Obtenido de http://www.pilar-tools.com/es/tools/pilar/

[4] EUMED. (05 de 2008). *LA GESTIÓN DE LA CALIDAD EN LOS SERVICIOS*. Obtenido de http://www.eumed.net/rev/cccss/0712/vrm.htm

[5] Fernández, C. M. (1988). *Seguridad en Sistemas Informáticos.* España: Ediciones Diaz de Santos S.A. Obtenido de cienciakarla.bligoo.com.mx/tag/tecnologia

[6] Guagalango Ricardo, M. P. (2011). Evualuación técnica de la seguridad de la informática del Data Center de la Escuela Politécnica del Ejército. Sangolquí, Pichincha, Ecuador.

[7] INTECO. (23 de 08 de 2013). *CURSO DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN*. Obtenido de http://es.slideshare.net/nyzapersa/curso-seguridad-en-sistemas-de-informacion

[8] López, F., & Amuto, M. (2006). Metodología de Análisis de Gestión de Riesgos de los Sistemas de Información.

[9] Martin, P. (2007). *Sociedad de la Información, Telecomunicaciones e Internet, Nuevas Tecnologías, Seguridad de la Información.*

[10] PILAR, E. (10 de 10 de 2012). *MAGERIT VERSION 3 ENTORNO DE ANÁLISIS DE RIESGO*. Obtenido de https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/

GLOSARIO

- **MAGERIT**

  Es una metodología para Análisis de Riesgo que permite ofrecer unos métodos sistemáticos que permite descubrir medidas oportunas para mantener los riesgos bajo control.

- **PILAR**

  Siglas de Procedimientos Informático Lógico para el Análisis de Riesgos.

- **INTEGRIDAD DE LA INFORMACIÓN**

  Es el valor del contenido de la información con el tiempo y generalmente se relaciona al trabajo del autor.

- **INFORMACIÓN**

  Conjunto organizado de datos procesados que constituyen un mensaje sobre un determinado fenómeno.

- **POLÍTICA**

  Actividad orientada, que define normas y procedimientos para alcanzar ciertos objetivos.

- **SEGURIDAD DE LA INFORMACIÓN**

  Preservación de la confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento dentro de una organización

- **NORMAS ISO 27000**

  La serie de la familia ISO 27000 es una Familia de Estándares internacionales para Sistemas de Gestión de Seguridad de la Información.

CURRICULUM VITAE

Nombres y Apellidos:

ERIKA PATRICIA MONCAYO SALAS

Lugar y Fecha de Nacimiento:

Guayaquil, 23 de diciembre de 1977

Educación Primaria:

Colegio de América

Educación Secundaria

Colegio de América

Educación Superior

Universidad de las Fuerzas Armadas ESPE-Sangolquí

Ingeniería en Sistemas e Informática

Títulos Obtenidos

Suficiencia en el Idioma Inglés

HOJA DE LEGALIZACIÓN DE FIRMAS

ELABORADO POR

MONCAYO SALAS ERIKA PATRICIA

_____

Sra. Erika Patricia Moncayo Salas

DIRECTOR DE LA CARRERA DE INGENIERÍA DE

SISTEMAS E INFORMÁTICA

_____

Sr. Ing. Mauricio Campaña

Sangolquí, Septiembre del 2014