ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría en Seguridad Informática Aplicada

"IMPLEMENTACIÓN DE UN ESQUEMA DE SEGURIDAD DE INFORMÁTICA APLICADO A LOS ACTIVOS DE LA FIEC, BASADO EN EL ESTÁNDAR ISO 27002"

TESIS DE GRADO

Previo a la obtención del título de

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

MARGARITA DEL ROCÍO FILIÁN GÓMEZ

GUAYAQUIL

2015

AGRADECIMIENTO

Agradezco a Dios, mi familia, profesores y amigos que me proporcionaron las fuerzas, guías, ayuda, conocimiento, aliento y apoyo para culminar este proyecto y seguir adelante.

DEDICATORIA

A mi familia y amigos.

TRIBUNAL DE GRADUACIÓN

_____

MG. LENIN FREIRE C.

DIRECTOR DE LA MSIA

DIRECTOR DE TESIS

_____

MG. ALBERT ESPINAL S.

MIEMBRO PRINCIPAL

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesis, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral".

_____

MARGARITA DEL ROCÍO FILIÁN GÓMEZ

RESUMEN

La presente tesis consiste en la implementación de un esquema de seguridad de informática para los activos de la FIEC, basado en el estándar ISO 27002, donde se identificarán las posibles amenazas y el riesgo al que los activos que administra el Departamento de Soporte Técnico (DST) están expuestos.

Este documento se divide en cuatro capítulos que se estructuran de la siguiente forma:

En el Capítulo I, se describe un antecedente del DST, la problemática que existe, se define el objetivo general, los objetivos específicos y se plantea una solución para poder implementar el esquema de seguridad. Además, se especifica el alcance de la tesis y se indica la metodología para llevar a cabo el presente proyecto.

En el Capítulo II, se abordan las definiciones de Seguridad Informática, estándares y normas de seguridad, metodología de análisis de riesgo, que serán usadas a lo largo del desarrollo de este documento, además se

presentan estadística actual de las seguridades de las instituciones en general.

En el Capítulo III, se presenta el análisis del DST en el cual se detalla la situación actual del mismo; se inicia con la identificación de activos que administra, para después realizar el análisis de riesgos de los activos basados en la metodología MAGERIT, donde se identifican amenazas y salvaguardas para los activos. Posteriormente se detalla el tratamiento del riesgo basado en el análisis que se realizó.

En el Capítulo IV, se seleccionan los controles basados en la Norma ISO 27002 para minimizar el riesgo de los activos que fueron analizados en el capítulo III, además se define la política de seguridad y procedimientos que posteriormente serán difundidos mediante una estrategia de seguridad.

Finalmente, se presentan las conclusiones y recomendaciones basadas en el desarrollo del presente documento.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

[C]: Confidencialidad

[D]: Disponibilidad

[Deg]: Degradación

[F]: Frecuencia

[I]: Integridad

[Imp]: Impacto

[pob]: Probabilidad

[rie]: Riesgo

[val]: Valor

CLUSIF: Asociación de empresas aseguradoras francesas

CTA: Central Computer and Telecommunications Agency

DST: Departamento de Soporte Técnico

FIEC: Facultad de Ingeniería en Electricidad y Computación

GTySI - Gerencia de Tecnología y Sistemas de Información

IEC: Comisión Electrotécnica Internacional

ISECOM: Institute for security and open methodologies

ISO: Organización Internacional de Normalización

MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

PWC: PricewaterhouseCoopers

RAE: Real Academia Española

SEI: Software Engineering Institute

ÍNDICE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

Este documento contiene información referente al estado actual del Departamento de Soporte Técnico de la FIEC, además de los activos que administra con el fin de analizar y determinar las amenazas que existen para minimizar los posibles riesgos, implementando un esquema de seguridad que se adapte a las necesidades del DST, aplicando los controles ofrecidos por el estándar ISO 27002:2013.

Actualmente, todas las instituciones tanto privadas como públicas tienen la necesidad de verificar periódicamente la seguridad de sus activos tales como datos, sistemas, hardware, etc., y así mismo asegurarlos, puesto que existen personas/organizaciones que monitorean, buscando encontrar alguna vulnerabilidad en estos activos con el objetivo de robarlos o modificarlos, en ciertos casos para hacer daño a la institución atacada.

Por lo tanto, el activo más importante para todas las instituciones es la información y es por esa razón que existen normas o estándares internacionales que nos sirven como una guía en la que se describen controles en cuanto a seguridad de la información se refiere.

Esta tesis busca aportar un esquema que ayude al manejo de la seguridad de los sistemas de información que administra el DST, conociendo que la mayoría de tareas y procedimientos hacen uso de la red de datos. El esquema formado por políticas y procedimientos de seguridad servirá para formalizar que se debe o no hacer y asignar responsables, garantizando así la integridad, confidencialidad y disponibilidad de los activos más importantes para el DST.

CAPÍTULO 1

GENERALIDADES

1.1 Antecedentes

La FIEC desde el año 1997 ha contado con el Laboratorio de Computación (Lab-Fiec) como parte fundamental en el soporte y desarrollo en el área de computación, asumiendo con responsabilidad el de colaborar con el crecimiento de la infraestructura tecnológica de la facultad.

El progresivo desarrollo del área tecnológica, comunicaciones y construcción de edificios hizo que desde el año 2001, se incorpore personal de planta para atender de mejor manera los requerimientos informáticos de la Facultad y desde el año 2003 se creó la “Sala de Asistentes”

En el año 2012 el Decanato, propuso crear el Departamento de Soporte Técnico (DST-FIEC) con el fin de mejorar administrativamente la “Sala de Asistentes”, teniendo adscrito al Laboratorio de Computación, LAB-FIEC.

El DST, sabe que la seguridad es un factor importante en el desarrollo de las tareas y responsabilidades diarias en lo que corresponde a la administración de los activos tecnológicos de la FIEC, además conoce que es importante prevenir, resguardar y mantener el correcto funcionamiento de activos pero actualmente lo hace de una manera informal dado que no existen formalmente documentos que le indiquen o sirvan de guía para proteger los bienes y servicios informáticos que administra.

Y es por eso que mediante este proyecto de tesis se implementarán políticas y procedimientos que ayuden en la administración de los activos de la FIEC como un esquema de seguridad de informática y en donde se informe a los usuarios lo que tienen que conocer para no caer fácilmente en ataques externos.

1.2 Descripción del problema

Actualmente la FIEC no cuenta con un esquema de seguridad informática que incluya una política de seguridad y procedimientos que establezcan controles de seguridad en cuanto a accesos y uso de los recursos informáticos. La Facultad ha crecido con el paso de los años, en laboratorios, equipos, personal, estudiantes e información, lo que implica que existe mayor riesgo en la seguridad de los activos de la información.

Con el tiempo, se han presentado algunos incidentes de seguridad, como por ejemplo hurtos de computadoras portátiles, daños de computadoras, ingresos no autorizados, entre otros incidentes. Donde se hace necesario tener y mantener controles a nivel de seguridad para garantizar la disponibilidad, confidencialidad e integridad de los activos de información.

El no mantener una política de seguridad, aumenta el riesgo de que ocurran pérdidas de información o de recursos informáticos, incidentes de seguridad, que afecten la disponibilidad de los sistemas y servicios con los que cuenta la Facultad, lo que implica directamente en pérdidas económicas por falta de control de los activos tecnológicos o tiempo del personal docente por clases afectadas, interrupción de procesos

administrativos, lo cual genera desconfianza sobre la imagen de la Facultad.

1.3 Solución propuesta

Elaborar, implantar y difundir un esquema en el cual se defina una política de seguridad informática soportada en procedimientos que ayuden a garantizar la seguridad de la información, recursos informáticos y personas que interactúan diariamente, haciendo uso de los servicios e infraestructura tecnológica que ofrece la Facultad, basados en el estándar ISO 27002, aplicando los controles necesarios de los dominios de Aspectos organizativos de la seguridad de la información, Gestión de activos, Control de Accesos, Seguridad Física y Ambiental y Seguridad en la operativas.

Esta norma proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos quienes estén interesados y sean responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información; preservando la confidencialidad, integridad y disponibilidad de la información. Es decir, que es un código de buenas prácticas (un documento de asesoramiento genérico) y no es una especificación formal, como la norma ISO / IEC

27001, lo que hace que se adapte a la necesidades o requerimientos de una organización.

Al hacer uso de esta norma se evaluarán las vulnerabilidades de los activos, a través de una identificación, análisis y tratamiento de riesgos, por el cual se definirá y aplicarán controles u otras formas para el tratamiento de los mismos.

Servirá como guía para la implementación de los controles de seguridad y de las prácticas más eficaces para gestionar la seguridad de la información. El estándar es lo suficientemente bueno para dar inicio a una cultura de seguridad en la FIEC.

1.4 Objetivo general

Implementar un esquema de seguridad Informática para la Facultad de Ingeniería en Electricidad y Computación - FIEC; con el propósito de mitigar los riesgos relacionados con el uso de los activos informáticos.

1.5 Objetivos específicos

- ✓ Analizar la situación actual del Departamento de Soporte Técnico–DST, encargado de administrar la infraestructura tecnológica de la FIEC.

- ✓ Identificar los activos de información que administra el DST y las posibles amenazas que puedan existir.

- ✓ Diseñar un esquema de seguridad, en base a los controles de la norma ISO 27002, tomando en cuenta la seguridad física y lógica de los activos de la FIEC, con el fin de definir políticas y procedimientos necesarios para asegurar el uso correcto de los recursos informáticos y sistemas de información por parte del personal administrativo, docentes y estudiantes de la FIEC.

- ✓ Implementar y difundir la política y procedimientos basados en el estándar ISO 27002.

1.6 Alcance

El alcance de esta tesis es ayudar a alinear la administración de infraestructura tecnológica en base a la misión del DST, considerando la seguridad informática, definiendo políticas y procedimientos en base a los dominios de la norma ISO 27002 que ayude a aplicar buenas prácticas y

permita reducir el riesgo. Los dominios que se comprenden son: Aspectos organizativos de la seguridad de la información, Gestión de activos, Control de Accesos, Seguridad Física y Ambiental y Seguridad en la operativa.

1.7 Metodología

La metodología para realizar el presente trabajo está compuesta por 3 fases, las cuales se pueden apreciar en la figura 1.1 y que se detalla en la Tabla 1.

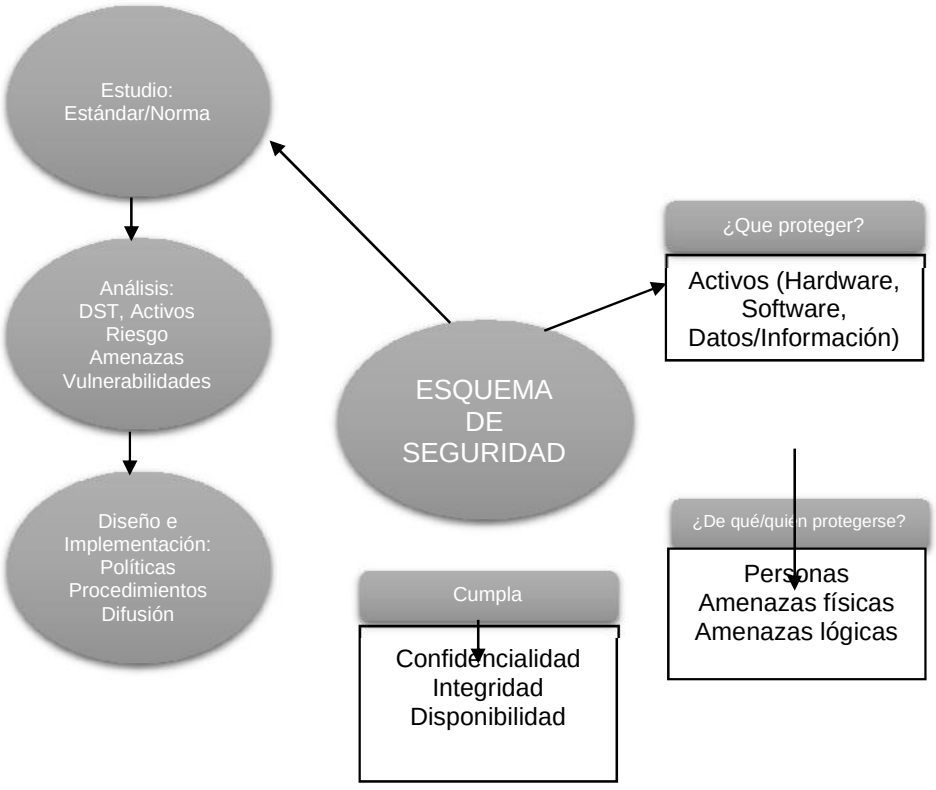

Figura 1.1 - Metodología de trabajo. Fuente: El autor.

Tabla 1 – Detalle de las fases de la metodología aplicada. Fuente: El autor

Fase	**Detalle**
Estudio del Estándar/Norma	Estudio de la norma ISO 27002:2013 y definir los dominios que se implementarán.
Análisis: DST, Activos Riesgo Amenazas Vulnerabilidades	Situación actual del DST, activos que maneja. Amenazas que podrían estar expuestos los activos, vulnerabilidades y riesgo basado en la valoración de las amenazas y los activos.
Diseño e Implementación: Políticas Procedimientos Difusión	Selección de controles que ayuden a reducir el riesgo, definición de políticas y procedimientos para asegurar los activos. Difusión de las políticas.

CAPÍTULO 2

MARCO TEÓRICO

2.1 Seguridad Informática

Partiendo de la definición de *seguro* en la que la RAE se refiere a “Libre y exento de todo peligro, daño o riesgo.” [1] y que *informática* es definida como el “conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores.” [2]; se puede decir que la seguridad informática se encarga de diseñar procedimientos, normas técnicas y métodos que nos ayuden a tener un sistema informático seguro y libre de riesgo o como “el trato de la prevención y la detección de acciones no autorizadas por los usuarios de un sistema informático” o “medidas que podemos tomar para hacer frente a las acciones intencionales de las partes que se comportan de una manera no deseada” [3].

Estas definiciones tienen algo en común y es que todas buscan asegurar un sistema informático, y no cabe duda que hoy en día las empresas / organizaciones dependen de la información y tecnología que están soportadas por sistemas informáticos, muy diferente a la realidad de hace algunos años atrás; por lo que las instituciones/organizaciones tienen la necesidad de proteger a sus activos críticos, de las amenazas internas o externas a los cuales pueden estar expuestos y uno de esos activos valiosos a considerar es la *información* con que cuentan, por lo tanto la deben proteger de posibles pérdidas, mal uso, etc. Por tal motivo, la seguridad informática ha ganado popularidad en los últimos años y ha pasado de ser considerada un gasto, a ser vista como una inversión por parte de los directivos de las empresas y organizaciones a nivel mundial [4].

2.1.1 Propiedades de la Seguridad Informática

Un sistema se considera seguro si cumple con las propiedades de integridad, confidencialidad y disponibilidad.

En donde ***la confidencialidad*** avala que la información puede ser consultada o accedida solamente por quien está debidamente autorizado, ***la integridad*** certifica que la misma no ha sido

modificada sin autorización y ***la disponibilidad*** garantiza que siempre esté disponible cuando se requiera. Si uno de estos ítems falla, entonces la información no está segura. [5]

2.2 Estándares y normas aplicables a la seguridad informática

Las normas son conocidas en el área de seguridad informática como un conjunto de lineamientos, recomendaciones, reglas y controles con el propósito de respaldar las políticas de seguridad y los objetivos que se definen en base a esta, y se cumplen a través de funciones, delegación de responsabilidades entre otras, con el fin de que se adapte a las necesidades de seguridad establecidas para el entorno de una organización.

Las organizaciones que hacen uso de tecnologías de la información, es recomendable que implementen el uso de buenas prácticas de seguridad informática con el fin de evitar que se generen vulnerabilidades que aumenten la posibilidad de riesgo en sus sistemas de información. Esta es la razón por la cual se han creado las normas y estándares internacionales con alto nivel para la administración de la seguridad informática, independientemente de su tamaño o actividad.

Las series del estándar ISO 27000 fue publicada en mayo de 2009. Contiene la descripción general que es empleada en toda la serie 27000. Se puede utilizar, entender la serie y la relación entre los diferentes documentos que la conforman. Esta serie ha sido reservada específicamente por la ISO (Organización Internacional de Normalización) que se refiere a seguridad de la información. Por supuesto, se alinea con una serie de otros temas, como lo son las normas ISO 9000 (gestión de calidad) e ISO 14000 (gestión medioambiental).

La serie 27000 serán alimentadas con un conjunto de normas y documentos individuales, algunos de ellos ya son bien conocidos, y de hecho, se han publicado. Otros están programados para su publicación. [6]

En la Tabla 2 se refleja las principales normas de funcionamiento de la serie:

Tabla 2 – Serie del estándar 27000 Fuente: ISO 27000.

ISO 27001 • Esta es la especificación de un sistema de gestión de seguridad de la información (SGSI) que sustituyó a la antigua norma BS7799. • Es la norma principal de requisitos de un SGSI. • La norma ISO 27001 se publicó en octubre	*ISO 27002* • Este es el número estándar de las serie 27000, lo que originalmente era la norma ISO 17799 (que en sí era conocido antes como BS7799-1). • La norma ISO 27002 fue publicada originalmente como un cambio de nombre de la norma ISO 17799 vigente, un código

de 2005, esencialmente, reemplazando la antigua norma BS7799-2. • Es la especificación para un SGSI, un Sistema de Gestión de Seguridad de la Información. • Sí BS7799 era una norma de larga data, publicado por primera vez en los años noventa como un código de prácticas. Como este maduró, una segunda parte surgió para cubrir los sistemas de gestión. • Los SGSIs deberán ser certificados por auditores externos a las organizaciones. • En su Anexo A, contempla una lista con los objetivos de control y controles que desarrolla la ISO 27002. • Hoy en día más de mil certificados están entregados en todo el mundo.	de prácticas para la seguridad de la información. • Básicamente describe cientos de potenciales controles y mecanismos de control, que pueden ser implementadas, en teoría, con sujeción a la orientación proporcionada en la norma ISO 27001. • Cuenta con 14 dominios, 35 objetivos de control y 114 controles.
ISO 27003 • Este es el número oficial de una nueva norma que pretende ofrecer una guía para la implementación de un SGSI (Sistema de Gestión de Seguridad Informática). • El propósito del desarrollo de este proyecto es proporcionar ayuda y orientación en la implementación de un SGSI (Sistema de Gestión de Seguridad de la Información). • Esto incluirá el enfoque del método PDCA, en relación con el establecimiento, implementación de revisión y la mejora del propio SGSI.	*ISO 27004* • Esta norma cubre la medición de información del sistema de seguridad y gestión de métricas, incluyendo controles alineado sugeridos de la ISO27002. • Publicada en diciembre de 2009. • Especifica las métricas y las técnicas de medida aplicables para determinar la eficiencia y eficacia de la implantación de un SGSI y de los controles relacionados
ISO 27005 • Este es una metodología independiente del estándar ISO para la gestión de riesgos de seguridad de información. • La norma proporciona directrices para la gestión de riesgos de seguridad de la información (GRSI) en una organización, apoyando específicamente los requisitos de un sistema de gestión de seguridad de la información que se define en la norma ISO 27001.	*ISO 27006* • Esta norma proporciona directrices para la acreditación de organizaciones que ofrecen la certificación del SGSI. • Una vez más, fue supervisado por el comité de ISO SC 27. • La norma anterior en relación con ésta era la EA 7/03. • Esta eficacia ha sido reemplazada por la nueva norma, para satisfacer las demandas del mercado para un mejor soporte de la ISO 27001. • En él se documenta de manera efectiva los requisitos adicionales a los especificados en la norma ISO 17021, que identifican los requisitos más genéricos.

2.2.1 ISO 27002:2013

Para la elaboración del documento de tesis se ha usado el estándar ISO 27002:2013, el cual tiene los lineamientos establecidos y los principios generales para iniciar, implementar, mantener y mejorar la gestión de seguridad de la información dentro de una organización estándar. Estos controles que conforman la norma están destinados a atender las necesidades identificadas a través de una evaluación de riesgos.

Además, la norma tiene por objeto proporcionar una guía para el desarrollo de normas de seguridad de la organización y las prácticas eficaces de gestión de la seguridad para ayudar a construir confianza en las actividades interinstitucionales.

La base de la norma fue originalmente un documento publicado por el gobierno del Reino Unido, que se convirtió en un estándar "adecuado" en 1995, cuando fue re-publicado por BSI como BS7799. En el 2000 fue publicado de nuevo, esta vez por la ISO, como ISO 17799. Una nueva versión de este apareció en 2005, junto con una nueva publicación, la norma ISO 27001. Estos dos

documentos están destinados a ser utilizados en conjunto, uno complementando el otro. [7]

En el 2013 se publicó la versión ISO 27002:2013, la cual contiene 114 controles, en comparación con los 133 documentados dentro de la versión 2005 y éstos se presentan en 14 secciones, en lugar de los 11 iniciales.

Es importante destacar que la ISO 27002 es independiente de la tecnología y se centra en los aspectos de gestión de seguridad de la información, la definición de los controles en un sentido genérico para que sean aplicables a través de diferentes aplicaciones, plataformas y tecnologías.

2.2.2 Contenido de la ISO 27002:2013

Las secciones de contenido son las siguientes:

- ✓ Política de seguridad
- ✓ Organización de la Seguridad de la Información

- ✓ Recursos de Seguridad Humana
- ✓ Gestión de activos
- ✓ Control de acceso
- ✓ Criptografía
- ✓ Física y Seguridad Ambiental
- ✓ Seguridad de Operaciones
- ✓ Seguridad Comunicaciones
- ✓ Sistemas de Información de adquisición, desarrollo, mantenimiento
- ✓ Relaciones con Proveedores
- ✓ Gestión de la información a Incidentes de Seguridad
- ✓ Aspectos Seguridad de la Información de la Continuidad del Negocio
- ✓ Conformidad

Dentro de cada sección se especifican los objetivos de los controles para la seguridad de la información y en cada uno de estos

controles tiene una guía de implementación. Cabe recalcar que cada organización considerará la selección de controles de acuerdo a las necesidades que tenga.

En el ANEXO A, se detallan los 14 dominios, 35 objetivos de control y 114 controles de la ISO 27002:2013.

2.3 Metodología de análisis y gestión de riesgo

Se conoce que el análisis y la gestión de riesgos conforman un método formal para determinar los riesgos de un sistema de información y en base a los resultados se recomiendan las medidas apropiadas que deberían ayudar para controlar estos riesgos.

El análisis de riesgo se enfoca en investigar los factores que contribuyen a que se presenten riesgos, es decir, implica que hay que evaluar el impacto que una violación de seguridad tendría sobre una organización, así como determinar las vulnerabilidades frente a las amenazas. Por lo tanto, el análisis de riesgo estima la magnitud de los riesgos a que está expuesta una organización.

En cambio la gestión de riesgos es un proceso que utiliza los resultados del análisis de riesgo para seleccionar medidas de seguridad adecuadas para controlar los riesgos identificados.

Las metodologías principales para el análisis y gestión de riesgo de los sistemas de información se detallan a continuación: [8]

- ✓ MAGERIT: es una metodología pública española creada en 1996 por el Ministerio de las Administraciones Públicas en colaboración con la empresa de tecnologías de la información Atos Origin y actualizada en su versión 3 en octubre del 2012.
- ✓ MARION: metodología francesa creada en 1985, se actualiza por CLUSIF (Asociación de empresas aseguradoras francesas)
- ✓ MELISA: es una metodología procedente del entorno militar francés, creada en 1984.
- ✓ CRAMM: del CTA (Central Computer and Telecommunications Agency) fue iniciada en 1985 y se usa en la administración pública británica.

- ✓ OCTAVE: del SEI (Software Engineering Institute) que vista desde el punto organizativo y técnico analiza los riesgos y propone un plan de mitigación.
- ✓ OSSTMM (Manual de Metodología Abierta de Testeo de Seguridad): del ISECOM (Institute for security and open methodologies) propone evaluar la seguridad en redes con testeos de intrusión, a través de Hacking Ético.

De esta lista de metodologías, el presente proyecto hace uso de MAGERIT, escogida porque ayuda a realizar un análisis de riesgo de los sistemas de información de forma organizada debido a que sus procesos están bien definidos, ofreciendo un método sistematizado que nos ayuda a planificar e identificar las medidas necesarias para reducir los riesgos. [9] Además, es fácil estimar el riesgo con esta metodología, usando la técnica de análisis mediante tablas.

2.3.1 Componentes y dimensiones de Seguridad para el análisis de riesgo.

Para realizar el análisis de riesgo de un sistema de información es importante conocer los elementos o componentes fundamentales

de seguridad, pues permitirá poder hacer un uso correcto de la metodología y así distinguir a los activos, las amenazas y las salvaguardias, los cuales la metodología las define como:

Activos: Son los componentes o funcionalidades de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. [10]

Amenazas: Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. [11]

Salvaguardias: Procedimientos o mecanismos tecnológicos que reducen el riesgo. [12]

Y en lo que refiere a las dimensiones de seguridad, la metodología define a las siguientes: [13]

Disponibilidad: o disposición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una

interrupción del servicio. La disponibilidad afecta directamente a la productividad de las organizaciones.

Integridad: o mantenimiento de las características de completitud y corrección de los datos. Contra la inseguridad, la información puede aparecer manipulada, corrupta o incompleta. La integridad afecta directamente al correcto desempeño de las funciones de una Organización.

Confidencialidad: o que la información llegue solamente a las personas autorizadas. Contra la confidencialidad o secreto pueden darse fugas y filtraciones de información, así como accesos no autorizados. La confidencialidad es una propiedad de difícil recuperación, pudiendo minar la confianza de los demás en la organización que no es diligente en el mantenimiento del secreto, y pudiendo suponer el incumplimiento de leyes y compromisos contractuales relativos a la custodia de los datos.

2.3.2 Magerit

La Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas – MAGERIT, presenta una guía de cómo se elabora el análisis de riesgos paso a

paso. A continuación se detallan los pasos que sigue esta metodología para determinar el riesgo: [14]

1. Determinar los activos que son relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio supondría su degradación.

2. Determinar a qué amenazas están expuestos los activos.

3. Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.

4. Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.

5. Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

La figura 2.1 muestra el recorrido de los elementos en el análisis de los riesgos potenciales, cuyos pasos se detallan en el siguiente subcapítulo:

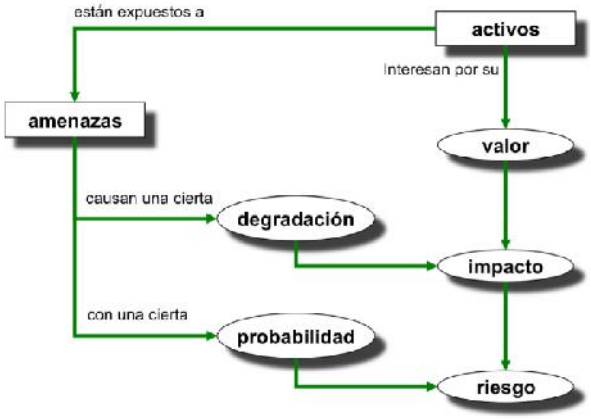

Figura 2.1 - Elementos del análisis de riesgos potenciales. Fuente: Magerit.

2.3.3 Pasos para el desarrollo de Magerit

Paso 1: Activos

En esta paso se identifican los activos más relevantes de la organización que constituye el objeto de estudio. En un sistema de información hay 2 tipos esenciales que manejan y son la información y los servicios que presta, adicionalmente la metodología identifica otros activos relevantes:

- ✓ Los *datos*: materializan la información
- ✓ *Servicios* auxiliares: se necesitan para poder organizar el sistema.

- ✓ Las *aplicaciones informáticas* (software): permiten manejar los datos.
- ✓ Los *equipos informáticos* (hardware): permiten hospedar datos, aplicaciones y servicios.
- ✓ Los *soportes de información*: son dispositivos de almacenamiento de datos.
- ✓ El *equipamiento auxiliar*: complementa el material informático.
- ✓ Las *redes de comunicaciones*: permiten intercambiar datos.
- ✓ Las *instalaciones*: acogen equipos informáticos y de comunicaciones.
- ✓ Las *personas*: explotan u operan todos los elementos anteriormente citados.

Ver ANEXO B, donde se detallan los tipos de activos que define MAGERIT.

Dependencias

Los activos esenciales dependen de otros como pueden ser los equipos, las comunicaciones, las instalaciones y las frecuentemente

olvidadas personas que trabajan con aquellos. Estas dependencias se establecen en modo jerárquico, evaluando la vinculación que existe entre activos y en base a las dimensiones de seguridad.

Valoración

Se puede establecer como la necesidad de proteger, por tanto, cuanto más valioso es un activo, mayor es el nivel de protección que se requiere en la dimensión o dimensiones de seguridad. El valor del activo puede ser propio, o puede ser acumulado, en donde los activos inferiores en un esquema de dependencias acumulan el valor de los activos que se soportan en ellos. Entonces el valor de un activo es la estimación del costo que causaría la materialización de una amenaza sobre dicho activo.

Paso 2: Amenazas

En este paso se determinan las amenazas que pueden afectar a cada activo. Las amenazas son consideradas como “cosas que ocurren”, y en caso de ocurrir, es de interés por lo que le pueda pasar a nuestros activos.

Identificación de las amenazas

Esta metodología presenta una relación de amenazas típicas como: [15]

- ✓ *De origen natural:* corresponde a accidentes naturales (terremotos, inundaciones, etc).
- ✓ Del entorno (de origen industrial): corresponde a desastres industriales (contaminación, fallos eléctricos, etc) ante los cuales el sistema de información es víctima pasiva.
- ✓ *Defectos de las aplicaciones:* corresponde a problemas que nacen directamente en el equipamiento propio por defectos en su diseño o en su implementación, con consecuencias potencialmente negativas sobre el sistema. Se denominan vulnerabilidades técnicas.
- ✓ *Causadas por las personas de forma accidental:* corresponde a las causadas por personas con acceso al sistema de información y que pueden ser causa de problemas no intencionados, típicamente por error o por omisión.
- ✓ *Causadas por las personas de forma deliberada:* corresponde a las causadas por las personas con acceso al sistema de información y pueden ser causa de problemas intencionados:

ataques deliberados; bien con ánimo de beneficiarse indebidamente o con el ánimo de causar daño.

Ver el catálogo de amenazas de la metodología MAGERIT en el ANEXO C.

Valoración

Una vez que las amenazas de los activos han sido identificadas, se debe proceder a valorar las amenazas, mediante los siguientes dos parámetros:

- ✓ ***Degradación:*** cuán perjudicado resultaría el valor de un activo, es decir, que mide el daño causado por un incidente en el caso supuesto de que ocurriera.
- ✓ ***Probabilidad/Frecuencia:*** cuán probable o improbable es que se materialice la amenaza. Es más compleja de determinar y de expresar y a veces se modela cualitativamente por medio de alguna escala nominal. A veces se modela numéricamente como una frecuencia de ocurrencia.

Impacto y Riesgo

- ✓ El impacto son las consecuencias del daño que causa la materialización de una amenaza sobre el activo.
- ✓ El riesgo es un indicador de lo que posiblemente suceda por causa de las amenazas.
- ✓ El impacto y el riesgo se tratan de mitigar definiendo salvaguardas.

Paso 3: Salvaguardas

En este paso se seleccionarán salvaguardas que en los pasos anteriores no se han tomado en cuenta. Estas se seleccionan de acuerdo al impacto y riesgo a que estarían expuestos los activos si no se protegieran y que ayudan a reducir el riesgo.

Selección de salvaguardas

Existe un listado de salvaguardias que la metodología nos a conocer y se debe saber cuál va a ser la más efectiva en contra de

las amenazas. Para lo cual se debe considerar los siguientes aspectos: [16]

- ✓ Tipo de activos a proteger, pues cada tipo se protege de una forma específica.
- ✓ Dimensión o dimensiones de seguridad que requieren protección.
- ✓ Amenazas de las que necesitamos protegernos.
- ✓ Si existen salvaguardas alternativas.

Además es importante establecer un principio de proporcionalidad y tener en consideración: [17]

- ✓ el mayor o menor valor propio o acumulado sobre un activo, centrándonos en lo más valioso y obviando lo irrelevante.
- ✓ la mayor o menor probabilidad de que una amenaza ocurra, centrándonos en los riesgos más importantes.
- ✓ la cobertura del riesgo que proporcionan salvaguardas alternativas.

A todo esto se puede decir que las salvaguardas limitan el factor de degradación de valor. Para ver el catálogo de salvaguardas de la metodología MAGERIT. Ver ANEXO D de salvaguardas.

2.4 Estadística actual

La compañía Black Hat, dedicados 17 años a proporcionar lo último en investigación en cuanto a seguridad de la información y desarrollo de tecnologías de información, efectuó una encuesta en Julio 2015 a 460 profesionales de seguridad de empresas con más de 1000 empleados.

En este estudió se determinó que lo que más consume el presupuesto del departamento de seguridad de tecnologías de información, son las fugas de información de los usuarios finales que no siguen la política de seguridad, además que el mayor riesgo a futuro y a lo que el departamento de seguridad de tecnologías de información debe prestar atención es al internet de las cosas y el BYOD, todo esto controlable bajo una buena política de seguridad. [18]

De acuerdo a un estudio efectuado por Kaspersky Lab, en su encuesta anual a los riesgos de la seguridad tecnológica [19], indica que los daños

por incidentes por seguridad de la información pueden ascender en promedio a los $720,000.00 dólares.

La firma auditora PWC – PricewaterhouseCoopers en unión con InfoSecurity Europe, en el año 2015, realizó un estudio a 664 empresas de diferentes nichos: salud, industrial, banca, etc. [20]. Con el fin de analizar las brechas de seguridad en empresas grandes y pequeñas, bajo el cual se determinó que el factor principal de fuga de información es el factor humano con un 75%, por incumplimiento o desconocimiento de la política de seguridad. Que el 72% de las compañías encuestadas no cuentan con una política de Seguridad clara y entendible, y que la mayoría de estos incidentes provienen porque no existe la prioridad o atención suficiente a la gestión de Seguridad.

Pero a pesar de lo manifestado, los pasos que han tomado estas compañías para mejorar su seguridad, es otorgarle mayor entrenamiento al Equipo de Seguridad (50%), cambiar la configuración de sus sistemas (47%) y cambiar políticas y procedimientos (39%), cuando se debería de partir por la política de Seguridad Interna. Y era de esperarse esos porcentajes, puesto a que solo un 25% de las empresas grandes

encuestadas han implementado la norma ISO 27001, a pesar de que el 51% de las empresas conocen la norma.

Por otra parte la FIEC durante estos 2 últimos años ha tenido 12 notificaciones de actividades maliciosas en diferentes equipos y han ocurrido 2 casos de hurto de equipos informáticos. Resultado de esto se han tomado medidas para evitar que ocurra, sin embargo, pudieron evitarse si se hubiese implementado controles para prevenirlas.

CAPÍTULO 3

ANÁLISIS DEL DST (Departamento de Soporte Técnico)

3.1 Situación actual

El Departamento de Soporte Técnico de la Facultad de Ingeniería en Electricidad y Computación - FIEC, es quien se encarga de administrar los recursos informáticos de la facultad y del funcionamiento de los laboratorios de computación que fueron creados para brindar servicio a los estudiantes y docentes y para que puedan desarrollar las actividades académicas por medio del préstamo de los computadores, adicionalmente a esto, el DST gradualmente fue incorporando otros servicios como la red inalámbrica y sistemas informáticos para uso de la comunidad de la FIEC, los cuales generan y mantienen información de interés que debe de mantenerse segura mediante el uso de alguna política de seguridad y claro está, tratando de mejorar constantemente la calidad en los servicios que brinda, sin embargo, el DST no cuenta con una política de seguridad ni procedimientos documentados, lo que puede

conllevar a que los activos informáticos se expongan a pérdidas y que esto afecte a las actividades que se realizan en la facultad.

Entre los problemas que presenta actualmente el DST se puede mencionar:

- ✓ Equipo portátil que se facilita no está asegurado con candados.
- ✓ Existen equipos que no cuentan con un regulador de energía.
- ✓ Existen pérdida de periféricos en los laboratorios.
- ✓ Los jefes de laboratorios no quieren asumir responsabilidad de los equipos.
- ✓ Los usuarios en general desconocen cómo proceder en el caso de recibir correo de un desconocido.

3.1.1 Misión del DST

Servir de apoyo tecnológico para profesores y estudiantes, a fin de que los recursos informáticos con los que cuenta la Facultad sean aprovechados al máximo, para potenciar el desarrollo académico-científico de la FIEC.

3.1.2 Visión del DST

Forjar líderes emprendedores para que aportando con sus capacidades, seamos referentes en implementaciones tecnológicas, que colaboren con el desarrollo de la ESPOL y de la sociedad en general.

3.1.3 Estrategia del DST

El Departamento de Soporte Técnico de la FIEC tiene los siguientes puntos como lineamientos básicos para establecer su conducta organizacional y estrategia administrativa:

- ✓ Establecer virtudes internas del personal, tales como:
  - o Puntualidad
  - o Responsabilidad
  - o Dinamismo
  - o Efectividad
  - o Eficiencia
  - o Orden

- ✓ Incentivar que quienes conforman el DST-FIEC estén continuamente actualizando sus conocimientos.
- ✓ Incentivar que los integrantes del DST-FIEC asuman su trabajo no sólo como una obligación, sino como una forma de alto aprendizaje. De esta manera, podrán aplicar los conocimientos adquiridos en su futuro profesional.
- ✓ Mantener un régimen de calidad, alineado con los objetivos establecidos en la Política de Calidad de la ESPOL.

3.1.4 Tareas del DST

Entre las tareas que tiene el DST se detalla las siguientes:

- ✓ Administración tecnológica en el ámbito informático y de comunicaciones de la Facultad.
- ✓ Servicio de correo y aplicaciones bajo plataforma google, con dominio FIEC.
- ✓ Soporte Técnico informático a los 35 laboratorios, grupos estudiantiles, personal administrativo y profesores de la Facultad, con un aproximado de 850 computadoras.
- ✓ Administración y soporte de Redes de datos y Servidores.

- ✓ Desarrollo, implementación, administración y soporte de Sistemas informáticos internos: CRM (Asistencia Técnica), Controlac, SATT, ARA-FIEC, Creación de cuentas, SR-FIEC, MSN-FIEC, Reservar Salas, ControlPC.
- ✓ Soporte a sistemas de audio y video proyección en Aulas, Auditorio y Laboratorios.
- ✓ Administración y soporte del Sitio Web.
- ✓ Administración del Laboratorio de Computación (Lab-Fiec), edificio 16-C, Programas Utilitarios 1 y 2 en el edificio 15A.

3.1.5 Funciones del personal del DST

En la Tabla 3 se detallan las funciones del personal que conforma el DST.

Tabla 3 – Funciones del personal del DST. Fuente: Documento de Perfiles y funciones del Departamento de Soporte Técnico de Computación de la FIEC.

Responsable:	Jefe del Laboratorio de Computación

Funciones:

- Administrar los recursos informáticos de la Facultad.
- Dirigir la implementación de proyectos informáticos para automatizar actividades administrativas/académicas de acuerdo a las necesidades de la Facultad.
- Dirigir y supervisar el trabajo del personal calificado del Departamento, de acuerdo al campo de acción.
- Administrar el inventario de Hardware (equipos de computación) y de las licencias de Software de la Facultad, en colaboración con el personal del Departamento.
- Servir de apoyo en la parte administrativa, según disposiciones del jefe inmediato.
- Ser responsable del cumplimiento de normas internas, tanto administrativas, operativas como de seguridad del área que abarca la Unidad, dentro del campo de acción.
- Recomendar la actualización de los equipos, servidores de la Facultad ó solicitar la garantía de los mismos cuando amerite.
- Solicitar al Decano la contratación de personal permanente y los temporales requeridos para proyectos específicos y/o cubrir servicios que brinda el Departamento.
- Presentar por lo menos una vez al año al Decano o Director informes de actividades y presupuestarios de la jefatura bajo su responsabilidad.
- Cumplir con cualquier actividad que dentro de la naturaleza de su cargo fuese solicitada por su jefe inmediato.

Responsable:	Asistente Técnico de Redes (1 Persona)

Funciones:

- Analizar nueva tecnología en el campo informático que pueda adoptarse para mejorar las labores de la Facultad, en las áreas académica y administrativa, o para las entidades que las requieran.
- Administrar los servidores de datos y web de la Facultad.
- Administrar los recursos de red cableada e inalámbrica de la Facultad.
- Administrar los recursos de impresión de la Facultad.
- Administrar los recursos de audio y video del Auditorio de la Facultad.
- Administrar los Sistemas de control de acceso, de seguridad y de Video-Conferencia de la Facultad.
- Mantener actualizados los diagramas de red de la Facultad.
- Participar en el diseño de nuevas redes que se implementen en la Facultad.
- Planificar el mantenimiento a las computadoras de los Laboratorios de la Facultad.
- Coordinar manejo de inventario de Hardware y Software de la Facultad.
- Coordinar los cambios en las plataformas de los servicios que ofrece el Departamento.
- Proponer soluciones informáticas a problemas que sean derivados hacia el Departamento, según su campo de acción.
- Coordinar cursos de capacitación sobre las tecnologías adoptadas e investigadas por el Departamento, según su ámbito de acción.
- Cumplir con cualquier actividad que dentro de la naturaleza de su cargo fuese solicitada por su jefe inmediato.

Responsable:	Asistente Técnico de Soporte (3 Persona)

Funciones:

- Ejecutar junto a los ayudantes técnicos de soporte, el mantenimiento preventivo y correctivo de las computadoras que prestan servicio en los laboratorios de la Facultad.
- Brindar mantenimiento preventivo básico a los proyectores de la Facultad, así como mantener actualizado el listado de suministros para reemplazo de lámparas de proyectores.
- Evaluar los paquetes de software a ser instalados en las computadoras de los

laboratorios.
- Capacitar a los respectivos ayudantes de los laboratorios, en el mantenimiento de los computadores de la Facultad, cuando sea necesario.
- Coordinar con el ayudante administrativo la actualización del inventario de computadores de la Facultad.
- Coordinar soporte de última línea a los Laboratorios de computación, al personal docente y administrativo de la facultad.
- Recomendar la actualización de los computadores de la Facultad, con un período no menor a 3 años.
- Mantener actualizado el inventario de hardware de la Facultad.
- Instalar y mantener los Sistemas Académicos en los computadores del personal docente y administrativo de la Facultad.
- Reportar a los jefes de laboratorios las partes de equipos de computación que deben ser reemplazados, para proceder a su reparación o reposición, previa verificación de stock de repuestos.
- Dar soporte al sistema de impresiones que dispone la Facultad.
- Compilar y mantener copia de paquetes de software que son usados en los servidores de la Facultad.
- Supervisar las tareas de los ayudantes técnicos de soporte.
- Cumplir con cualquier actividad que dentro de la naturaleza de su cargo fuese solicitada por su jefe inmediato.

Responsable:	Asistente Técnico de Desarrollo (1Persona)

Funciones:

- Coordinar el análisis, adaptación e implementación de soluciones de software bajo licenciamiento libre que le sean requeridos a la Unidad, de acuerdo a su ámbito de acción.
- Administrar los sistemas implementados por la Unidad.
- Coordinar la instalación, prueba y soporte de los paquetes de software que son implementados o adaptados por la Unidad.
- Coordinar cursos de capacitación sobre las tecnologías adoptadas e investigadas por la Unidad, según su ámbito de acción.
- Realizar la actualización de los programas a nuevas versiones o diferentes sistemas operativos.
- Implementar manuales de uso de los sistemas implementados por la Unidad.
- Cumplir con cualquier actividad que dentro de la naturaleza de su cargo fuese solicitada por su jefe inmediato.

Responsable:	Webmaster (1Persona)

Funciones:

- Administrar el sitio web de la Facultad y de las entidades adscritas a la unidad.
- Realizar periódicamente respaldos de la información del Web-Site
- Recomendar la incorporación de nuevos contenidos, tecnologías y servicios dentro del Web-Site de la Facultad o de las entidades que lo requieran en el ámbito de acción de la Unidad.
- Realizar evaluaciones periódicas del desempeño de los web sites a cargo de la Unidad.
- Diseñar la publicidad, flujo de carreras, afiches y demás artículos de promoción para actividades de la Facultad y para las demás entidades que lo requieran en el ámbito de acción de la Unidad.
- Crear, mantener y administrar las bases de datos del sistema.
- Coordinar visitas técnicas a entidades que requieran de diseño Web.
- Cumplir con cualquier actividad que dentro de la naturaleza de su cargo fuese solicitada por su jefe inmediato.

3.1.6 Reglamento

EL DST se maneja un reglamento que sólo rigen para el LAB-FIEC y se detalla a continuación:

Reglamento Básico del Laboratorio de Computación de la FIEC

1. Las máquinas serán prestadas con el carnet estudiantil actualizado, previa verificación del ayudante de turno.
2. Está terminantemente prohibido prestar el User y Password a otra persona, al igual que ausentarse de la máquina para que la utilice otro usuario.
3. Las máquinas serán prestadas por un tiempo máximo de 2 horas al día.
4. No se permiten mover las sillas entre laboratorios.
5. No se permite utilizar el messenger ni ningún otro programa de chat.
6. No se permiten personas de pie dentro del laboratorio.
7. Debe mantener el silencio dentro del laboratorio.

8. Está terminantemente prohibido ingresar a sitios Web donde exhiban material pornográfico, ni a otros que atenten a la moral.

9. Sólo se permite un usuario por máquina y silla.

10. No puede ingresar al laboratorio con comida y/o bebida.

11. No se permite utilizar Laptops que ocupen el espacio físico de una PC en los laboratorios.

12. En caso de préstamo de PC y/o proyector para alguna exposición, deberá llenar la solicitud respectiva y, se sujetará a disponibilidad de los mismos. El estudiante o profesor se hará responsable de los equipos durante el periodo del préstamo. No se podrán prestar PCs que se utilizan dentro de los Laboratorios de Computación.

URBANIDAD BÁSICA

- ✓ Mantenga silencio dentro del Laboratorio.
- ✓ No ingrese con comida.
- ✓ Solo una persona por silla/computadora.

- ✓ Siéntese bien y al salir cierre la silla.
- ✓ No dejar desperdicios dentro del laboratorio.
- ✓ Apague el computador al terminar.

3.2 Identificación de activos de información

Los activos que administran el DST se detallan en la Tabla 4.

Tabla 4 - Activos que administra el DST. Fuente: El autor.

ACTIVOS DE LA FIEC
[bd_crm] Base de Datos de CRM
[bd_reservar] Base de Datos de Reservar Salas
[bd_controlac] Base de Datos de Controlac
[bd_reunion] Base de datos de Reuniones
[bd_ara] Base de Datos de ARA
[bd_satt] Base de Datos de SATT
[backup] Copias de respaldo
[source] Código fuente
[files] Archivos
[bd_controlpc] Base de Datos de CONTROLPC
[conf] Datos de configuración
[log] Registro de actividad
[bd_ldap] LDAP
[bd_sitioFiec] Base de Datos del sitio Web de la FIEC
[S] Servicios
[serv_a/v] Audio y Video
[serv_equi] Préstamo de equipos
[serv_support] Asistencia técnica
[serv_dev] Implementación y administración de sistemas/sitio web para la FIEC
[serv_acco] Gestión de identidades (creación de cuentas)
[serv_wifi] Red inalámbrica exclusiva de la FIEC
[email] Correo electrónico
[serv_mante] Mantenimiento a equipos
[serv_file] Almacenamiento de archivos y aplicaciones desarrolladas por estudiantes
[serv_labs] Préstamo de laboratorios
[sis_crm] Sistema CRM
[sis_control] Sistema Controlac
[sis_creacion] Sistema Creación de Cuentas
[sis_reunion] Sistema de Reuniones
[sis_reservar] Sistema Reservar Salas

[sis_ara] Sistema ARA
[sis_satt] Sistema SATT
[pkt] Repositorio de Software vario
[sis_controlpc] Sistema CONTROLPC
[av] Anti virus
[sis_portal] Portal Cautivo
[print] Medios de impresión
[scan] Escáneres
[cam] Cámara IP
[mobile] Laptop
[srv_strmg]Streaming
[wap] Punto de acceso inalámbrico
[pc] Computador
[srv_files] Archivos
[srv_control] Control-PC
[srv_dhcp] DHCP
[srv_radius] Radius
[switch] Conmutadores
[router] Ruteadores
[srv_mail]Correos
[srv_db] Base de Datos
[srv_web] Web
[srv_ant] Antivirus
[wifi] Red inalámbrica
[Media] Soportes de información
[disk] Discos
[san] Almacenamiento en red
[tape] Cinta magnética
[furniture] Mobiliario: armarios, racks etc
[tools] Herramientas de soporte y mantenimiento
[tools_network] Herramientas de soporte y mantenimiento redes
[ss] Sistema de seguridad
[ups] Sistemas de alimentación ininterrumpida
[ac] Equipos de climatización
[building] Edificio
[local] Cuarto de rack y servidores
[adm] Administradores de la infraestructura tecnológica
[com] Administrador de redes y servidores
[ast] Analista de soporte técnico
[des] Desarrolladores / programadores
[wm] Web master

3.3 Análisis de riesgo basado en MAGERIT

Para realizar el análisis de riesgo de los activos se ha usado la metodología MAGERIT en la que primero se debe identificar los activos,

y para ello se los ha categorizado según la metodología lo describe en el capítulo II de este documento.

3.3.1 Identificación de activos

Esta constituye la primera etapa de desarrollo de la metodología de magerit, lo que implica que si se realiza una buena identificación de activos, permitirá valorar a los activos correctamente, identificar las amenazas, vulnerabilidades y asociar las salvaguardas que ayuden a preservar a los mismos. En la Tabla 5 se detalla la clasificación de activos mientras que en la Tabla 6 se identifican los activos de acuerdo a la clasificación que la metodología ha definido.

Tabla 5 - Clasificación de los activos. Fuente: El autor

[D] Datos / Información	Corresponde a los datos que administra el DST.
[S] Servicios	Son los servicios que pueden hacer uso estudiantes, docentes y administrativos.
[SW] Aplicaciones (software)	Son los aplicaciones/sistemas que el DST ha desarrollado para uso de la comunidad de la FIEC.
[HW] Equipo Informático (hardware)	Corresponde al equipo informático de la FIEC que administra el DST.
[COM] Redes de comunicaciones	Son los medios de transporta de la información que cuenta la FIEC.
[Media] Soportes de información	Son los soportes de almacenamiento de la información.

[AUX] Equipamiento auxiliar	Corresponde a equipamiento adicional que posee la FIEC para soportar a los equipos de red, servidores y servicios que ofrece.
[L] Instalaciones	Corresponde a la infraestructura física donde se encuentran los centros de datos y cableado de la FIEC.
[P] Personal	Personal responsable de la administración de la infraestructura informática de la FIEC.

Tabla 6 - Identificación de los activos. Fuente: El autor

[D] Datos / Información
[bd_crm] Base de Datos de CRM (1) [bd_reservar] Base de Datos de Reservar Salas (2) [bd_controlac] Base de Datos de Controlac (3) [bd_reunion] Base de datos de Reuniones (4) [bd_ara] Base de Datos de ARA (5) [bd_satt] Base de Datos de SATT (6) [backup] Copias de respaldo (7) [source] Código fuente (8) [files] Archivos (9) [bd_controlpc] Base de Datos de CONTROLPC (10) [conf] Datos de configuración (11) [log] Registro de actividad (12) [bd_ldap] LDAP (13) [bd_sitioFiec] Base de Datos del sitio Web de la FIEC (14**)**
(1) Base con datos de los tickets que corresponden a los incidentes registrados, asociados a los usuarios. (2) Base de datos con las reservas de aulas, laboratorios y otras instalaciones. (3) Base con datos de los cursos, detalle de clases y registro de docentes por semestre. (4) Base con datos de reuniones, listas de convocados y asistencia. (5) Base con datos de estudiantes, directores de proyectos/tesis y artículo de fin de carrera. (6) Base con datos de estudiantes, evaluadores, directores de proyectos/tesis, tema y temario de trabajo de fin de carrera. (7) Respaldos de información de los usuarios, servidores, imágenes de equipos o archivos importantes. (8) Código fuente de proyectos desarrollados en el DST. (9) Archivos de los registros de instalación, de red, inventario, oficios, actas y manuales que maneja el DST. (10) Base de con datos de equipos, ips, usuarios, horarios de uso de laboratorios. (11) Datos de configuración de los equipos de red, servidores, computadoras, etc. (12) Registro de actividad de los servidores, registro de accesos a equipos y sitios. (13) Datos de los usuarios de la FIEC. (14) Datos de los contenidos del sitio de la FIEC.
[S] Servicios
[serv_a/v] Audio y Video (1) [serv_equi] Préstamo de equipos (2)

[serv_support] Asistencia técnica (3)
[serv_dev] Implementación y administración de sistemas/sitio web para la FIEC (4)
[serv_acco] Gestión de identidades (creación de cuentas) (5)
[serv_wifi] Red inalámbrica exclusiva de la FIEC (6)
[email] correo electrónico (7)
[serv_mante] Mantenimiento a equipos (8)
[serv_file] Almacenamiento de archivos y aplicaciones desarrolladas por estudiantes (9)
[serv_labs] Préstamo de laboratorios (10)

(1) Servicio interno de video conferencias, audio y video para auditorio y otras instalaciones.
(2) Servicio interno de préstamo de equipos informáticos para docentes, administrativos y grupo estudiantiles.
(3) Servicio interno de asistencia y soporte técnico para docentes, administrativos y laboratorios en general.
(4) Servicio interno de implementación y administración de sistemas y sitio web de la facultad.
(5) Servicio de creación de cuentas de usuarios para hacer uso de los servicios informáticos que ofrece la facultad.
(6) Servicio interno de administración de la red inalámbrica de la FIEC.
(7) Servicio de correo electrónico a través de la plataforma de gmail.
(8) Servicio interno de mantenimiento de equipos informáticos que sean considerados bienes de la FIEC.
(9) Servicio interno de almacenamiento de archivos y sistemas temporales.
(10) Servicio interno de préstamo de laboratorios a docentes y estudiantes de la facultad.

[SW] Aplicaciones (software)

[sis_crm] Sistema CRM (1)
[sis_control] Sistema Controlac (2)
[sis_creacion] Sistema Creación de Cuentas (3)
[sis_reunion] Sistema de Reuniones (4)
[sis_reservar] Sistema Reservar Salas (5)
[sis_ara] Sistema ARA (6)
[sis_satt] Sistema SATT (7)
[pkt] Repositorio de Software vario (8)
[sis_controlpc] Sistema CONTROLPC (9)
[av] Anti virus (10)
[sis_portal] Portal Cautivo (11)

(1) Sistema para atender incidentes.
(2) Sistema para registrar las clases de las materias que dictan los docentes.
(3) Sistema para creación de cuentas de usuario para estudiante.
(4) Sistema para convocar a reuniones y registrar y asistencia a la misma.
(5) Sistema para reservar aula o laboratorios para clases.
(6) Sistema de repositorio de artículos de fin de carrera
(7) Sistema de administración de temas y temarios.
(8) Repositorio de Software vario para uso de docentes y administrativos.
(9) Sistema para administrar los laboratorios y computadoras de los laboratorios.
(10) Antivirus institucional
(11) Portal cautivo para acceso de la red inalámbrica.

[HW] Equipo Informático (hardware)

[print] Medios de impresión (1)
[scan] Escáneres (2)
[cam] Cámara IP (3)
[mobile] Laptop (4)
[srv_strmg] Streaming (5)

[wap] Punto de acceso inalámbrico (6) [pc] Computador (7) [srv_files] Archivos (8) [srv_control] Control-PC (9) [srv_dhcp] DHCP (10) [srv_radius] Radius (11) [switch] Conmutadores (12) [router] Ruteadores (13) [srv_mail] Correos (14) [srv_db] Base de Datos (15) [srv_web] Web (16) [srv_ant] Antivirus (17)
(1) Impresoras de la facultad. (2) Escáneres. (3) Cámaras IP. (4) Laptops asignadas a docentes, administrativos y de uso para clases. (5) Equipos para realizar streaming y servidor. (6) Equipos de punto de acceso inalámbrico. (7) Computadoras de la FIEC. (8) Servidor de archivos, donde se alojan registros de instalación, de red, inventario, oficios, actas y manuales que maneja el DST. (9) Servidor del Sistema ControlPC. (10) Servidor DHCP. (11) Servidor Radius. (12) Equipo de red, conmutadores. (13) Equipo de red, ruteadores. (14) Servidor de correo. (15) Servidor de Base de datos. (16) Servidor Web. (17) Servidor de antivirus.
[COM] Redes de comunicaciones
[wifi] Red inalámbrica (1) [LAN] Red local (2)
(1) Red inalámbrica para uso los usuarios de la FIEC. (2) Red cableada administrada por el DST.
[Media] Soportes de información
[disk] Discos (1) [san] Almacenamiento en red (2) [tape] Cinta magnética (3)
(1) Discos duros. (2) Equipo para almacenamiento en red y respaldos. (3) Cintas magnéticas para realizar respaldos.
[AUX] Equipamiento auxiliar
[furniture] Mobiliario: armarios, racks etc (1) [tools] Herramientas de soporte y mantenimiento (2) [tools_network] Herramientas de soporte y mantenimiento redes (3) [ss] Sistema de seguridad (4) [ups] Sistemas de alimentación ininterrumpida (5) [ac] Equipos de climatización (6)

(1) Mobiliario de red. (2) Herramientas para poder dar soporte técnico y mantenimiento. (3) Herramientas para poder dar soporte técnico y mantenimiento de redes. (4) Sistema de seguridad conformado por paneles, baterías, lectores entre otros. (5) Equipos de alimentación ininterrumpida UPS. (6) Acondicionador de aire.
[L] Instalaciones
[building] edificio (1) [local] cuarto de rack y servidores (2)
(1) 15, 15A, 16AB-C, 24 AB. (2) Rack y Servidores.
[P] Personal
[adm] Administradores de la infraestructura tecnológica (1) [com] Administrador de redes y servidores (2) [ast] Analista de soporte técnico (3) [des] Desarrolladores / programadores (4) [wm] Web master (5)
(1) Administradores de la infraestructura tecnológica de la FIEC. (2) Administrador de redes y servidores de la FIEC. (3) Analista de soporte técnico de la FIEC. (4) Analista de soporte técnico de desarrollo de la FIEC. (5) Web master de la FIEC.

3.3.2 Valoración de activos

En la Tabla 8 se presenta la valorización de activos, tomando en consideración los criterios del ANEXO E y la escala de valores de la Tabla 7.

Tabla 7 - Escala de valorización de los activos. Fuente: Magerit.

Valor	
10	extremo
9	muy alto
6-8	alto
3-5	medio
1-2	bajo
0	despreciable

Dimensiones a evaluar:

- **[D]** Disponibilidad
- **[I]** Integridad
- **[C]** Confidencialidad

Tabla 8 - Valorización de los activos. Fuente: El autor.

CLASF.	ACTIVOS	[D]		[I]		[C]		[A]		[T]		VALOR
[D] Datos / Información	[bd_crm]	3	3.olm	5	3.lg, 5.adm	5	5.lbl, 3.lg	3	3.lg	3	3.si	4
	[bd_reservar]	4	4.pi1	5	5.adm, 3.lg	2	2.lbl	0	0.04	3	3.si	3
	[bd_controlac]	6	6.pi1	3	3.adm, 3.lg	6	6.lbl, 3.lg	5	3.lg, 5.olm	3	3.si	5
	[bd_reunion]	3	3.olm	5	5.adm, 5.olm	7	7.lbl, 3.lg	5	3.lg, 5.olm	3	3.si	5
	[bd_ara]	5	5.olm	5	5.adm	2	2.lbl	1	1.lg	3	3.si	3
	[bd_satt]	5	5.adm, 5.pi	5	5.olm	7	7.lbl, 3.lg	3	3.adm, 3.lg	3	3.si	5
	[backup]	7	7.olm	3	3.adm	7	7.lbl, 3.lg	3	3.da, 3,lg, 3.olm	3	3.si	5
	[source]	7	7.olm, 7.adm	7	7.adm	7	7.lbl, 3.lg	3	3.olm	7	7.si	6
	[files]	7	7.olm	5	5.adm	7	7.lbl	3	3.da, 3.olm	3	3.si	5
	[bd_controlpc]	3	3.adm	3	3.olm	7	7.lbl	0	0.04	3	3.si	3
	[conf]	7	7.olm, 1.da	5	5.adm	8	8.lbl, 1.si	3	3.da, 1.si, 3.olm	7	7.si	6
	[log]	7	7.olm, 7.si	5	5.olm, 3.si	7	7.lbl, 3.si	3	3.da, 3.si, 3.olm	7	7.si	6
	[bd_ldap]	7	7.olm, 3.da, 5.adm, 3.lg	7	7.olm, 3.da, 5.adm	8	8.lbl	3	3.da, 3,lg	7	7.si	6
	[bd_sitioFiec]	7	5.olm, 7.adm	7	7.olm, 3.da, 5.adm	7	7.lbl, 3.lg	3	3.da, 3,lg, 3.olm	7	7.si	6
[S] Servicios	[serv_a/v]	3	3.da					3	3.da, 3.lg	3	3.si	3
	[serv_equi]	3	3.da					3	3.da, 3.lg	3	3.si	3
	[serv_support]	3	3.da					3	3.lg	3	3.si	3
	[serv_dev]	3	3.da,					3	3.da,	3	3.si	3

			1.olm, 1.adm						1.olm, 1.adm, 3.si			
	[serv_acco]	3	3.da					3	3.da	3	3.si	3
	[serv_wifi]	3	3.da, 1.da, 3.olm					3	3.da,3. si	3	3.si	3
	[email]	3	3.da, 3.adm, 3.olm					3	3.da, 3.adm, 3.olm	3	3.si	3
	[serv_mante]	5	5.da					3	3.lg	3	3.si	4
	[serv_file]	5	5.da					3	3.da	3	3.si	4
	[serv_labs]	5	5.da					3	3.da	3	3.si	4
[SW] Aplicaciones (software)	[sis_crm]	3	3.olm, 3.adm	2	1.adm, 2.lg	3	1.olm, 3.lg	3	3.da,3. adm	3	3.si	3
	[sis_control]	4	4.pi1	1	1.adm	2	1.olm, 2.lg	3	3.lg	3	3.si	3
	[sis_creacion]	4	4.pi1	3	3.adm	1	1.olm, 1.adm	3	3.da,1.l g	3	3.si	3
	[sis_reunion]	5	5.adm	5	5.adm	3	1.olm, 3.lg	5	3.da,5. adm	3	3.si	4
	[sis_reservar]	4	4.pi1	5	5.adm	1	1.olm, 0.4	3	3.da,1. adm	3	3.si	3
	[sis_ara]	5	5.adm	5	5.adm	3	1.olm, 3.lg	3	3.da,1. adm	3	3.si	4
	[sis_satt]	5	5.olm	5	5.adm	1	1.olm	3	3.da	3	3.si	3
	[pkt]	5	5.olm	3	3.olm	3	3.lg	3	3.da	3	3.si	3
	[sis_controlpc]	5	5.adm	5	5.adm	1	1.olm, 1.adm	3	3.da,1. adm	1	1.si	3
	[av]	5	5.adm	5	5.adm	5	5.olm	3	3.da	3	3.si	4
	[sis_portal]	5	5.adm	5	5.adm	5	5.olm	3	3.da	3	3.si	4
[HW] Equipo Informático (hardware)	[print]	1	1.da, 1.adm	1	1.da, 1.adm	0	0.4			3	3.si	1
	[scan]	1	1.da, 1.adm	1	1.da, 1.adm	0	0.4			3	3.si	1
	[cam]	3	3.si	3	3.olm	1	1.olm			3	3.si	3
	[mobile]	3	3.adm	3	3.adm	3	3.olm			7	7.si	4
	[srv_strmg]	1	1.adm	3	3.si	3	1.olm			7	7.si	4
	[wap]	5	5.adm, 1.da, 3.olm	3	3.olm, 3.adm	3	3.olm			7	7.si	5
	[pc]	7	7.adm	7	7.adm	3	3.olm			7	7.si	6
	[srv_files]	5	5.adm	5	5.adm, 3.olm	5	5.olm, 3.si			9	9.si	6
	[srv_control]	5	5.adm, 3.da	5	5.adm, 3.da	5	5.olm, 3.si			9	9.si	6
	[srv_dhcp]	5	5.adm, 3.da	5	5.adm, 3.da	5	5.olm, 3.si			9	9.si	6
	[srv_radius]	5	5.adm, 3.da, 1.olm	5	5.adm, 3.da, 1.olm	5	5.olm, 3.si			9	9.si	6
	[switch]	9	9.adm, 9.olm, 3.da	7	1.da, 7.olm, 7.adm, 7.si	7	7.olm, 7.si			7	7.si	8
	[router]	9	9.adm, 9.olm,	9	9.olm, 9.si, 1.da,	9	9.olm, 7.si			7	7.si	9

			3.da		7.adm							
	[srv_mail]	7	7.adm, 1.olm	9	9.si, 3.da, 7.olm, 5.adm	9	9.olm, 9.si			9	9.si	9
	[srv_db]	7	7.adm, 3.da, 9.olm	9	9.si, 3.da, 7.olm, 5.adm	9	9.olm, 9.si			9	9.si	9
	[srv_web]	7	5.adm, 3.olm	9	5.adm, 3.olm	9	9.olm, 9.si			9	9.si	9
	[srv_ant]	7	7.adm, 9.si, 3.olm	9	9.si	9	9.olm			9	9.si	9
[COM] Redes de comunicaciones	[wifi]	5	5.adm	5	5.adm	3	3.olm			9	9.si	6
	[LAN]	9	9.adm, 3.da, 9.olm	9	9.olm, 9.si	9	9.olm, 9.si			9	9.si	9
[Media] Soportes de información	[disk]	5	5.adm	6	6.pi1	7	7.olm	3	3.da	3	3.si	5
	[san]	7	7.adm	6	6.pi1	7	7.olm	3	3.da	3	3.si	5
	[tape]	7	7.adm	6	6.pi1	7	7.olm	3	3.da	3	3.si	5
[AUX] Equipamiento auxiliar	[furniture]	1	1.adm	1	1.olm							1
	[tools]	3	3.adm	3	3.adm							3
	[tools_network]	3	3.adm	3	3.adm							3
	[ss]	7	7.olm, 7.si	7	7.olm, 3.si							7
	[ups]	9	9.adm	9	9.olm, 7.adm							9
	[ac]	9	9.adm	9	9.olm, 7.adm							9
[L] Instalaciones	[building]	7	7.olm	9	9.olm							5
	[local]	7	7.olm	9	9.olm							5
[P] Personal	[adm]	7	7.adm	7	7.olm							7
	[com]	7	7.adm	7	7.olm							7
	[ast]	7	7.adm	7	7.olm							7
	[des]	7	7.adm	7	7.olm							7
	[wm]	7	7.adm	7	7.olm							7

Como resultado de esta evaluación podemos notar que los activos que tienen mayor valoración son los que se encuentran dentro del grupo de Equipo informático, Redes de telecomunicaciones y Equipamiento auxiliar.

3.3.3 Dependencias entre activos.

Las dependencias entre los activos que administra el DST se detallan en el ANEXO F, de acuerdo a lo establecido por la metodología que se usa en el presente documento.

3.3.4 Identificación de las amenazas.

El desarrollo de esta tarea puede apreciarse en la Tabla 9, donde se identifican las amenazas que pueden afectar a los activos.

Tabla 9 - Identificación de amenazas de los activos. Fuente: El autor.

	ACTIVOS																											
	[D]			[S]			[SW]			[HW]			[Media]			[AUX]			[L]			[COM]			[P]		
	[D]	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]
AMENAZAS																												
[N] Desastres naturales																												
[N.1]Fuego										x			x			x			x									
[N.2] Daños por agua										x			x			x			x									
[I] De origen industrial																												
[I.1] Fuego										x			x			x			x									
[I.2] Daños por agua										x			x			x			x									
[I.*] Desastres industriales										x			x			x			x									
[I.3] Contaminación mecánica										x			x			x												
[I.4] Contaminación electromagnética										x			x			x												
[I.5] Avería de origen físico o lógico							x			x			x			x												
[I.6] Corte de suministro eléctrico										x			x			x												
[I.7] Condiciones inadecuadas de temperatura o humedad										x			x			x												
[I.8] Falla de servicios de comunicaciones																						x						
[I.10] Degradación de los soportes de almacenamiento de información													x															
[E]Errores y fallos no intencionados																												
[E.1] Errores de los usuarios	x	x	x	x	x	x	x	x	x				x	x	x													
[E.2] Errores del administrador	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x				x	x	x				
[E.3] Errores de monitorización (log)		x																										

[E.4] Errores de configuración		x																									
[E.8] Difusión de Software dañino							x	x	x																		
[E.19] Fugas de información						x			x															x			
[E.15] Alteración accidental de la información		x																									
[E.18] Destrucción de información	x																										
[E.19] Fugas de información			x						x					x			x			x			x			x	
[E.20] Vulnerabilidades de los programas (software)							x	x	x																		
[E.21] Errores de mantenimiento / actualización de programas (software)							x	x																			
[E.23] Errores de mantenimiento / actualización de equipos (hardware)										x			x			x											
[E.24] Caída del sistema por agotamiento de recursos				x																							
[E.25] Pérdida de equipos										x		x	x		x	x		x									
[E.28] Indisponibilidad del personal																										x	
[A] Ataques intencionados																											
[A.3] Manipulación de los registros de actividad (log)		x																									
[A.4] Manipulación de la configuración	x	x	x																								
[A.5] Suplantación de la identidad del usuario	x	x	x	x	x	x	x	x	x													x	x	x			
[A.6] Abuso de privilegios de acceso	x	x	x	x	x	x	x	x	x	x	x	x										x	x	x			
[A.7] Uso no previsto				x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x						
[A.8] Difusión de software dañino (virus, spyware, troyanos, gusanos, etc)							x	x	x																		
[A.9] [Re-]encaminamiento de mensajes									x															x			
[A.10] Alteración de secuencia					x			x															x				
[A.11] Acceso no autorizado		x	x			x	x				x	x		x	x		x	x		x	x		x	x			
[A.12] Análisis de tráfico																								x			
[A.13] Repudio		x			x																						

[A.14] Interceptación de información (escucha)																									x			
[A.15] Modificación deliberada de la información		x			x			x						x						x							
[A.18] Destrucción de información	x			x			x						x						x			x					
[A.19] Divulgación de información			x			x			x						x						x			x			
[A.22] Manipulación de programas							x	x	x																		
[A.23] Manipulación de los equipos										x	x	x															
[A.24] Denegación de servicio				x						x												x					
[A.25] Robo										x		x	x		x	x		x									
[A.26] Ataque destructivo										x			x			x			x								
[A.28] Indisponibilidad del personal																										x		
[A.29] Extorsión																										x	x	x
[A.30] Ingeniería social																										x	x	x

3.3.5 Valoración de amenazas

Para esta tarea se hace uso de las escalas de la Tabla 10 y 11, la primera es de utilidad para evaluar la probabilidad de ocurrencia de la amenaza que se relaciona con cada activo, mientras que la segunda tabla sirve para evaluar la degradación que causarían las amenazas en los activos si ésta llega a materializar. Desde la tabla 12 a la tabla 20 se puede ver la valoración de las amenazas de acuerdo a lo señalado anteriormente.

Tabla 10 - Tabla de frecuencia. Fuente: Magerit.

Frecuencia	
MA	100
A	10
M	1
B	1/10
MB	1/100

Tabla 11 - Tabla de degradación. Fuente: Magerit.

Degradación	
MA	100
A	80
M	50
B	30
MB	5

Estas tablas servir para evaluar que tan afectado resulta un activo por causa de un incidente en caso de que ocurriera.

Tabla 12 - Valoración de amenazas por activos de DATOS. Fuente: El autor.

ACTIVO**: DATOS**																							
				[bd_crm]				**[bd_reservar]**				**[bd_controlac]**				**[bd_reunion]**				**[bd_ara]**			
				[F]	**[Deg]**			**[F]**	**[Deg]**			**[F]**	**[Deg]**			**[F]**	**[Deg]**			**[F]**	**[Deg]**		
AMENAZAS	**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**
[E.1] Errores de los usuarios	x	x	x	1	5	50	5	10	5	50	5	1	5	80	5	1	30	100	5	10	5	80	5
[E.2] Errores del administrador	x	x	x	0,1	80	80	5	0,1	80	80	5	0,1	80	80	5	0,1	80	80	5	0,1	80	80	5
[E.3] Errores de monitorización (log)		x																					
[E.4] Errores de configuración		x																					
[E.15] Alteración accidental de la información		x		0,1		50		0,1		50		0,1		100		0,1		80		0,1		100	
[E.18] Destrucción de información	x			0,1	100			0,1	100			0,1	100			0,1	100			0,1	100		
[E.19] Fugas de información			x	0,1			5	0,1			5	0,1			5	0,1			50	0,1			5
[A.3] Manipulación de los registros de actividad (log)		x																					
[A.4] Manipulación de la configuración	x	x	x																				
[A.5] Suplantación de la identidad del usuario	x	x	x	0,1	80	80	5	0,1	50	80	5	0,1	80	80	30	0,1	80	80	50	0,1	80	80	30
[A.6] Abuso de privilegios de acceso	x	x	x	0,1	50	50	30	0,1	50	80	30	0,1	50	50	30	0,1	80	80	30	0,1	50	50	30
[A.11] Acceso no autorizado		x	x	0,1	80	100	5	0,1	80	100	5	0,1	80	100	30	0,1	80	80	50	0,1	80	80	30
[A.13] Repudio		x																					
[A.15] Modificación deliberada de la información		x		0,1		80		0,1		50		0,1		80		0,1		80		0,1		80	
[A.18] Destrucción de información	x			0,1	100			0,1	100			0,1	100			0,1	100			0,1	100		
[A.19] Divulgación de información			x	0,1			5	0,1			5	0,1			5	0,1			30	0,1			5

				[bd_satt]				[backup]				[source]				[files]				[bd_controlpc]			
				[F]	[Deg]			[F]	[Deg]			[F]	[Deg]			[F]	[Deg]			[F]	[Deg]		
AMENAZAS	**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**
[E.1] Errores de los usuarios	x	x	x	1	5	30	5																
[E.2] Errores del administrador	x	x	x	0,1	80	80	80	0,1	80	80	80	0,1	30	80	5	1	50	50	50	0,1	50	80	5
[E.3] Errores de monitorización (log)		x																					
[E.4] Errores de configuración		x																					
[E.15] Alteración accidental de la información		x		0,1		50		0,1		80		0,1		80		0,1		80		0,1		50	
[E.18] Destrucción de información	x			0,1	100			0,01	100			0,1	100			0,1	100			0,01	100		
[E.19] Fugas de información			x	0,1			30	0,01			80	0,1			80	0,1			80	0,01			5
[A.3] Manipulación de los registros de actividad (log)		x																					
[A.4] Manipulación de la configuración	x	x	x																				
[A.5] Suplantación de la identidad del usuario	x	x	x	0,1	80	80	30	0,1	80	80	80	0,1	80	80	80	0,01	80	80	30	0,1	80	80	5
[A.6] Abuso de privilegios de acceso	x	x	x	0,1	80	80	50	0,1	50	50	50	0,1	50	50	30	0,01	80	80	50	0,1	50	50	5
[A.11] Acceso no autorizado		x	x	0,1	80	80	50	0,1	80	80	80	0,1	80	80	100	0,01	80	80	80	0,1	80	80	5
[A.13] Repudio		x																					
[A.15] Modificación deliberada de la información		x		0,1		80		0,1		100		0,1		100		0,1		100		0,1		80	
[A.18] Destrucción de información	x			0,1	100			0,1	100			0,1	100			0,1	100			0,1	100		
[A.19] Divulgación de información			x	0,1			30	0,1			80	0,1			80	0,1			80	0,1			5

				[conf]				[log]				[bd_ldap]				[bd_sitioFiec]			
				[F]	[Deg]			[F]	[Deg]			[F]	[Deg]			[F]	[Deg]		
AMENAZAS	**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**
[E.1] Errores de los usuarios	x	x	x																
[E.2] Errores del administrador	x	x	x	0,1	80	80	80	0,1	80	80	5	0,1	80	80	30	0,1	80	80	30
[E.3] Errores de monitorización (log)		x						0,1		80									
[E.4] Errores de configuración		x		0,1		80													
[E.15] Alteración accidental de la información		x		0,1		80		0,1		80		0,1		100		0,1		100	
[E.18] Destrucción de información	x			0,1	100			0,1	100			0,1	100			0,1	100		
[E.19] Fugas de información			x	0,1			100	0,01			80	0,1			50	0,1			50
[A.3] Manipulación de los registros de actividad (log)		x						0,1		80									
[A.4] Manipulación de la configuración	x	x	x	0,1	80	80	80												
[A.5] Suplantación de la identidad del usuario	x	x	x	0,01	80	80	80	0,01	80	80	80	0,01	80	80	80	0,01	80	80	80
[A.6] Abuso de privilegios de acceso	x	x	x	0,01	50	50	50	0,01	80	80	80	0,01	80	80	80	0,01	80	80	80
[A.11] Acceso no autorizado		x	x	0,01	80	80	80	0,1	80	80	80	0,01	80	80	80	0,01	80	80	80
[A.13] Repudio		x						0,1		80									
[A.15] Modificación deliberada de la información		x		0,01		100		0,1		80		0,01		100		0,01		100	
[A.18] Destrucción de información	x			0,1	100			0,1	100			0,1	100			0,1	100		
[A.19] Divulgación de información			x	0,1			100	0,01			80	0,01			80	0,01			80

Tabla 13 - Valoración de amenazas por activos de SERVICIOS. Fuente: El autor.

ACTIVO**: SERVICIOS**

				[servi_a/v]				[servi_equi]				[servi_support]				[servi_dev]				[servi_acco]			
				[F]	[Deg]			[F]	[Deg]			[F]	[Deg]			[F]	[Deg]			[F]	[Deg]		
AMENAZAS	**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**
[E.1] Errores de los usuarios	x	x	x	1	50	50	50	1	50	50	50	1	50	50	50					1	5	5	5
[E.2] Errores del administrador	x	x	x	1	80	50	50	1	80	50	50	1	80	50	50	1	80	50	50	1	80	80	80
[E.24] Caída del sistema por agotamiento de recursos	x			1	80			1	80			1	80			1	50			1	80		
[A.7] Uso no previsto	x	x	x	1	50	50	50	1	50	50	50	10	50	50	50	0,01	50	50	50	0,01	50	80	50
[A.11] Acceso no autorizado			x	1			50	1			50	1			50	0,01			100	0,01			80
[A.24] Denegación de servicio	x			1	80			1	80			1	80			0,1	80			0,1	80		

				[servi_wifi]				[email]				[servi_mante]				[servi_file]				[servi_labs]			
				[F]	[Deg]			[F]	[Deg]			[F]	[Deg]			[F]	[Deg]			[F]	[Deg]		
AMENAZAS	**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**
[E.1] Errores de los usuarios	x	x	x	1	50	30	30	1	50	50	50	1	50	50	50	1	80	80	80	1	50	50	50
[E.2] Errores del administrador	x	x	x	1	80	80	80	1	80	50	50	1	80	50	50	1	80	80	80	1	80	50	50
[E.24] Caída del sistema por agotamiento de recursos	x			10	80			1	100			1	80			1	80			1	80		
[A.7] Uso no previsto	x	x	x	1	50	50	50	1	50	50	50	10	50	50	50	1	50	50	50	1	50	50	50
[A.11] Acceso no autorizado			x	0,1			50	1			50	1			50					1			50
[A.24] Denegación de servicio	x			10	80			1	100			1	80			1	80			1	80		

Tabla 14 - Valoración de amenazas por activos de SOFTWARE. Fuente: El autor.

ACTIVO: **SOFTWARE**																			
				[sis_crm]				**[sis_controlac]**				**[sis_creacion]**				**[sis_reunion]**			
				[F]	**[Deg]**			**[F]**	**[Deg]**			**[F]**	**[Deg]**			**[F]**	**[Deg]**		
AMENAZAS	**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**
[I.5] Avería de origen físico o lógico	x			1	100			1	100			1	100			1	100		
[E.1] Errores de los usuarios	x	x	x	0,1	5	30	5	0,1	5	30	5	0,1	5	5	5	0,1	30	80	5
[E.2] Errores del administrador	x	x	x	0,1	30	80	30	0,1	30	80	30	0,1	80	80	50	0,1	50	80	5
[E.20] Vulnerabilidades de los programas (software)	x	x	x	1	30	30	5	1	50	50	5	1	80	80	30	1	50	50	5
[E.21] Errores de mantenimiento / actualización de programas	x	x		0,1	80	50		0,1	80	50		0,1	50	50		0,1	80	50	
[A.5] Suplantación de la identidad del usuario	x	x	x	0,1	5	50	30	0,1	5	50	30	0,1	5	80	50	0,1	5	30	30
[A.6] Abuso de privilegios de acceso	x	x	x	0,01	5	50	30	0,01	5	50	30	0,01	5	5	5	0,01	30	50	30
[A.7] Uso no previsto	x	x	x																
[A.8] Difusión de software dañino	x	x	x																
[A.9] [Re-]encaminamiento de mensajes			x	0,01			30					0,01			30				
[A.11] Acceso no autorizado	x			0,1	5			0,1	5			0,1	5			0,1	5		
[A.15] Modificación deliberada de la información		x		0,1		80		0,1		80		0,1		5		0,1		80	
[A.18] Destrucción de información	x			0,1	100			0,1	5			0,1	100			0,1	100		
[A.19] Divulgación de información			x	0,1			5	0,1			5	0,1			5	0,1			5
[A.22] Manipulación de programas	x	x	x	0,1	80	80	50	0,1	80	80	50	0,1	80	80	80	0,1	80	80	50

				[sis_reservar]				[sis_ara]				[sis_satt]				[pkt]			
				[F]	[Deg]			[F]	[Deg]			[F]	[Deg]			[F]	[Deg]		
AMENAZAS	**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**
[I.5] Avería de origen físico o lógico	x			1	100			1	100			1	100			1	100		
[E.1] Errores de los usuarios	x	x	x	0,1	5	50	5	0,1	5	50	5	0,1	5	50	5	1	30	50	30
[E.2] Errores del administrador	x	x	x	0,1	5	50	5	0,1	30	80	5	0,1	5	50	5	0,1	50	80	80
[E.20] Vulnerabilidades de los programas (software)	x	x	x	1	50	50	5	1	50	50	5	0,1	50	50	5	1	50	50	5
[E.21] Errores de mantenimiento / actualización de programas	x	x		0,1	50	50		0,1	80	50	5	0,1	50	50		0,1	30	30	
[A.5] Suplantación de la identidad del usuario	x	x	x	0,1	5	30	30	0,1	5	30	50	0,1	5	30	30	0,1	30	30	80
[A.6] Abuso de privilegios de acceso	x	x	x	0,01	5	50	30	0,01	5	80	30	0,01	5	50	30	0,01	5	50	30
[A.7] Uso no previsto	x	x	x													0,01	80	80	80
[A.8] Difusión de software dañino	x	x	x													1	80	80	80
[A.9] [Re-]encaminamiento de mensajes			x					0,01			50	0,1			50				
[A.11] Acceso no autorizado	x			0,1	5			0,1	5			0,1	5			0,1	80		
[A.15] Modificación deliberada de la información		x		0,1		80		0,1		80		0,1		80		0,1		80	
[A.18] Destrucción de información	x			0,1	100			0,1	100			0,1	100			0,1	80		
[A.19] Divulgación de información			x	0,1			5	0,1			30	0,1			5	0,1			50
[A.22] Manipulación de programas	x	x	x	0,1	80	80	50	0,1	80	80	50	0,1	80	80	50	0,1	80	80	50

				[sis_controlpc]				[av]				[sis_portal]			
				[F]	[Deg]			[F]	[Deg]			[F]	[Deg]		
AMENAZAS	**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**
[I.5] Avería de origen físico o lógico	x			1	100			1	100			1	100		
[E.1] Errores de los usuarios	x	x	x	0,1	5	5	5	0,1	5	30	5	0,01	5	5	5
[E.2] Errores del administrador	x	x	x	0,1	80	50	5	0,1	80	80	80	0,1	50	80	50
[E.20] Vulnerabilidades de los programas (software)	x	x	x	1	50	50	5	1	50	50	50	1	50	80	50
[E.21] Errores de mantenimiento / actualización de programas	x	x		0,1	50	50		0,1	80	50		0,1	80	50	
[A.5] Suplantación de la identidad del usuario	x	x	x	0,1	5	5	5	0,1	5	50	30	0,1	5	30	50
[A.6] Abuso de privilegios de acceso	x	x	x	0,01	5	30	30	0,01	5	50	30	0,01	5	50	50
[A.7] Uso no previsto	x	x	x					1	80	80	80	0,1	80	80	80
[A.8] Difusión de software dañino	x	x	x					1	80	80	80	1	80	80	80
[A.9] [Re-]encaminamiento de mensajes			x												
[A.11] Acceso no autorizado	x			0,1	5			0,1	5			0,1	50		
[A.15] Modificación deliberada de la información		x		0,1		80		0,1		50		0,1		80	
[A.18] Destrucción de información	x			0,1	100			0,1	100			0,1	100		
[A.19] Divulgación de información			x	0,1			5	0,1			5	0,1			80
[A.22] Manipulación de programas	x	x	x	0,1	80	80	50	0,1	80	80	50	0,1	80	80	30

Tabla 15 - Valoración de amenazas por activos de HARDWARE. Fuente: El autor.

ACTIVO**: HARDWARE**																								
				[print]				**[scan]**				**[cam]**				**[mobile]**				**[srv_strmg]**				
				[F]	**[Deg]**			**[F]**	**[Deg]**			**[F]**	**[Deg]**			**[F]**	**[Deg]**			**[F]**	**[Deg]**		
AMENAZAS	**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**
[N.1]Fuego	x			0,01	100			0,01	100			0,01	100			0,01	80			0,01	100		
[N.2] Daños por agua	x			0,01	80			0,01	80			0,01	80			0,01	80			0,01	80		
[I.1] Fuego	x			0,01	100			0,01	100			0,01	100			0,01	80			0,01	100		
[I.2] Daños por agua	x			0,01	80			0,01	80			0,01	80			1	80			0,01	80		
[I.*] Desastres industriales	x			0,1	80			0,1	80			0,1	80			0,1	80			0,1	80		
[I.3] Contaminación mecánica	x			1	50			1	50			1	50			10	50			1	50		
[I.4] Contaminación electromagnética	x			0,1	30			0,1	30			0,1	30			0,1	30			0,1	30		
[I.5] Avería de origen físico o lógico	x			1	80			1	80			1	80			1	80			1	80		
[I.6] Corte de suministro eléctrico	x			1	80			1	80			1	80			0,1	50			0,1	80		
[I.7] Condiciones inadecuadas de temperatura	x			0,1	50			0,1	50			0,1	50			0,1	50			0,1	50		
[E.2] Errores del administrador	x	x	x	0,1	30	50	5	0,1	30	50	5	0,1	30	50	5	0,1	30	50	5	0,1	30	50	30
[E.23] Errores de mantenimiento / actualización de eq.	x			0,1	30			0,1	30			0,1	30			0,1	30			0,1	50		
[E.25] Pérdida de equipos	x		x	0,01	80		30	0,01	80		5	0,01	80		5	0,1	80		50	0,01	80		50
[A.6] Abuso de privilegios de acceso	x	x	x	0,01	50	50	30	0,01	50	50	5	0,01	50	50	30	0,1	50	50	30	0,1	50	50	30
[A.7] Uso no previsto	x	x	x	0,1	30	50	30	0,1	30	50	5	0,1	30	50	50	0,1	30	50	50	0,1	50	50	30
[A.11] Acceso no autorizado		x	x	0,1		50	5	0,1		50	5	0,1		50	80	0,1		50	50	0,1		50	30
[A.23] Manipulación de los equipos	x	x	x	0,1	50	80	5	0,1	50	50	5	0,1	50	50	5	0,1	80	50	50	0,1	80	50	30
[A.24] Denegación de servicio	x																			1	80		
[A.25] Robo	x		x	0,1	100		50	0,1	100		5	0,1	100		5	0,1	100		5	0,01	100		50
[A.26] Ataque destructivo	x			0,1	80			0,1	80			0,1	80			0,1	80			0,1	80		

				[wap]				[pc]				[srv_files]				[srv_control]			
				[F]	[Deg]			[F]	[Deg]			[F]	[Deg]			[F]	[Deg]		
AMENAZAS	**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**
[N.1]Fuego	x			0,01	100			0,01	100			0,01	100			0,01	100		
[N.2] Daños por agua	x			0,01	80			0,01	80			0,01	80			0,01	80		
[I.1] Fuego	x			0,01	100			0,01	100			0,01	100			0,01	100		
[I.2] Daños por agua	x			0,1	80			1	80			0,01	80			0,01	80		
[I.*] Desastres industriales	x			0,1	80			0,1	80			0,1	80			0,1	80		
[I.3] Contaminación mecánica	x			1	50			10	50			1	50			1	50		
[I.4] Contaminación electromagnética	x			1	30			0,1	30			0,1	30			0,1	30		
[I.5] Avería de origen físico o lógico	x			1	80			1	80			1	80			1	80		
[I.6] Corte de suministro eléctrico	x			0,1	80			0,1	80			0,1	80			0,1	80		
[I.7] Condiciones inadecuadas de temperatura	x			1	50			0,1	50			0,1	50			0,1	50		
[E.2] Errores del administrador	x	x	x	0,1	80	50	5	0,1	50	50	50	0,1	50	50	50	0,1	30	50	50
[E.23] Errores de mantenimiento / actualización de eq.	x			0,1	50			0,1	80			0,1	50			0,1	50		
[E.25] Pérdida de equipos	x		x	0,1	80		50	0,1	80		80	0,01	80		50	0,01	80		50
[A.6] Abuso de privilegios de acceso	x	x	x	0,1	50	50	80	0,1	50	50	50	0,1	50	50	50	0,1	50	50	50
[A.7] Uso no previsto	x	x	x	0,1	50	50	50	0,1	30	50	50	0,1	50	50	50	0,1	50	50	30
[A.11] Acceso no autorizado		x	x	0,1		50	50	0,1		50	80	0,1		50	50	0,1		50	30
[A.23] Manipulación de los equipos	x	x	x	0,1	80	50	50	0,1	80	50	50	0,1	80	50	30	0,1	80	50	30
[A.24] Denegación de servicio	x			1	80							1	80			1	80		
[A.25] Robo	x		x	0,1	100		5	0,1	100		50	0,01	100		50	0,01	100		50
[A.26] Ataque destructivo	x			0,1	80			0,1	80			0,1	80			0,1	80		

				[srv_dhcp]				[srv_radius]				[switch]				[router]			
				[F]	[Deg]			[F]	[Deg]			[F]	[Deg]			[F]	[Deg]		
AMENAZAS	**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**
[N.1]Fuego	x			0,01	100			0,01	100			0,01	100			0,01	100		
[N.2] Daños por agua	x			0,01	80			0,01	80			0,01	80			0,01	80		
[I.1] Fuego	x			0,01	100			0,01	100			0,01	100			0,01	100		
[I.2] Daños por agua	x			0,01	80			0,01	80			0,01	80			0,01	80		
[I.*] Desastres industriales	x			0,1	80			0,1	80			0,1	80			0,1	80		
[I.3] Contaminación mecánica	x			1	50			1	50			1	50			1	50		
[I.4] Contaminación electro.	x			0,1	30			0,1	30			0,1	30			0,1	30		
[I.5] Avería de origen físico o lógico	x			1	80			1	80			1	80			1	80		
[I.6] Corte de suministro eléctrico	x			0,1	80			0,1	80			0,1	80			0,1	80		
[I.7] Cond. inadecuadas de temp.	x			0,1	50			0,1	50			0,1	50			0,1	50		
[E.2] Errores del administrador	x	x	x	0,1	50	50	50	0,1	30	50	30	0,1	30	50	30	0,1	30	50	30
[E.23] Errores de mant. / act. de eq.	x			0,1	50			0,1	50			0,1	50			0,1	50		
[E.25] Pérdida de equipos	x		x	0,01	80		50	0,01	80		50	0,01	80		50	0,01	80		50
[A.6] Abuso de privilegios de acceso	x	x	x	0,1	50	50	30	0,1	50	50	50	0,1	50	50	30	0,1	50	50	30
[A.7] Uso no previsto	x	x	x	0,1	50	50	30	0,1	50	50	30	0,1	50	50	30	0,1	50	50	30
[A.11] Acceso no autorizado		x	x	0,1		50	30	0,1		50	30	0,1		50	30	0,1		50	30
[A.23] Manipulación de los equipos	x	x	x	0,1	80	50	30	0,1	80	50	30	0,1	80	50	30	0,1	80	50	30
[A.24] Denegación de servicio	x			1	80			1	80			1	80			1	80		
[A.25] Robo	x		x	0,01	100		50	0,01	100		50	0,01	100		50	0,01	100		50
[A.26] Ataque destructivo	x			0,1	80			0,1	80			0,1	80			0,1	80		

				[srv_mail]				[srv_db]				[srv_web]				[srv_ant]			
				[F]	[Deg]			[F]	[Deg]			[F]	[Deg]			[F]	[Deg]		
AMENAZAS	**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**
[N.1]Fuego	x			0,01	100			0,01	100			0,01	100			0,01	100		
[N.2] Daños por agua	x			0,01	80			0,01	80			0,01	80			0,01	80		
[I.1] Fuego	x			0,01	100			0,01	100			0,01	100			0,01	100		
[I.2] Daños por agua	x			0,01	80			0,01	80			0,01	80			0,01	80		
[I.*] Desastres industriales	x			0,1	80			0,1	80			0,1	80			0,1	80		
[I.3] Contaminación mecánica	x			1	50			1	50			1	50			1	50		
[I.4] Contaminación electro.	x			0,1	30			0,1	30			0,1	30			0,1	30		
[I.5] Avería de origen físico o lógico	x			1	80			1	80			1	80			1	80		
[I.6] Corte de suministro eléctrico	x			0,1	80			0,1	80			0,1	80			0,1	80		
[I.7] Cond. inadecuadas de temp.	x			0,1	50			0,1	50			0,1	50			0,1	50		
[E.2] Errores del administrador	x	x	x	0,1	50	50	50	0,1	50	50	50	0,1	50	50	30	0,1	50	50	50
[E.23] Errores de mant. / act. de eq.	x			0,1	50			0,1	50			0,1	50			0,1	50		
[E.25] Pérdida de equipos	x		x	0,01	80		50	0,01	80		50	0,01	80		50	0,01	80		50
[A.6] Abuso de privilegios de acceso	x	x	x	0,1	50	50	50	0,1	50	50	50	0,1	50	50	50	0,1	50	50	30
[A.7] Uso no previsto	x	x	x	0,1	50	50	30	0,1	50	50	30	0,1	50	50	30	0,1	50	50	30
[A.11] Acceso no autorizado		x	x	0,1		50	30	0,1		50	30	0,1		50	30	0,1		50	30
[A.23] Manipulación de los equipos	x	x	x	0,1	80	50	30	0,1	80	50	30	0,1	80	50	30	0,1	80	50	30
[A.24] Denegación de servicio	x			1	80			1	80			1	80			1	80		
[A.25] Robo	x		x	0,01	100		50	0,01	100		50	0,01	100		50	0,01	100		50
[A.26] Ataque destructivo	x			0,1	80			0,1	80			0,1	80			0,1	80		

Tabla 16 - Valoración de amenazas por activos de SOPORTES DE INFORMACIÓN. Fuente: El autor.

ACTIVO**: SOPORTES DE INFORMACIÓN**

				[disk]				[san]				[tape]			
				[F]	[Deg]			[F]	[Deg]			[F]	[Deg]		
AMENAZAS	**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**
[N.1]Fuego	x			0,01	100			0,01	100			0,01	100		
[N.2] Daños por agua	x			0,01	80			0,01	80			0,01	80		
[I.1] Fuego	x			0,01	100			0,01	100			0,01	100		
[I.2] Daños por agua	x			0,1	80			0,1	80			0,1	80		
[I.*] Desastres industriales	x			0,1	80			0,1	80			0,1	80		
[I.3] Contaminación mecánica	x			0,1	50			0,1	50			0,1	50		
[I.4] Contaminación electromagnética	x			0,1	30			0,1	30			0,1	30		
[I.5] Avería de origen físico o lógico	x			1	80			1	80			1	80		
[I.6] Corte de suministro eléctrico	x			0,1	80			1	80			0,1	80		
[I.7] Condiciones inadecuadas de temperatura o humedad	x			0,1	50			0,1	50			0,1	50		
[I.10] Degradación de los soportes de almacenamiento de información	x			1	80			1	80			1	80		
[E.2] Errores del administrador	x	x	x	0,1	30	50	50	0,1	30	50	50	0,1	30	50	50
[E.19] Fugas de información			x	0,1			80	0,1			80	0,1			80
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	x			0,1	80			0,1	80			0,1	80		
[E.25] Pérdida de equipos	x		x	0,1	80		50	0,1	80		50	0,1	80		50
[A.7] Uso no previsto	x	x	x	0,1	30	50	50	0,1	30	50	50	0,1	30	50	50
[A.11] Acceso no autorizado		x	x	1		50	50	1		50	50	1		50	50
[A.15] Modificación deliberada de la información		x		0,1		50		0,1		50		0,1		50	
[A.18] Destrucción de información	x			1	80			1	80			1	80		
[A.19] Divulgación de información			x	0,1			50	0,1			50	0,1			50
[A.25] Robo	x		x	0,1	100		80	0,1	100		80	0,1	100		80
[A.26] Ataque destructivo	x			0,1	80			0,1	80			0,1	80		

Tabla 17 - Valoración de amenazas por activos de EQUIPAMIENTO AUXILIAR. Fuente: El autor.

ACTIVO**: EQUIPAMIENTO AUXILIAR**

				[furniture]				[tools]				[tools_network]				[ss]				[ups]				[ac]			
					[Deg]				[Deg]				[Deg]				[Deg]				[Deg]				[Deg]		
AMENAZAS	**[D]**	**[I]**	**[C]**	**[F]**	**[D]**	**[I]**	**[C]**	**[F]**	**[D]**	**[I]**	**[C]**	**[F]**	**[D]**	**[I]**	**[C]**	**[F]**	**[D]**	**[I]**	**[C]**	**[F]**	**[D]**	**[I]**	**[C]**	**[F]**	**[D]**	**[I]**	**[C]**
[N.1]Fuego	x			0,01	80			0,01	80			0,01	80			0,01	100			0,01	100			0,01	100		
[N.2] Daños por agua	x			0,01	5			0,01	5			0,01	30			0,01	30			0,01	80			0,01	80		
[I.1] Fuego	x			0,01	80			0,01	80			0,01	80			0,01	100			0,01	100			0,01	100		
[I.2] Daños por agua	x			0,1	5			0,1	5			0,1	30			0,1	30			0,1	80			0,1	80		
[I.*] Desastres industriales	x			0,1	80			0,1	80			0,1	80			0,1	80			0,1	80			0,1	80		
[I.3] Contaminación mecánica	x			0,1	5			0,1	5			0,1	30			0,1	30			0,1	30			0,1	30		
[I.4] Contaminación electromagnética	x			0,1	5			0,1	5			0,1	5			0,1	30			0,1	50			0,1	50		
[I.5] Avería de origen físico o lógico	x			1	30			1	30			1	50			1	50			1	80			1	80		
[I.6] Corte de suministro eléctrico	x															0,1	80			0,1	50			0,1	80		
[I.7] Condiciones inadecuadas de temperatura	x			0,1	5			0,1	5			0,1	5			0,1	30			0,1	30			0,1	30		
[E.23] Errores de manten. / actualización de Eq.	x			0,1	5			0,1	5			0,1	5			0,1	50			0,1	50			0,1	50		
[E.25] Pérdida de equipos	x		x	0,1	50		5	0,1	50		5	0,1	50		5	0,1	80		5	0,1	50		5	0,1	80		5
[A.7] Uso no previsto	x	x	x	0,1	5	5	5	0,1	5	5	5	0,1	5	5	5	0,1	30	5	5	0,1	5	5	5	0,1	5	5	5
[A.25] Robo	x		x	0,01	100		5	0,1	100		5	0,1	100		5	0,01	100		5	0,01	100		5	0,01	100		5
[A.26] Ataque destructivo	x			0,1	80			0,1	80			0,1	80			0,1	80			0,1	80			0,1	80		

Tabla 18 - Valoración de amenazas por activos de INSTALACIONES. Fuente: El autor.

ACTIVO**: INSTALACIONES**											
				[building]				**[local]**			
				[F]	**[Deg]**			**[F]**	**[Deg]**		
AMENAZAS	**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**
[N.1]Fuego	x			0,01	80			0,01	80		
[N.2] Daños por agua	x			0,01	30			0,01	30		
[I.1] Fuego	x			0,01	80			0,01	80		
[I.2] Daños por agua	x			0,1	30			0,1	30		
[I.*] Desastres industriales	x			0,1	80			0,1	80		
[A.7] Uso no previsto	x	x	x	0,1	5	50	50	0,1	5	50	50
[A.11] Acceso no autorizado		x	x	0,1		80	50	0,1		80	50
[A.26] Ataque destructivo	x			0,1	80		50	0,1	80		50

Tabla 19 - Valoración de amenazas por activos de REDES DE COMUNICACIONES. Fuente: El autor.

ACTIVO: **REDES DE COMUNICACIONES**											
				[wifi]				**[LAN]**			
				[F]	**[Deg]**			**[F]**	**[Deg]**		
AMENAZAS	**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**
[A.5] Suplantación de la identidad del usuario	x	x	x	0,1	30	50	50	0,1	80	80	50
[A.6] Abuso de privilegios de acceso	x	x	x	0,1	50	80	50	0,1	80	80	50
[A.10] Alteración de secuencia		x		0,1		80		0,1		80	
[A.11] Acceso no autorizado		x	x	0,1		50	50	0,1		80	50
[A.12] Análisis de tráfico			x	1			80	1			80
[A.14] Interceptación de información (escucha)			x	1			80	1			80
[A.24] Denegación de servicio	x			1	80			1	80		

Tabla 20 - Valoración de amenazas por activos PERSONAL. Fuente: El autor.

ACTIVO**: PERSONAL**																								
				[adm]				**[com]**				**[ast]**				**[des]**				**[wm]**				
				[F]	**[Deg]**			**[F]**	**[Deg]**			**[F]**	**[Deg]**			**[F]**	**[Deg]**			**[F]**	**[Deg]**		
AMENAZAS	**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**		**[D]**	**[I]**	**[C]**
[E.7]Deficiencias en la organización	x			0,1	80			0,1	80			0,1	80			0,1	80			0,1	80		
[E.19] Fugas de información			x	0,1			80	0,1			80	0,1			80	0,1			80	0,1			80
[E.28] Indisponibilidad del personal	x			0,1	80			0,1	80			0,1	80			0,1	80			0,1	80		
[A.28] Indisponibilidad del personal	x			0,1	80			0,1	80			0,1	80			0,1	80			0,1	80		
[A.29] Extorsión	x	x	x	0,1	80	80	80	0,1	80	80	80	0,1	80	80	80	0,1	80	80	80	0,1	80	80	80
[A.30] Ingeniería social (picaresca)	x	x	x	0,1	80	80	80	0,1	80	80	80	0,1	80	80	80	0,1	80	80	80	0,1	80	80	80

3.3.6 Estimación del impacto

En esta tarea se procede a estimar el impacto que producen las amenazas que puedan materializarse sobre un activo, para esto se hará uso de la Tabla 21 que muestra una escala cualitativa.

Tabla 21 - Estimación del impacto. Fuente: Magerit.

impacto		degradación		
		1%	10%	100%
activo	MA	**M**	**A**	**MA**
	A	B	**M**	**A**
	M	MB	B	**M**
	B	MB	MB	B
	MB	MB	MB	MB

Escalas: (**MA** - muy alto, **A** – alto, **M**- medio, **B**- bajo, **MB**- muy bajo)

3.3.7 Estimación del riesgo

El objetivo de esta tarea es estimar el riesgo en base al impacto y a la probabilidad por medio de una escala cualitativa según se muestra en la Tabla 22.

Tabla 22 - Estimación del Riesgo. Fuente: Magerit.

riesgo		probabilidad				
		MB	B	M	A	MA
impacto	MA	**A**	**MA**	**MA**	**MA**	**MA**
	A	**M**	**A**	**A**	**MA**	**MA**
	M	B	**M**	**M**	**A**	**A**
	B	MB	B	B	**M**	**M**
	MB	MB	MB	MB	B	B

Escalas:

- **impacto (MA:** muy alto, **A:** alto, **M:** medio, **B:** bajo, **MB:** muy bajo)
- **probabilidad (MA:** prácticamente seguro, **A:** probable, **M:** posible **B:** poco probable, **MB:** muy raro)
- **riesgo (MA:** crítico, **A:** importante, **M:** apreciable, **B:** bajo, **MB:** despreciable)

A continuación se muestra desde la Tabla 23 a la Tabla 31 el impacto y el riesgo de cada uno de los tipos de activos:

Tabla 23 - Estimación de impacto y riesgo del activo DATOS. Fuente: El autor.

ESTIMACIÓN DE IMPACTO Y RIESGO EN ACTIVO**: DATOS**

	[bd_crm]					[bd_reservar]					[bd_controlac]					[bd_reunion]					[bd_ara]				
AMENAZAS	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**
[E.1] Errores de los usuarios	M	M	MB	M	MB	M	M	MB	A	B	A	A	M	M	M	MA	A	A	M	A	A	M	B	A	M
[E.2] Errores del administrador	A	M	B	B	B	A	M	B	B	B	A	A	M	B	M	A	A	M	B	M	A	M	B	B	B
[E.3] Errores de monitorización (log)																									
[E.4] Errores de configuración																									
[E.15] Alteración accidental de la información	M	M	MB	B	MB	M	M	MB	B	MB	MA	A	A	B	A	A	A	M	B	M	MA	M	M	B	M
[E.18] Destrucción de información	MA	M	M	B	M	MA	M	M	B	M	MA	A	A	B	A	MA	A	A	B	A	MA	M	M	B	M
[E.19] Fugas de información	MB	M	MB	B		MB	M	MB	B	MB	MB	A	MB	B	MB	M	A	B	B	B	MB	M	MB	B	MB
[A.3] Manipulación de los registros de actividad (log)																									
[A.4] Manipulación de la configuración																									
[A.5] Suplantación de la identidad del usuario	A	M	B	B	B	A	M	B	B	B	A	A	M	B	M	A	A	M	B	M	A	M	B	B	B
[A.6] Abuso de privilegios de acceso	M	M	MB	B	MB	A	M	B	B	B	M	A	B	B	B	A	A	M	B	M	M	M	MB	B	MB
[A.11] Acceso no autorizado	MA	M	M	B	M	MA	M	M	B	M	MA	A	A	B	A	A	A	M	B	M	A	M	B	B	B
[A.13] Repudio																									
[A.15] Modificación deliberada de la información	A	M	B	B	B	M	M	MB	B	MB	A	A	M	B	M	A	A	M	B	M	A	M	B	B	B
[A.18] Destrucción de información	MA	M	M	B	M	MA	M	M	B	M	MA	A	A	B	A	MA	A	A	B	A	MA	M	M	B	M
[A.19] Divulgación de información	MB	M	MB	B	MB	MB	M	MB	B	MB	MB	A	MB	B	MB	B	A	MB	B	MB	MB	M	MB	B	MB

AMENAZAS	[bd_satt]					[backup]					[source]					[files]					[bd_controlpc]				
	[deg]	[val]	[imp]	[pro]	[rie]	[deg]	[val]	[imp]	[pro]	[rie]	[deg]	[val]	[imp]	[pro]	[rie]	[deg]	[val]	[imp]	[pro]	[rie]	[deg]	[val]	[imp]	[pro]	[rie]
[E.1] Errores de los usuarios	B	A	MB	M	MB																				
[E.2] Errores del administrador	A	A	M	B	M	A	A	M	B	M	A	A	M	B	M	M	A	B	M	B	A	A	M	B	M
[E.3] Errores de monitorización (log)																									
[E.4] Errores de configuración																									
[E.15] Alteración accidental de la información	M	A	B	B	B	A	A	M	B	M	A	A	M	B	M	A	A	M	B	M	M	A	B	B	B
[E.18] Destrucción de información	MA	A	A	B	A	MA	A	A	MB	M	MA	A	A	B	A	MA	A	A	B	A	MA	A	A	MB	M
[E.19] Fugas de información	B	A	MB	B	MB	A	A	M	MB	B	A	A	M	B	M	A	A	M	B	M	MB	A	MB	MB	MB
[A.3] Manipulación de los registros de actividad (log)																									
[A.4] Manipulación de la configuración																									
[A.5] Suplantación de la identidad del usuario	A	A	M	B	M	A	A	M	B	M	A	A	M	B	M	A	A	M	MB	B	A	A	M	B	M
[A.6] Abuso de privilegios de acceso	A	A	M	B	M	M	A	B	B	B	M	A	B	B	B	A	A	M	MB	B	M	A	B	B	B
[A.11] Acceso no autorizado	A	A	M	B	M	A	A	M	B	M	MA	A	A	B	A	A	A	M	MB	B	A	A	M	B	M
[A.13] Repudio																									
[A.15] Modificación deliberada de la información	A	A	M	B	M	MA	A	A	B	A	MA	A	A	B	A	MA	A	A	B	A	A	A	M	B	M
[A.18] Destrucción de información	MA	A	A	B	A	MA	A	A	B	A	MA	A	A	B	A	MA	A	A	B	A	MA	A	A	B	A
[A.19] Divulgación de información	B	A	MB	B	MB	A	A	M	B	M	A	A	M	B	M	A	A	M	B	M	MB	A	MB	B	MB

	[conf]					[log]					[bd_ldap]					[bd_sitioFiec]				
AMENAZAS	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**
[E.1] Errores de los usuarios																				
[E.2] Errores del administrador	A	A	M	B	M	A	A	M	B	M	A	A	M	B	M	A	A	M	B	M
[E.3] Errores de monitorización (log)						A	A	M	B	M										
[E.4] Errores de configuración	A	A	M	B	M															
[E.15] Alteración accidental de la información	A	A	M	B	M	A	A	M	B	M	MA	A	A	B	A	MA	A	A	B	A
[E.18] Destrucción de información	MA	A	A	B	A	MA	A	A	B	A	MA	A	A	B	A	MA	A	A	B	A
[E.19] Fugas de información	MA	A	A	B	A	A	A	M	MB	B	M	A	B	B	B	M	A	B	B	B
[A.3] Manipulación de los registros de actividad (log)						A	A	M	B	M										
[A.4] Manipulación de la configuración	A	A	M	B	M															
[A.5] Suplantación de la identidad del usuario	A	A	M	MB	B	A	A	M	MB	B	A	A	M	MB	B	A	A	M	MB	B
[A.6] Abuso de privilegios de acceso	M	A	B	MB	MB	A	A	M	MB	B	A	A	M	MB	B	A	A	M	MB	B
[A.11] Acceso no autorizado	A	A	M	MB	B	A	A	M	B	M	A	A	M	MB	B	A	A	M	MB	B
[A.13] Repudio						A	A	M	B	M										
[A.15] Modificación deliberada de la información	MA	A	A	MB	M	A	A	M	B	M	MA	A	A	MB	M	MA	A	A	MB	M
[A.18] Destrucción de información	MA	A	A	B	A	MA	A	A	B	A	MA	A	A	B	A	MA	A	A	B	A
[A.19] Divulgación de información	MA	A	A	B	A	A	A	M	MB	B	A	A	M	MB	B	A	A	M	MB	B

Tabla 24 - Estimación de impacto y riesgo del activo DATOS. Fuente: El autor.

ESTIMACIÓN DE IMPACTO Y RIESGO EN ACTIVO**: SERVICIOS**

	[servi_a/v]					[servi_equi]					[servi_support]					[servi_dev]					[servi_acco]				
AMENAZAS	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**
[E.1] Errores de los usuarios	M	M	MB	M	MB	M	M	MB	M	MB	M	M	MB	M	MB						MB	M	MB	M	MB
[E.2] Errores del administrador	A	M	B	M	B	A	M	B	M	B	A	M	B	M	B	A	M	B	M	B	A	M	B	M	B
[E.24] Caída del sistema por agotamiento de recursos	A	M	B	M	B	A	M	B	M	B	A	M	B	M	B	M	M	MB	M	MB	A	M	B	M	B
[A.7] Uso no previsto	M	M	MB	M	MB	M	M	MB	M	MB	M	M	MB	A	B	M	M	MB	MB	MB	A	M	B	MB	MB
[A.11] Acceso no autorizado	M	M	MB	M	MB	M	M	MB	M	MB	M	M	MB	M	MB	MA	M	M	MB	B	A	M	B	MB	MB
[A.24] Denegación de servicio	A	M	B	M	B	A	M	B	M	B	A	M	B	M	B	A	M	B	B	B	A	M	B	B	B

	[servi_wifi]					[email]					[servi_mante]					[servi_file]					[servi_labs]				
AMENAZAS	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**
[E.1] Errores de los usuarios	M	M	MB	M	MB	M	M	MB	M	MB	M	M	MB	M	MB	A	M	B	M	B	M	M	MB	M	MB
[E.2] Errores del administrador	A	M	B	M	B	A	M	B	M	B	A	M	B	M	B	A	M	B	M	B	A	M	B	M	B
[E.24] Caída del sistema por agotamiento de recursos	A	M	B	A	M	A	M	B	M	M	A	M	B	M	B	A	M	B	M	B	A	M	B	M	B
[A.7] Uso no previsto	M	M	MB	M	MB	M	M	MB	M	MB	M	M	MB	A	B	M	M	MB	M	MB	M	M	MB	M	MB
[A.11] Acceso no autorizado	M	M	MB	B	MB	M	M	MB	M	MB	M	M	MB	M	MB						M	M	MB	M	MB
[A.24] Denegación de servicio	A	M	B	A	M	A	M	B	M	M	A	M	B	M	B	A	M	B	M	B	A	M	B	M	B

Tabla 25 - Estimación de impacto y riesgo del activo SOFTWARE. Fuente: El autor.

ESTIMACIÓN DE IMPACTO Y RIESGO EN ACTIVO**: SOFTWARE**

	[sis_crm]					[sis_controlac]					[sis_creacion]					[sis_reunion]				
AMENAZAS	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**
[I.5] Avería de origen físico o lógico	MA	M	M	M	M	MA	M	M	M	M	MA	M	M	M	M	MA	M	M	M	M
[E.1] Errores de los usuarios	B	M	MB	B	MB	B	M	MB	B	MB	MB	M	MB	B	MB	A	M	B	B	B
[E.2] Errores del administrador	A	M	B	B	B	A	M	B	B	B	A	M	B	B	B	A	M	B	B	B
[E.20] Vulnerabilidades de los programas (software)	B	M	MB	M	MB	M	M	MB	M	MB	A	M	B	M	B	M	M	MB	M	MB
[E.21] Errores de mantenimiento / actual. de progs.	A	M	B	B	B	A	M	B	B	B	M	M	MB	B	MB	A	M	B	B	B
[A.5] Suplantación de la identidad del usuario	M	M	MB	B	MB	M	M	MB	B	MB	A	M	B	B	B	B	M	MB	B	MB
[A.6] Abuso de privilegios de acceso	M	M	MB	MB	MB	M	M	MB	MB	MB	MB	M	MB	MB	MB	M	M	MB	MB	MB
[A.7] Uso no previsto																				
[A.8] Difusión de software dañino																				
[A.9] [Re-]encaminamiento de mensajes	B	M	MB	MB	MB						B	M	MB	MB	MB					
[A.11] Acceso no autorizado	MB	M	MB	B	MB	MB	M	MB	B	MB	MB	M	MB	B	MB	MB	M	MB	B	MB
[A.15] Modificación deliberada de la información	A	M	B	B	B	A	M	B	B	B	MB	M	MB	B	MB	A	M	B	B	B
[A.18] Destrucción de información	MA	M	M	B	M	MA	M	M	B	M	MA	M	M	B	M	MA	M	M	B	M
[A.19] Divulgación de información	MB	M	MB	B	MB	MB	M	MB	B	MB	MB	M	MB	B	MB	MB	M	MB	B	MB
[A.22] Manipulación de programas	A	M	B	B	B	A	M	B	B	B	A	M	B	B	B	A	M	B	B	B

AMENAZAS	[sis_reservar]					[sis_ara]					[sis_satt]					[pkt]				
	[deg]	[val]	[imp]	[pro]	[rie]	[deg]	[val]	[imp]	[pro]	[rie]	[deg]	[val]	[imp]	[pro]	[rie]	[deg]	[val]	[imp]	[pro]	[rie]
[I.5] Avería de origen físico o lógico	MA	M	M	M	M	MA	M	M	M	M	MA	M	M	M	M	MA	M	M	M	M
[E.1] Errores de los usuarios	M	M	MB	B	MB	M	M	MB	B	MB	M	M	MB	B	MB	M	M	MB	M	MB
[E.2] Errores del administrador	M	M	MB	B	MB	A	M	B	B	B	M	M	MB	B	MB	A	M	B	B	B
[E.20] Vulnerabilidades de los programas (software)	M	M	MB	M	MB	M	M	MB	M	MB	M	M	MB	B	MB	M	M	MB	M	MB
[E.21] Errores de mantenimiento / actual. de progs.	M	M	MB	B	MB	A	M	B	B	B	M	M	MB	B	MB	B	M	MB	B	MB
[A.5] Suplantación de la identidad del usuario	B	M	MB	B	MB	M	M	MB	B	MB	B	M	MB	B	MB	A	M	B	B	B
[A.6] Abuso de privilegios de acceso	M	M	MB	MB	MB	A	M	B	MB	MB	M	M	MB	MB	MB	M	M	MB	MB	MB
[A.7] Uso no previsto																A	M	B	MB	MB
[A.8] Difusión de software dañino																A	M	B	M	B
[A.9] [Re-]encaminamiento de mensajes						M	M	MB	MB	MB	M	M	MB	B	MB					
[A.11] Acceso no autorizado	MB	M	MB	B	MB	MB	M	MB	B	MB	MB	M	MB	B	MB	A	M	B	B	B
[A.15] Modificación deliberada de la información	A	M	B	B	B	A	M	B	B	B	A	M	B	B	B	A	M	B	B	B
[A.18] Destrucción de información	MA	M	M	B	M	MA	M	M	B	M	MA	M	M	B	M	MA	M	M	B	M
[A.19] Divulgación de información	MB	M	MB	B	MB	B	M	MB	B	MB	MB	M	MB	B	MB	M	M	MB	B	MB
[A.22] Manipulación de programas	A	M	B	B	B	A	M	B	B	B	A	M	B	B	B	A	M	B	B	B

AMENAZAS	[sis_controlpc]					[av]					[sis_portal]				
	[deg]	[val]	[imp]	[pro]	[rie]	[deg]	[val]	[imp]	[pro]	[rie]	[deg]	[val]	[imp]	[pro]	[rie]
[I.5] Avería de origen físico o lógico	MA	M	M	M	M	MA	M	M	M	M	MA	M	M	M	M
[E.1] Errores de los usuarios	MB	M	MB	B	MB	B	M	MB	B	MB	MB	M	MB	MB	MB
[E.2] Errores del administrador	A	M	B	B	B	A	M	B	B	B	A	M	B	B	B
[E.20] Vulnerabilidades de los programas (software)	M	M	MB	M	MB	M	M	MB	M	MB	A	M	B	M	B
[E.21] Errores de mantenimiento / actual. de progs.	M	M	MB	B	MB	A	M	B	B	B	A	M	B	B	B
[A.5] Suplantación de la identidad del usuario	MB	M	MB	B	MB	M	M	MB	B	MB	M	M	MB	B	MB
[A.6] Abuso de privilegios de acceso	B	M	MB	MB	MB	M	M	MB	MB	MB	M	M	MB	MB	MB
[A.7] Uso no previsto						A	M	B	M	B	A	M	B	B	B
[A.8] Difusión de software dañino						A	M	B	M	B	A	M	B	M	B
[A.9] [Re-]encaminamiento de mensajes															
[A.11] Acceso no autorizado	MB	M	MB	B	MB	MB	M	MB	B	MB	M	M	MB	B	MB
[A.15] Modificación deliberada de la información	A	M	B	B	B	M	M	MB	B	MB	A	M	B	B	B
[A.18] Destrucción de información	MA	M	M	B	M	MA	M	M	B	M	MA	M	M	B	M
[A.19] Divulgación de información	MB	M	MB	B	MB	MB	M	MB	B	MB	A	M	B	B	B
[A.22] Manipulación de programas	A	M	B	B	B	A	M	B	B	B	A	M	B	B	B

Tabla 26 - Estimación de impacto y riesgo del activo HARDWARE. Fuente: El autor.

ESTIMACIÓN DE IMPACTO Y RIESGO EN ACTIVO**: HARDWARE**

	[print]					[scan]					[cam]					[mobile]					[srv_strmg]				
AMENAZAS	[deg]	[val]	[imp]	[pro]	[rie]	[deg]	[val]	[imp]	[pro]	[rie]	[deg]	[val]	[imp]	[pro]	[rie]	[deg]	[val]	[imp]	[pro]	[rie]	[deg]	[val]	[imp]	[pro]	[rie]
[N.1]Fuego	MA	A	A	MB	M	MA	M	M	MB	B	MA	M	M	MB	B	A	A	M	MB	B	MA	A	A	MB	M
[N.2] Daños por agua	A	A	M	MB	B	A	M	B	MB	MB	A	M	B	MB	MB	A	A	M	MB	B	A	A	M	MB	B
[I.1] Fuego	MA	A	A	MB	M	MA	M	M	MB	B	MA	M	M	MB	B	A	A	M	MB	B	MA	A	A	MB	M
[I.2] Daños por agua	A	A	M	MB	B	A	M	B	MB	MB	A	M	B	MB	MB	A	A	M	M	M	A	A	M	MB	B
[I.*] Desastres industriales	A	A	M	B	M	A	M	B	B	B	A	M	B	B	B	A	A	M	B	M	A	A	M	B	M
[I.3] Contaminación mecánica	M	A	B	M	B	M	M	MB	M	MB	M	M	MB	M	MB	M	A	B	A	M	M	A	B	M	B
[I.4] Contaminación electromagnética	B	A	MB	B	MB	B	M	MB	B	MB	B	M	MB	B	MB	B	A	MB	B	MB	B	A	MB	B	MB
[I.5] Avería de origen físico o lógico	A	A	M	M	M	A	M	B	M	B	A	M	B	M	B	A	A	M	M	M	A	A	M	M	M
[I.6] Corte de suministro eléctrico	A	A	M	M	M	A	M	B	M	B	A	M	B	M	B	M	A	B	B	B	A	A	M	B	M
[I.7] Condiciones inadecuadas de temp.	M	A	B	B	B	M	M	MB	B	MB	M	M	MB	B	MB	M	A	B	B	B	M	A	B	B	B
[E.2] Errores del administrador	M	A	B	B	B	M	M	MB	B	MB	M	M	MB	B	MB	M	A	B	B	B	M	A	B	B	B
[E.23] Errores de mant, / actual. de eq.	B	A	MB	B	MB	B	M	MB	B	MB	B	M	MB	B	MB	B	A	MB	B	MB	M	A	B	B	B
[E.25] Pérdida de equipos	A	A	M	MB	B	A	M	B	MB	MB	A	M	B	MB	MB	A	A	M	B	M	A	A	M	MB	B
[A.6] Abuso de privilegios de acceso	M	A	B	MB	MB	M	M	MB	MB	MB	M	M	MB	MB	MB	M	A	B	B	B	M	A	B	B	B
[A.7] Uso no previsto	M	A	B	B	B	M	M	MB	B	MB	M	M	MB	B	MB	M	A	B	B	B	M	A	B	B	B
[A.11] Acceso no autorizado	M	A	B	B	B	M	M	MB	B	MB	A	M	B	B	B	M	A	B	B	B	M	A	B	B	B
[A.23] Manipulación de los equipos	A	A	M	B	M	M	M	MB	B	MB	M	M	MB	B	MB	A	A	M	B	M	A	A	M	B	M
[A.24] Denegación de servicio																					A	A	M	M	M
[A.25] Robo	MA	A	A	B	A	MA	M	M	B	M	MA	M	M	B	M	MA	A	A	B	A	MA	A	A	MB	M
[A.26] Ataque destructivo	A	A	M	B	M	A	M	B	B	B	A	M	B	B	B	A	A	M	B	M	A	A	M	B	M

	[srv_dhcp]					[srv_radius]					[switch]					[router]				
AMENAZAS	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**
[N.1]Fuego	MA	MA	MA	MB	A	MA	MA	MA	MB	A	MA	MA	MA	MB	A	MA	MA	MA	MB	A
[N.2] Daños por agua	A	MA	A	MB	M	A	MA	A	MB	M	A	MA	A	MB	M	A	MA	A	MB	M
[I.1] Fuego	MA	MA	MA	MB	A	MA	MA	MA	MB	A	MA	MA	MA	MB	A	MA	MA	MA	MB	A
[I.2] Daños por agua	A	MA	A	MB	M	A	MA	A	MB	M	A	MA	A	MB	M	A	MA	A	MB	M
[I.*] Desastres industriales	A	MA	A	B	A	A	MA	A	B	A	A	MA	A	B	A	A	MA	A	B	A
[I.3] Contaminación mecánica	M	MA	M	M	M	M	MA	M	M	M	M	MA	M	M	M	M	MA	M	M	M
[I.4] Contaminación electromagnética	B	MA	MB	B	MB	B	MA	MB	B	MB	B	MA	MB	B	MB	B	MA	MB	B	MB
[I.5] Avería de origen físico o lógico	A	MA	A	M	A	A	MA	A	M	A	A	MA	A	M	A	A	MA	A	M	A
[I.6] Corte de suministro eléctrico	A	MA	A	B	A	A	MA	A	B	A	A	MA	A	B	A	A	MA	A	B	A
[I.7] Condiciones inadecuadas de temp.	M	MA	M	B	M	M	MA	M	B	M	M	MA	M	B	M	M	MA	M	B	M
[E.2] Errores del administrador	M	MA	M	B	M	M	MA	M	B	M	M	MA	M	B	M	M	MA	M	B	M
[E.23] Errores de mant, / actual. de eq.	M	MA	M	B	M	M	MA	M	B	M	M	MA	M	B	M	M	MA	M	B	M
[E.25] Pérdida de equipos	A	MA	A	MB	M	A	MA	A	MB	M	A	MA	A	MB	M	A	MA	A	MB	M
[A.6] Abuso de privilegios de acceso	M	MA	M	B	M	M	MA	M	B	M	M	MA	M	B	M	M	MA	M	B	M
[A.7] Uso no previsto	M	MA	M	B	M	M	MA	M	B	M	M	MA	M	B	M	M	MA	M	B	M
[A.11] Acceso no autorizado	M	MA	M	B	M	M	MA	M	B	M	M	MA	M	B	M	M	MA	M	B	M
[A.23] Manipulación de los equipos	A	MA	A	B	A	A	MA	A	B	A	A	MA	A	B	A	A	MA	A	B	A
[A.24] Denegación de servicio	A	MA	A	M	A	A	MA	A	M	A	A	MA	A	M	A	A	MA	A	M	A
[A.25] Robo	MA	MA	MA	MB	A	MA	MA	MA	MB	A	MA	MA	MA	MB	A	MA	MA	MA	MB	A
[A.26] Ataque destructivo	A	MA	A	B	A	A	MA	A	B	A	A	MA	A	B	A	A	MA	A	B	A

	[srv_mail]					[srv_db]					[srv_web]					[srv_ant]				
AMENAZAS	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**
[N.1]Fuego	MA	MA	MA	MB	A	MA	MA	MA	MB	A	MA	MA	MA	MB	A	MA	MA	MA	MB	A
[N.2] Daños por agua	A	MA	A	MB	M	A	MA	A	MB	M	A	MA	A	MB	M	A	MA	A	MB	M
[I.1] Fuego	MA	MA	MA	MB	A	MA	MA	MA	MB	A	MA	MA	MA	MB	A	MA	MA	MA	MB	A
[I.2] Daños por agua	A	MA	A	MB	M	A	MA	A	MB	M	A	MA	A	MB	M	A	MA	A	MB	M
[I.*] Desastres industriales	A	MA	A	B	A	A	MA	A	B	A	A	MA	A	B	A	A	MA	A	B	A
[I.3] Contaminación mecánica	M	MA	M	M	M	M	MA	M	M	M	M	MA	M	M	M	M	MA	M	M	M
[I.4] Contaminación electromagnética	B	MA	MB	B	MB	B	MA	MB	B	MB	B	MA	MB	B	MB	B	MA	MB	B	MB
[I.5] Avería de origen físico o lógico	A	MA	A	M	A	A	MA	A	M	A	A	MA	A	M	A	A	MA	A	M	A
[I.6] Corte de suministro eléctrico	A	MA	A	B	A	A	MA	A	B	A	A	MA	A	B	A	A	MA	A	B	A
[I.7] Condiciones inadecuadas de temp.	M	MA	M	B	M	M	MA	M	B	M	M	MA	M	B	M	M	MA	M	B	M
[E.2] Errores del administrador	M	MA	M	B	M	M	MA	M	B	M	M	MA	M	B	M	M	MA	M	B	M
[E.23] Errores de mant, / actual. de eq.	M	MA	M	B	M	M	MA	M	B	M	M	MA	M	B	M	M	MA	M	B	M
[E.25] Pérdida de equipos	A	MA	A	MB	M	A	MA	A	MB	M	A	MA	A	MB	M	A	MA	A	MB	M
[A.6] Abuso de privilegios de acceso	M	MA	M	B	M	M	MA	M	B	M	M	MA	M	B	M	M	MA	M	B	M
[A.7] Uso no previsto	M	MA	M	B	M	M	MA	M	B	M	M	MA	M	B	M	M	MA	M	B	M
[A.11] Acceso no autorizado	M	MA	M	B	M	M	MA	M	B	M	M	MA	M	B	M	M	MA	M	B	M
[A.23] Manipulación de los equipos	A	MA	A	B	A	A	MA	A	B	A	A	MA	A	B	A	A	MA	A	B	A
[A.24] Denegación de servicio	A	MA	A	M	A	A	MA	A	M	A	A	MA	A	M	A	A	MA	A	M	A
[A.25] Robo	MA	MA	MA	MB	A	MA	MA	MA	MB	A	MA	MA	MA	MB	A	MA	MA	MA	MB	A
[A.26] Ataque destructivo	A	MA	A	B	A	A	MA	A	B	A	A	MA	A	B	A	A	MA	A	B	A

Tabla 27 - Estimación de impacto y riesgo del activo SOPORTE DE INFORMACIÓN. Fuente: El autor.

ESTIMACIÓN DE IMPACTO Y RIESGO EN ACTIVO**: SOPORTES DE INFORMACIÓN.**

	[disk]					[san]					[tape]				
AMENAZAS	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**
[N.1]Fuego	MA	A	A	MB	M	MA	A	A	MB	M	MA	A	A	MB	M
[N.2] Daños por agua	A	A	M	MB	B	A	A	M	MB	B	A	A	M	MB	B
[I.1] Fuego	MA	A	A	MB	M	MA	A	A	MB	M	MA	A	A	MB	M
[I.2] Daños por agua	A	A	M	B	M	A	A	M	B	M	A	A	M	B	M
[I.*] Desastres industriales	A	A	M	B	M	A	A	M	B	M	A	A	M	B	M
[I.3] Contaminación mecánica	M	A	B	B	B	M	A	B	B	B	M	A	B	B	B
[I.4] Contaminación electromagnética	B	A	MB	B	MB	B	A	MB	B	MB	B	A	MB	B	MB
[I.5] Avería de origen físico o lógico	A	A	M	M	M	A	A	M	M	M	A	A	M	M	M
[I.6] Corte de suministro eléctrico	A	A	M	B	M	A	A	M	M	M	A	A	M	B	M
[I.7] Condiciones inadecuadas de temperatura o humedad	M	A	B	B	B	M	A	B	B	B	M	A	B	B	B
[I.10] Degradación de los soportes de almacenamiento de información	A	A	M	M	M	A	A	M	M	M	A	A	M	M	M
[E.2] Errores del administrador	M	A	B	B	B	M	A	B	B	B	M	A	B	B	B
[E.19] Fugas de información	A	A	M	B	M	A	A	M	B	M	A	A	M	B	M
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	A	A	M	B	M	A	A	M	B	M	A	A	M	B	M
[E.25] Pérdida de equipos	A	A	M	B	M	A	A	M	B	M	A	A	M	B	M
[A.7] Uso no previsto	M	A	B	B	B	M	A	B	B	B	M	A	B	B	B
[A.11] Acceso no autorizado	M	A	B	M	B	M	A	B	M	B	M	A	B	M	B
[A.15] Modificación deliberada de la información	M	A	B	B	B	M	A	B	B	B	M	A	B	B	B
[A.18] Destrucción de información	A	A	M	M	M	A	A	M	M	M	A	A	M	M	M
[A.19] Divulgación de información	M	A	B	B	B	M	A	B	B	B	M	A	B	B	B
[A.25] Robo	MA	A	A	B	A	MA	A	A	B	A	MA	A	A	B	A
[A.26] Ataque destructivo	A	A	M	B	M	A	A	M	B	M	A	A	M	B	M

Tabla 28 - Estimación de impacto y riesgo del activo EQUIPAMIENTO AUXILIAR. Fuente: El autor.

ESTIMACIÓN DE IMPACTO Y RIESGO EN ACTIVO**: EQUIPAMIENTO AUXILIAR**

	[furniture]					[tools]					[tools_network]				
AMENAZAS	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**
[N.1]Fuego	A	B	MB	MB	MB	A	M	B	MB	MB	A	M	B	MB	MB
[N.2] Daños por agua	MB	B	MB	MB	MB	MB	M	MB	MB	MB	B	M	MB	MB	MB
[I.1] Fuego	A	B	MB	MB	MB	A	M	B	MB	MB	A	M	B	MB	MB
[I.2] Daños por agua	MB	B	MB	B	MB	MB	M	MB	B	MB	B	M	MB	B	MB
[I.*] Desastres industriales	A	B	MB	B	MB	A	M	B	B	B	A	M	B	B	B
[I.3] Contaminación mecánica	MB	B	MB	B	MB	MB	M	MB	B	MB	B	M	MB	B	MB
[I.4] Contaminación electromagnética	MB	B	MB	B	MB	MB	M	MB	B	MB	MB	M	MB	B	MB
[I.5] Avería de origen físico o lógico	B	B	MB	M	MB	B	M	MB	M	MB	M	M	MB	M	MB
[I.6] Corte de suministro eléctrico															
[I.7] Condiciones inadecuadas de temp.	MB	B	MB	B	MB	MB	M	MB	B	MB	MB	M	MB	B	MB
[E.23] Errores de manten. / actualización de Eq.	MB	B	MB	B	MB	MB	M	MB	B	MB	MB	M	MB	B	MB
[E.25] Pérdida de equipos	M	B	MB	B	MB	M	M	MB	B	MB	M	M	MB	B	MB
[A.7] Uso no previsto	MB	B	MB	B	MB	MB	M	MB	B	MB	MB	M	MB	B	MB
[A.25] Robo	MA	B	B	B	B	MA	M	M	B	M	MA	M	M	B	M
[A.26] Ataque destructivo	A	B	MB	B	MB	A	M	B	B	B	A	M	B	B	B

	[ss]					[ups]					[ac]				
AMENAZAS	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**
[N.1]Fuego	MA	A	A	MB	M	MA	MA	MA	MB	A	MA	MA	MA	MB	A
[N.2] Daños por agua	B	A	MB	MB	MB	A	MA	A	MB	M	A	MA	A	MB	M
[I.1] Fuego	MA	A	A	MB	M	MA	MA	MA	MB	A	MA	MA	MA	MB	A
[I.2] Daños por agua	B	A	MB	B	MB	A	MA	A	B	A	A	MA	A	B	A
[I.*] Desastres industriales	A	A	M	B	M	A	MA	A	B	A	A	MA	A	B	A
[I.3] Contaminación mecánica	B	A	MB	B	MB	B	MA	MB	B	MB	B	MA	MB	B	MB
[I.4] Contaminación electromagnética	B	A	MB	B	MB	M	MA	M	B	M	M	MA	M	B	M
[I.5] Avería de origen físico o lógico	M	A	B	M	B	A	MA	A	M	A	A	MA	A	M	A
[I.6] Corte de suministro eléctrico	A	A	M	B	M	M	MA	M	B	M	A	MA	A	B	A
[I.7] Condiciones inadecuadas de temp.	B	A	MB	B	MB	B	MA	MB	B	MB	B	MA	MB	B	MB
[E.23] Errores de manten. / actualización de Eq.	M	A	B	B	B	M	MA	M	B	M	M	MA	M	B	M
[E.25] Pérdida de equipos	A	A	M	B	M	M	MA	M	B	M	A	MA	A	B	A
[A.7] Uso no previsto	B	A	MB	B	MB	MB	MA	MB	B	MB	MB	MA	MB	B	MB
[A.25] Robo	MA	A	A	B	A	MA	MA	MA	B	A	MA	MA	MA	B	A
[A.26] Ataque destructivo	A	A	M	B	M	A	MA	A	B	A	A	MA	A	B	A

Tabla 29 - Estimación de impacto y riesgo del activo INSTALACIONES. Fuente: El autor.

ESTIMACIÓN DE IMPACTO Y RIESGO EN ACTIVO**: INSTALACIONES**										
	[building]					**[local]**				
AMENAZAS	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**
[N.1]Fuego	A	MA	A	MB	M	A	MA	A	MB	M
[N.2] Daños por agua	B	MA	MB	MB	MB	B	MA	MB	MB	MB
[I.1] Fuego	A	MA	A	MB	M	A	MA	A	MB	M
[I.2] Daños por agua	B	MA	MB	B	MB	B	MA	MB	B	MB
[I.*] Desastres industriales	A	MA	A	B	A	A	MA	A	B	A
[A.7] Uso no previsto	M	MA	M	B	M	M	MA	M	B	M
[A.11] Acceso no autorizado	A	MA	A	B	A	A	MA	A	B	A
[A.26] Ataque destructivo	A	MA	A	B	A	A	MA	A	B	A

Tabla 30 - Estimación de impacto y riesgo del activo REDES DE COMUNICACIONES. Fuente: El autor.

ESTIMACIÓN DE IMPACTO Y RIESGO EN ACTIVO**: REDES DE COMUNICACIONES**

	[wifi]					[LAN]				
AMENAZAS	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**
[A.5] Suplantación de la identidad del usuario	M	MA	M	B	M	A	MA	A	B	A
[A.6] Abuso de privilegios de acceso	A	MA	A	B	A	A	MA	A	B	A
[A.10] Alteración de secuencia	A	MA	A	B	A	A	MA	A	B	A
[A.11] Acceso no autorizado	M	MA	M	B	M	A	MA	A	B	A
[A.12] Análisis de tráfico	A	MA	A	M	A	A	MA	A	M	A
[A.14] Interceptación de información (escucha)	A	MA	A	M	A	A	MA	A	M	A
[A.24] Denegación de servicio	A	MA	A	M	A	A	MA	A	M	A

Tabla 31 - Estimación de impacto y riesgo del activo PERSONAL. Fuente: El autor.

ESTIMACIÓN DE IMPACTO Y RIESGO EN ACTIVO**: PERSONAL**																									
	[adm]					**[com]**					**[ast]**					**[des]**					**[wm]**				
AMENAZAS	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**	**[deg]**	**[val]**	**[imp]**	**[pro]**	**[rie]**
[E.7]Deficiencias en la organización	A	A	M	B	M	A	A	M	B	M	A	A	M	B	M	A	A	M	B	M	A	A	M	B	M
[E.19] Fugas de información	A	A	M	B	M	A	A	M	B	M	A	A	M	B	M	A	A	M	B	M	A	A	M	B	M
[E.28] Indisponibilidad del personal	A	A	M	B	M	A	A	M	B	M	A	A	M	B	M	A	A	M	B	M	A	A	M	B	M
[A.28] Indisponibilidad del personal	A	A	M	B	M	A	A	M	B	M	A	A	M	B	M	A	A	M	B	M	A	A	M	B	M
[A.29] Extorsión	A	A	M	B	M	A	A	M	B	M	A	A	M	B	M	A	A	M	B	M	A	A	M	B	M
[A.30] Ingeniería social	A	A	M	B	M	A	A	M	B	M	A	A	M	B	M	A	A	M	B	M	A	A	M	B	M

3.4 Tratamiento de riesgo

El tratamiento de riesgo es un proceso que consiste en seleccionar las medidas más convenientes con el objetivo de poder modificar el riesgo y evitar posibles daños. A continuación se detalla en la Tabla 32 algunas formas de tratar el riesgo como lo es el **evitar** las circunstancias que lo provocan, **reducir** las posibilidades de que ocurra, **compartirlo** con otra organización, **aceptando** que pueda ocurrir y previendo recursos para actuar cuando sea necesario. Adicionalmente se muestran vulnerabilidades y salvaguardas que ayudan a mitigar las amenazas que presentan los activos.

Tabla 32 - Tratamiento de riesgo. Fuente: El autor.

DATOS			
Amenaza	**Vulnerabilidades**	**Salvaguarda**	**Tratamiento**
[A.11] Acceso no autorizado	Gestión de acceso o red no adecuada	H.AC Control de acceso	Reducirlo
[A.13] Repudio	Falta de gestión de logs	H.LA análisis de logs	Reducirlo
[A.15] Modificación deliberada de la información	Falta de seguridad en puertos o contraseñas por default	H.IA Identificación y autenticación H.AC Control de acceso lógico	Reducirlo
[A.18] Destrucción de información	Falta de control para asegurar la información	H.AC Control de acceso D.A Copias de seguridad de los datos (backup)	Reducirlo
[A.19] Divulgación de información	Falta de política de confidencialidad	D Protección de la Información	Reducirlo
[A.3] Manipulación de los registros de actividad (log)	Falta de seguridad en puertos o contraseñas por default	H.LA análisis y gestión de logs H.AC Control de acceso lógico D.A Copias de seguridad de los datos (backup)	Reducirlo
[A.4] Manipulación de la configuración	Falta de seguridad en puertos o contraseñas por default	H.AC Control de acceso lógico D.A Copias de seguridad de los datos (backup)	Reducirlo
[A.5] Suplantación	Falta de protección en las	H.IA Identificación y	Reducirlo

de la identidad del usuario	redes Falta de política acerca del uso de contraseñas y de equipos informáticos	autenticación H.AC Control de acceso lógico	
[A.6] Abuso de privilegios de acceso	Falta de control para asegurar la información	H.IA Identificación y autenticación H.AC Control de acceso lógico	Reducirlo
[E.1] Errores de los usuarios	Falta de capacitación sobre uso del sistema/aplicación	D.A Copias de seguridad de los datos (backup)	Reducirlo
[E.15] Alteración accidental de la información	Falta de capacitación sobre uso del sistema/aplicación	D.A Copias de seguridad de los datos (backup)	Reducirlo
[E.18] Destrucción de información	Falta de plan de respaldo de información	H.AC Control de acceso D.A Copias de seguridad de los datos (backup)	Reducirlo
[E.19] Fugas de información	Falta de política de confidencialidad	D Protección de la Información	Reducirlo
[E.2] Errores del administrador	Falta de capacitación sobre uso del sistema/aplicación	D.A Copias de seguridad de los datos (backup)	Reducirlo
[E.3] Errores de monitorización (log)	Falta de procedimiento o mecanismo de monitoreo	H.LA análisis y gestión de logs	Reducirlo
[E.4] Errores de configuración	Falta de manuales de configuración	Creación de manuales	Reducirlo
SERVICIOS			
Amenaza	**Vulnerabilidades**	**Salvaguarda**	**Tratamiento**
[E.24] Caída del sistema por agotamiento de recursos	Falta de un plan o procedimiento para verificar problemas	S.www Protección de servicios S.email Protección del correo electrónico	Reducirlo
[A.24] Denegación de servicio	Forma no adecuada de la gestión de red Falta de plan de monitoreo	S.SC Se aplican perfiles de seguridad	Reducirlo
SOFTWARE			
Amenaza	**Vulnerabilidades**	**Salvaguarda**	**Tratamiento**
[I.5] Avería de origen físico o lógico	Falta de gestión de modificaciones o plan de mantenimiento/actualización	SW.A Copias de seguridad (backup) SW.CM Cambios (actualizaciones y mantenimiento)	Reducirlo
[A.18] Destrucción de información	Falta de control de accesos	H.AC Control de acceso	Reducirlo
HARDWARE			
Amenaza	**Vulnerabilidades**	**Salvaguarda**	**Tratamiento**
[A.11] Acceso no autorizado	Falta de control de acceso	H.AC Control de acceso físico HW.SC Se aplican perfiles de seguridad	Reducirlo
[A.23] Manipulación de los equipos	Falta de control de acceso	H.AC Control de acceso físico HW.SC Se aplican perfiles de seguridad	Reducirlo
[A.24] Denegación de servicio	Falta de monitoreo y control de acceso	H.AC Control de acceso físico HW.SC Se aplican perfiles de seguridad	Reducirlo

[A.25] Robo	Falta de control de acceso Falta de inventario	H.AC Control de acceso físico HW.SC Se aplican perfiles de seguridad	Reducirlo
[A.26] Ataque destructivo	Falta de control de acceso	H.AC Control de acceso físico HW.SC Se aplican perfiles de seguridad	Reducirlo
[A.6] Abuso de privilegios de acceso	Falta de control de acceso	H.AC Control de acceso físico HW.SC Se aplican perfiles de seguridad	Reducirlo
[A.7] Uso no previsto	Falta de control de acceso	H.AC Control de acceso físico HW.SC Se aplican perfiles de seguridad	Reducirlo
[E.2] Errores del administrador	Falta de manual de instalación y configuración Falta de conocimiento del personal	Procedimiento de instalación / configuración	Reducirlo
[E.23] Errores de mantenimiento / actualización de equipos	Falta de plan de mantenimiento y actualización	HW.CM Cambios (actualizaciones y mantenimiento)	Reducirlo
[E.25] Pérdida de equipos	Falta de control de acceso	H.AC Control de acceso físico HW.SC Se aplican perfiles de seguridad	Reducirlo
[I.*] Desastres industriales	Instalaciones eléctricas no protegidas	H.IR Gestión de incidencias	Reducirlo
[I.1] Fuego	Productos inflamables	H.IR Gestión de incidencias	Reducirlo
[I.2] Daños por agua	Daño de cañerías o fugas de agua	H.IR Gestión de incidencias	Reducirlo
[I.3] Contaminación mecánica	Falta de mantenimiento del equipo y área	Plan de mantenimiento	Reducirlo
[I.5] Avería de origen físico o lógico	Equipos con defectos de fábrica	Gestión de garantía o partes	Reducirlo
[I.6] Corte de suministro eléctrico	Apagones inesperados	Gestión de UPS	Reducirlo
[I.7] Condiciones inadecuadas de temperatura o humedad	Falta de condiciones ambientales adecuadas	Plan de mantenimiento de acondicionadores de aire	Reducirlo
[N.1]Fuego	Falta de sistema contra incendio	H.IR Gestión de incidencias	Reducirlo
[N.2] Daños por agua	Goteras	H.IR Gestión de incidencias	Reducirlo
MEDIA			
Amenaza	**Vulnerabilidades**	**Salvaguarda**	**Tratamiento**
[A.25] Robo	Falta de control de acceso	H.AC Control de acceso	Reducirlo
[A.26] Ataque destructivo	Falta de control de acceso	H.AC Control de acceso	Reducirlo
[E.19] Fugas de información	Falta de política de confidencialidad	D Protección de la Información MP.end Destrucción de soportes	Reducirlo

[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Falta de plan de mantenimiento	Plan de mantenimiento de medios MP.clean Limpieza de contenidos	Reducirlo
[E.25] Pérdida de equipos	Falta de control de acceso	H.AC Control de acceso	Reducirlo
[I.*] Desastres industriales	Falta de procedimiento de manipulación	Procedimiento de manipulación	Reducirlo
[I.1] Fuego	Productos inflamables	H.IR Gestión de incidencias	Reducirlo
[I.2] Daños por agua	Daño de cañerías o fugas de agua	H.IR Gestión de incidencias	Reducirlo
[I.5] Avería de origen físico o lógico	Equipos con defectos de fábrica	Gestión de garantía o partes	Reducirlo
[I.6] Corte de suministro eléctrico	Apagones inesperados	Gestión de UPS	Reducirlo
[N.1]Fuego	Falta de sistema contra incendio	Geston de extintores	Reducirlo
AUX			
Amenaza	**Vulnerabilidades**	**Salvaguarda**	**Tratamiento**
[A.25] Robo	Falta de control de acceso	H.AC Control de acceso	Reducirlo
[A.26] Ataque destructivo	Falta de control de acceso	H.AC Control de acceso	Reducirlo
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Falta de plan de mantenimiento	Plan de mantenimiento	Reducirlo
[E.25] Pérdida de equipos	Falta de control de acceso	H.AC Control de acceso	Reducirlo
[I.1] Fuego	Productos inflamables	H.IR Gestión de incidencias	Reducirlo
[I.2] Daños por agua	Daño de cañerías o fugas de agua	H.IR Gestión de incidencias	Reducirlo
[I.5] Avería de origen físico o lógico	Equipos con defectos de fábrica	Gestión de garantía o partes	Reducirlo
[I.6] Corte de suministro eléctrico	Apagones inesperados	Gestión de UPS AUX.power Suministro eléctrico	Reducirlo
[N.1]Fuego	Falta de sistema contra incendio	Gestión de extintores	Reducirlo
[N.2] Daños por agua	Goteras	H.IR Gestión de incidencias	Reducirlo
LOCALIDAD			
Amenaza	**Vulnerabilidades**	**Salvaguarda**	**Tratamiento**
[A.11] Acceso no autorizado	Falta de control de acceso	L.AC Control de los accesos físicos	Reducirlo
[A.26] Ataque destructivo	Falta de control de acceso	L.AC Control de los accesos físicos	Reducirlo
[A.7] Uso no previsto	Falta de control de acceso	L.AC Control de los accesos físicos	Reducirlo
[I.*] Desastres industriales	Instalaciones eléctricas no protegidas	H.IR Gestión de incidencias	Reducirlo
[I.1] Fuego	Productos inflamables	H.IR Gestión de incidencias	Reducirlo
[N.1]Fuego	Falta de sistema contra incendio	Geston de extintores	Reducirlo

COMUNICACIONES			
Amenaza	**Vulnerabilidades**	**Salvaguarda**	**Tratamiento**
[A.10] Alteración de secuencia	Gestión de acceso o red no adecuada	H.AC Control de acceso	Reducirlo
[A.11] Acceso no autorizado	Gestión de acceso o red no adecuada	H.AC Control de acceso	Reducirlo
[A.12] Análisis de tráfico	Gestión de acceso o red no adecuada	Plan de monitoreo y análisis de tráfico	Reducirlo
[A.14] Interceptación de información (escucha)	Gestión de acceso o red no adecuada	H.AC Control de acceso Procedimiento de monitoreo	Reducirlo
[A.24] Denegación de servicio	Falta de monitoreo y control de acceso	H.AC Control de acceso físico HW.SC Se aplican perfiles de seguridad	Reducirlo
[A.5] Suplantación de la identidad del usuario	Falta de protección en las redes Falta de política acerca del uso de contraseñas y de equipos informáticos	H.IA Identificación y autenticación H.AC Control de acceso lógico	Reducirlo
[A.6] Abuso de privilegios de acceso	Falta de control para asegurar accesos	H.IA Identificación y autenticación H.AC Control de acceso lógico	Reducirlo
PERSONAL			
Amenaza	**Vulnerabilidades**	**Salvaguarda**	**Tratamiento**
[E.7]Deficiencias en la organización	Falta de capacitación sobre la seguridad de la información Falta de políticas de uso correcto de la infraestructura tecnológica Falta de control en la entrega de activos Falta de motivación	PS.AT Formación y concienciación	Reducirlo
[E.19] Fugas de información	Falta de política de confidencialidad	D Protección de la Información	Reducirlo
[E.28] Indisponibilidad del personal	Falta de plan de contingencia en caso de ausencia Enfermedad	Plan de contingencia de personal	Reducirlo
[A.28] Indisponibilidad del personal	Falta de plan de responsabilidades y deberes	Documento de responsabilidades	Reducirlo
[A.29] Extorsión	Falta de motivación	PS.AT Formación y concienciación	Reducirlo
[A.30] Ingeniería social (picaresca)	Falta de capacitación sobre la seguridad de la información Falta de políticas de uso correcto de la infraestructura tecnológica Falta de control en la entrega de activos Falta de motivación	PS.AT Formación y concienciación	Reducirlo

Una vez que se ha definido el tratamiento de riesgo, es importante indicar que por más eficiente que sea el tratamiento, siempre existirá un riesgo.

CAPÍTULO 4

DISEÑO E IMPLEMENTACIÓN DEL ESQUEMA DE SEGURIDAD.

4.1 Selección de controles basados en la Norma ISO 27002

Para llevar a cabo el diseño e implementación del esquema de seguridad tanto física como lógica, se realizará la selección de controles de la norma ISO 27002:2013, la cual nos ofrece una lista de controles que ayudan a reducir los riesgos identificados de acuerdo al análisis de los activos previos. En la Tabla 33 se detallan los controles seleccionados:

Tabla 33 – Controles seleccionados. Fuente: El autor.

DATOS: [bd_crm] [bd_reservar] [bd_controlac] [bd_reunion] [bd_ara] [bd_satt] [backup]	 [source] [files] [bd_controlpc] [conf] [log] [bd_ldap] [bd_sitioFiec]
Amenaza	**Control**
[A.11] Acceso no autorizado	Política de control de acceso. (9.1.1)
[A.13] Repudio	Registro de actividad y supervisión. (12.4)
[A.15] Modificación deliberada de la información	Gestión de los derechos de acceso asignados a usuarios. (9.2.2) Política de control de acceso. (9.1.1)

[A.18] Destrucción de información	Política de control de acceso. (9.1.1) Copias de seguridad de la información. (12.3.1)
[A.19] Divulgación de información	Responsabilidades del usuario. (9.3)
[A.3] Manipulación de los registros de actividad (log)	Política de control de acceso. (9.1.1) Copias de seguridad de la información. (12.3.1)
[A.4] Manipulación de la configuración	Política de control de acceso. (9.1.1) Copias de seguridad de la información. (12.3.1) Segregación de tareas. (6.1.2)
[A.5] Suplantación de la identidad del usuario	Política de control de acceso. (9.1.1) Responsabilidades del usuario. (9.3)
[A.6] Abuso de privilegios de acceso	Segregación de tareas. (6.1.2) Responsabilidades del usuario. (9.3) Política de control de acceso. (9.1.1)
[E.1] Errores de los usuarios	Concienciación, educación y capacitación en seguridad de la información (7.2.2) Copias de seguridad de la información. (12.3.1)
[E.15] Alteración accidental de la información	Concienciación, educación y capacitación en seguridad de la información (7.2.2) Copias de seguridad de la información. (12.3.1)
[E.18] Destrucción de información	Política de control de acceso. (9.1.1) Copias de seguridad de la información. (12.3.1)
[E.19] Fugas de información	Uso aceptable de los activos. (8.1.3)
[E.2] Errores del administrador	Uso aceptable de los activos. (8.1.3) Copias de seguridad de la información. (12.3.1)
[E.3] Errores de monitorización (log)	Registro de actividad y supervisión. (12.4) Responsabilidades del usuario. (9.3)
[E.4] Errores de configuración	Asignación de responsabilidades para la seguridad de la información. (6.1.1) Organización interna. (6.1) Documentación de procedimientos de operación. (12.1.1)
SERVICIOS: [servi_wifi] [email]	
Amenaza	**Control**
[E.24] Caída del sistema por agotamiento de recursos	Responsabilidades y procedimientos de operación. (12.1) Documentación de procedimientos de operación. (12.1.1) Registro de actividad y supervisión. (12.4)
[A.24] Denegación de servicio	Responsabilidades y procedimientos de operación. (12.1) Registro de actividad y supervisión. (12.4) Registro y gestión de eventos de actividad. (12.4.1)
SOFTWARE: [sis_crm] [sis_controlac] [sis_creacion] [sis_reunion] [sis_reservar] [sis_ara] [sis_satt] [pkt] [sis_controlpc] [av] [sis_portal]	
Amenaza	**Control**
[I.5] Avería de origen físico o lógico	Uso aceptable de los activos. (8.1.3) Copias de seguridad de la información. (12.3.1) Responsabilidades y procedimientos de operación. (12.1)

[A.18] Destrucción de información	Política de control de acceso. (9.1.1)
HARDWARE: [print] [scan] [cam] [mobile] [srv_strmg] [wap] [pc] [srv_files] [srv_control] [srv_dhcp] [srv_radius] [switch] [router] [srv_mail] [srv_db] [srv_web] [srv_ant]	
Amenaza	**Control**
[A.11] Acceso no autorizado	Política de control de acceso. (9.1.1) Segregación de tareas. (6.1.2) Responsabilidades del usuario. (9.3)
[A.23] Manipulación de los equipos	Política de control de acceso. (9.1.1) Responsabilidades y procedimientos de operación. (12.1) Documentación de procedimientos de operación. (12.1.1)
[A.24] Denegación de servicio	Perímetro de seguridad física. (11.1.1) Controles físicos de entrada. (11.1.2) Protección contra las amenazas externas y ambientales. (11.1.4)
[A.25] Robo	Seguridad de los equipos. (11.2) Inventario de activos. (8.1.1)
[A.26] Ataque destructivo	Controles físicos de entrada. (11.1.2) Responsabilidades y procedimientos de operación. (12.1)
[A.6] Abuso de privilegios de acceso	Controles físicos de entrada. (11.1.2) Perímetro de seguridad física. (11.1.1)
[A.7] Uso no previsto	Controles físicos de entrada. (11.1.2) Perímetro de seguridad física. (11.1.1) Responsabilidades del usuario. (9.3)
[E.2] Errores del administrador	Responsabilidades y procedimientos de operación. (12.1) Documentación de procedimientos de operación. (12.1.1)
[E.23] Errores de mantenimiento / actualización de equipos	Responsabilidades y procedimientos de operación. (12.1) Documentación de procedimientos de operación. (12.1.1)
[E.25] Pérdida de equipos	Controles físicos de entrada. (11.1.2) Perímetro de seguridad física. (11.1.1) Salida de activos fuera de las dependencias de la empresa. (11.2.5)
[I.*] Desastres industriales	Protección contra las amenazas externas y ambientales. (11.1.4)
[I.1] Fuego	Protección contra las amenazas externas y ambientales. (11.1.4)
[I.2] Daños por agua	Protección contra las amenazas externas y ambientales. (11.1.4)
[I.3] Contaminación mecánica	Mantenimiento de los equipos. (11.2.4)
[I.5] Avería de origen físico o lógico	Segregación de tareas. (6.1.2)
[I.6] Corte de suministro eléctrico	Instalaciones de suministro. (11.2.2)
[I.7] Condiciones inadecuadas de temperatura o humedad	Mantenimiento de los equipos. (11.2.4)

[N.1]Fuego	Protección contra las amenazas externas y ambientales. (11.1.4)
[N.2] Daños por agua	Protección contra las amenazas externas y ambientales. (11.1.4)
MEDIA: [disk] [san] [tape]	
Amenaza	**Control**
[A.25] Robo	Seguridad de los equipos. (11.2) Inventario de activos. (8.1.1) Controles físicos de entrada. (11.1.2)
[A.26] Ataque destructivo	Controles físicos de entrada. (11.1.2) Responsabilidades y procedimientos de operación. (12.1)
[E.19] Fugas de información	Uso aceptable de los activos. (8.1.3) Manejo de los soportes de almacenamiento. (8.3)
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Manejo de los soportes de almacenamiento. (8.3) Gestión de soportes extraíbles. (8.3.1) Mantenimiento de los equipos. (11.2.4)
[E.25] Pérdida de equipos	Seguridad de los equipos. (11.2) Inventario de activos. (8.1.1) Controles físicos de entrada. (11.1.2)
[I.*] Desastres industriales	Protección contra las amenazas externas y ambientales. (11.1.4) Gestión de soportes extraíbles. (8.3.1)
[I.1] Fuego	Protección contra las amenazas externas y ambientales. (11.1.4) Gestión de soportes extraíbles. (8.3.1)
[I.2] Daños por agua	Protección contra las amenazas externas y ambientales. (11.1.4) Gestión de soportes extraíbles. (8.3.1)
[I.5] Avería de origen físico o lógico	Gestión de soportes extraíbles. (8.3.1)
[I.6] Corte de suministro eléctrico	Instalaciones de suministro. (11.2.2)
[N.1]Fuego	Protección contra las amenazas externas y ambientales. (11.1.4) Manejo de los soportes de almacenamiento. (8.3)
AUX: [tools] [tools_network] [ss] [ups] [ac]	
Amenaza	**Control**
[A.25] Robo	Controles físicos de entrada. (11.1.2)
[A.26] Ataque destructivo	Controles físicos de entrada. (11.1.2)
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Mantenimiento de los equipos. (11.2.4)
[E.25] Pérdida de equipos	Controles físicos de entrada. (11.1.2)
[I.1] Fuego	Protección contra las amenazas externas y ambientales. (11.1.4)
[I.2] Daños por agua	Protección contra las amenazas externas y ambientales. (11.1.4)
[I.5] Avería de origen físico o lógico	Segregación de tareas. (6.1.2)
[I.6] Corte de suministro eléctrico	Instalaciones de suministro. (11.2.2)
[N.1]Fuego	Protección contra las amenazas externas y ambientales. (11.1.4)

[N.2] Daños por agua	Protección contra las amenazas externas y ambientales. (11.1.4)
LOCALIDAD: [building] [local]	
Amenaza	**Control**
[A.11] Acceso no autorizado	Controles físicos de entrada. (11.1.2) Perímetro de seguridad física. (11.1.1) Responsabilidades del usuario. (9.3)
[A.26] Ataque destructivo	Controles físicos de entrada. (11.1.2) Perímetro de seguridad física. (11.1.1) Responsabilidades del usuario. (9.3)
[A.7] Uso no previsto	Controles físicos de entrada. (11.1.2) Perímetro de seguridad física. (11.1.1) Responsabilidades del usuario. (9.3)
[I.*] Desastres industriales	Protección contra las amenazas externas y ambientales. (11.1.4)
[I.1] Fuego	Protección contra las amenazas externas y ambientales. (11.1.4)
[N.1]Fuego	Protección contra las amenazas externas y ambientales. (11.1.4)
COMUNICACIONES: [wifi] [LAN	
Amenaza	**Control**
[A.10] Alteración de secuencia	Uso aceptable de los activos. (8.1.3)
[A.11] Acceso no autorizado	Política de control de acceso. (9.1.1) Gestión de acceso de usuario. (9.2) Revisión de los derechos de acceso de los usuarios. (9.2.5) Responsabilidades y procedimientos de operación. (12.1)
[A.12] Análisis de tráfico	Registro de actividad y supervisión. (12.4) Registro y gestión de eventos de actividad. (12.4.1)
[A.14] Interceptación de información (escucha)	Política de control de acceso. (9.1.1) Registro de actividad y supervisión. (12.4) Registro y gestión de eventos de actividad. (12.4.1)
[A.24] Denegación de servicio	Controles físicos de entrada. (11.1.2) Política de control de acceso. (9.1.1)
[A.5] Suplantación de la identidad del usuario	Política de control de acceso. (9.1.1) Registro de actividad y supervisión. (12.4) Gestión de los derechos de acceso asignados a usuarios. (9.2.2)
[A.6] Abuso de privilegios de acceso	Gestión de acceso de usuario. (9.2) Gestión de los derechos de acceso asignados a usuarios. (9.2.2) Política de control de acceso. (9.1.1)
PERSONAL: [adm] [com] [ast] [des] [wm]	
Amenaza	**Control**
[E.7]Deficiencias en la organización	Asignación de responsabilidades para la seguridad de la información. (6.1.1) Segregación de tareas. (6.1.2) Concienciación, educación y capacitación en seguridad de la información (7.2.2)

[E.19] Fugas de información	Responsabilidad sobre los activos. (8.1) Uso aceptable de los activos. (8.1.3)
[E.28] Indisponibilidad del personal	Segregación de tareas. (6.1.2)
[A.28] Indisponibilidad del personal	Segregación de tareas. (6.1.2)
[A.29] Extorsión	Concienciación, educación y capacitación en seguridad de la información (7.2.2)
[A.30] Ingeniería social (picaresca)	Concienciación, educación y capacitación en seguridad de la información (7.2.2)

4.2 Definición de la Política

La FIEC cuenta con el DST el cual es el encargado de la administración de la infraestructura tecnológica de los activos, además de brindar servicio de soporte a laboratorios y usuarios; por ende está encargado de preservar estos recursos informáticos, por lo que ha sido necesario definir una política informática que será de uso para el DST y la FIEC en general, la cual se detalla continuación:

4.2.1 Política de seguridad informática

Objetivo:

Brindar orientación y soporte por parte del DST, para que los recursos informáticos sean usados adecuadamente, preservando la seguridad de los mismos.

Alcance:

Activos con mayor riesgo según el análisis de riesgo realizado.

Esta política está dirigida a los usuarios o personal del DST de acuerdo a las siguientes viñetas:

- Para personal del DST

o Para todos los usuarios: docentes, administrativos y estudiantes.

I. De los aspectos organizativos de la seguridad de la información.

Organización interna. (6.1)

Controles aplicados:

- *Asignación de responsabilidades para la seguridad de la información. (6.1.1)*
    - El DST poseerá en el esquema de seguridad de informática, la definición de roles y responsabilidades, los cuales considere las actividades de administración, operación y gestión de la seguridad de la información.

- El DST debe asignar las funciones, roles y responsabilidades al personal para que lleve a cabo las tareas de operación y administración de la infraestructura tecnológica de la FIEC.

- El DST debe revisar que en los manuales de función y procedimientos no existan inconsistencias, en lo relacionado a roles y responsabilidades de seguridad de la información.

- *Segregación de tareas. (6.1.2)*
  - Las funciones, roles y responsabilidades del personal del DST deben estar documentadas y apropiadamente segregadas. Ver ANEXO G.

Dispositivos móviles y teletrabajo. (6.2)

Controles aplicados:

- *Política de uso de dispositivos para movilidad. (6.2.1)*
  - El DST debe instalar un software de antivirus en los dispositivos móviles de la facultad y en el caso de equipos personales que hagan uso de los servicios que

brinda el DST, se deberá realizar la instalación o sugerir un software antivirus no institucional.

- El DST debe probar las opciones de protección de los dispositivos móviles que pertenecen a la facultad y dispositivos que hagan uso de los servicios que brinda la FIEC.
- El DST debe establecer las configuraciones necesarias para los dispositivos móviles que hagan uso de los servicios que brinda la FIEC.

o Los usuarios deben evitar hacer uso de los dispositivos móviles de la facultad en lugares que no les ofrezcan las garantías necesarias de seguridad física para evitar pérdida o robo de los mismos.

o Los usuarios no deben modificar las configuraciones de seguridad de los dispositivos móviles de la facultad, ni desinstalar el software provisto al momento de la entrega del equipo.

o Los usuarios deben evitar la instalación de programas desde fuentes desconocidas; sólo se debe instalar aplicaciones desde los repositorios o medios dispuestos por el DST o la GTySI.

- Si requiere la instalación de algún software en su equipo móvil deberá solicitarlo al personal del DST.
- Los usuarios deben evitar hacer uso de redes inalámbricas que no sean de la ESPOL y FIEC.
- Los usuarios deben evitar conectar los dispositivos móviles de la facultad tales como usb, discos externos, tablets, etc. a cualquier computador que no sea de la FIEC (computador de personales, hoteles, cybers, entre otros). Ver sección control de acceso.

- *Teletrabajo. (6.2.2)*
  - EL DST configurará la conexión remota (VPN de la ESPOL) en los equipos que necesiten tener acceso a los sistemas o software institucional fuera de la red de ESPOL, para que dicha conexión se realice de manera segura.
  - Los usuarios deben evitar establecer conexiones remotas en computadores desde computadores públicos, cybers, entre otros.

II. De la seguridad ligada a los recursos humanos.

Durante la contratación. (7.2)

Controles aplicados:

- *Concienciación, educación y capacitación en seguridad de la información (7.2.2)*
    - o Todos quienes laboran o hacen uso de los recursos informáticos de la FIEC, deberán leer el documento de políticas de seguridad de informática para su conocimiento.

Cese o cambio de puesto de trabajo. (7.3)

- *Cese o cambio de puesto* de trabajo. (7.3.1)
    - El DST debe de ser notificado cuando exista terminación o cambio de personal, para comunicar al nuevo personal de las responsabilidades y deberes en lo que refiere a tareas y seguridad de la información que tiene a cargo.

III. De la gestión de activos.

Responsabilidad sobre los activos. (8.1)

- El personal del DST es el encargado de realizar instalación, cambio, modificación o eliminación de los activos que administra.

- El DST es responsable de establecer una configuración adecuada para los activos, con el fin de preservar la seguridad y hacer un uso adecuado de los mismos.
- El DST es responsable de preparar las estaciones de trabajo fijas y/o portátiles del personal docente y administrativo y de hacer entrega de las mismas mediante un acta.

o A los usuarios que le son asignados recursos tecnológicos, se comprometen a hacer uso adecuado y eficiente de los mismos.

o Los recursos tecnológicos de la FIEC, deben ser utilizados de forma ética y cumpliendo la presente política, con el fin de evitar daños o pérdidas que afecten la imagen de la facultad u operación del mismo.

Controles aplicados:

- *Inventario de activos. (8.1.1)*
    - Todos los activos deben ser registrados.
    - El DST debe tener los activos importantes identificados por lo que se debe elaborar y mantener un inventario de los mismos. Ver ANEXO H que corresponde al modelo de manejo de inventario.

- El DST debe verificar al finalizar de cada término académico que el inventario de los activos que administra está completo.

- *Propiedad de los activos. (8.1.2)*
  - Los activos deben estar asociados a una persona responsable, quien hace uso del mismo. En el caso del DST tiene personal encargado del inventario y dar mantenimiento. Ver ANEXO I.
  - El DST debe monitorear periódicamente la validez de los usuarios (propietarios/responsables) y sus perfiles de acceso a los activos de información.

- *Uso aceptable de los activos. (8.1.3)*
  - El DST asignará activos de información para apoyar a docentes y administrativos en sus actividades laborables diarias, estos activos deben ser usados de manera aceptable y para ello se definen las siguientes reglas:

Para el uso de equipos

  - Los usuarios no deberán hacer uso de los equipos para asuntos personales.

- Para solicitar un equipo se debe tener la autorización de la máxima autoridad de la facultad, adicionalmente deberá firmar un acta de entrega/recepción del mismo, comprometiéndose a entregarlo en la fecha definida en las mismas condiciones en que fue entregado.
- Si el equipo se traslada fuera de la facultad o la ESPOL es necesario que dispongan de un transporte seguro para preservar la integridad del mismo, además de tener copia de un acta de entrega/recepción con las siguientes firmas: Custodio, Decano y Responsable.

Para el uso de laboratorios

- Los docentes pueden realizar el préstamo del laboratorio haciendo uso del sistema de Reservar Salas.
- Para hacer uso de laboratorios con actividades que están fuera de la planificación académica, debe solicitar autorización de la máxima autoridad de la facultad y deberá ser responsable de entregar el laboratorio en las mismas condiciones en que fue recibido.

Para el uso de documentos

- Los documentos que están a disposición del personal del DST solo deben ser usados dentro de la facultad.
- Si es necesario trasladar un documento fuera del DST, se debe notificar al Jefe del DST. Ver ANEXO J que corresponden al acuerdo de confidencialidad.

Para el uso de Internet

- El DST tomará las medidas necesarias en caso de que se detecte amenazas que afecten el rendimiento de la red. Por ejemplo el acceso a páginas maliciosas con software dañino que pueden infectar el equipo y poner en riesgo toda la red.

o Todos los usuarios podrán hacer uso de la red internet para fines relacionados con su trabajo, desde el computador que se le ha asignado.

Para el uso de correo electrónico:

o Toda la comunidad de la FIEC, entiéndase por comunidad a docentes, administrativos y estudiantes, tiene derecho a una cuenta de correo electrónico de la FIEC.

- EL usuario de la cuenta de correo, es responsable de hacer buen uso de la misma en lo que corresponde a:
  - La cuenta de correo debe ser usada exclusivamente para fines académicos y administrativos.
  - No hacer uso de la cuenta para fines comerciales.
  - No enviar y/o contestar correos masivos, ni cadenas de correos.
- Se le asignará sólo una cuenta al usuario.
- Su cuenta de correo es personal e intransferible, no deberá permitir que otras personas hagan uso de ella. (Sólo se permitirá en caso de asuntos de trabajo)
- El usuario será responsable de la información que sea enviada a través de su cuenta de correo, es decir, que debe asegurarse de no enviar SPAMS, ni archivos anexos que pudieran ser nocivos para otros usuarios como por ejemplo troyanos/virus.
- La cuenta de correo se dará de baja una vez que el personal haya terminado sus funciones.
- El usuario es responsable de cambiar su contraseña con regularidad y deberá tener en consideración que cumpla

con los requisitos de contraseña segura: caracteres de 8-12 y al menos un número.

- El DST procederá a monitorear las cuentas que presenten un comportamiento sospechoso para la seguridad de la facultad.
- El correo no debe usarse para distribuir de forma ilegal licencias de software o información sin conocimiento del propietario de la misma.
- Si el usuario no hace buen uso de la cuenta de correo que se le ha asignado, puede ocasionar la suspensión de la misma, previa autorización de la máxima autoridad.
- La cuota del correo es de 30GB y es responsabilidad del usuario hacer respaldos de sus archivos de correo y eliminar los mismos cuando este alcanzando la cuota máxima.

Para el uso de software y sistemas

- El DST es el propietario de los activos de información correspondientes a las bases de datos, sistemas informáticos desarrollados para la facultad y responsable por el software que se encuentra en los repositorios, por

lo tanto, el DST debe asegurar su apropiada operación y administración.

- Los usuarios podrán usar los sistemas a través del sitio web de la facultad con usuario y contraseña según corresponda y no deberá permitir que otras personas hagan uso de los sistemas con sus credenciales.
- Los usuarios que se les haya asignado un equipo de trabajo pueden solicitar la instalación de software, siempre y cuando sea software con licencia institucional o libre.
- Los usuarios de los laboratorios pueden solicitar la instalación de software en los equipos de laboratorio con al menos una semana de anticipación.
- A los usuarios de los laboratorios se les solicitará al término de cada semestre, la lista de software y versión que necesitan para poder hacer uso del mismo en el siguiente término académico.
- Los usuarios no deben utilizar software no autorizado en equipos que el DST le haya facilitado.

- *Devolución de activos. (8.1.4)*

- El DST es responsable de recibir los equipos de trabajo fijo y/o portátil para que sean reasignados o queden a disposición, realizar copias de seguridad de la información en el caso de que sea necesario o formatear el equipo del personal docente o administrativo que se retire o cambie de funciones.
  - Los usuarios que se desvinculen o cambien de labores, deben realizar la entrega de su puesto de trabajo y los recursos informáticos que se le facilitaron al momento de su vinculación al Custodio de la facultad o a quien delegue la máxima autoridad de la facultad.

Manejo de los soportes de almacenamiento. (8.3)

- El DST definirá el uso de los soportes de almacenamiento que administra, tomando en consideración las tareas que realizan los usuarios y la necesidad de uso; con el fin de evitar que se divulgue, modifique, elimine o destruya información almacenada en los medios que administra.

Controles aplicados:

- *Gestión de soportes extraíbles. (8.3.1)*

- Los usuarios que se hacen uso de un computador asignado por el DST, no deben utilizar medios de almacenamiento prestados o de terceros y adicionalmente debe cumplir con lo siguiente:
  - Deben escanear el soporte extraíble con el antivirus institucional.
  - Debe tener desactivada la reproducción automática de archivos ejecutables.

- *Eliminación de soportes. (8.3.2)*
  - La información será eliminada de los medios de soporte de forma segura cuando ya no sea necesaria y previa autorización del dueño de la información. Ver ANEXO K de procedimiento de eliminación de soportes.

IV. Del control de acceso.

Requisitos de negocio para el control de accesos. (9.1)

Controles aplicados:

- *Política de control de accesos. (9.1.1)*
  - Con esta política se busca disminuir los inconvenientes de seguridad que se pueden producir por el abuso de privilegios de acceso y por accesos no autorizados.

- El usuario es responsable del acceso que se le ha proporcionado, es decir identificador de usuario y contraseña, que le permite acceder a los recursos informáticos que administra el DST, por lo cual deberá mantenerlo de forma confidencial.
- Solamente personal del DST podrá acceder a los repositorios de sistemas y software.
- Los docentes y personal administrativo podrán acceder a recursos y sistemas informáticos de acuerdo con lo siguiente:

Sistemas:	**Acceso para:**
Sistema CRM	Docentes y personal administrativo
Sistema Controlac	Docentes
Sistema Creación de Cuentas	Estudiantes
Sistema de Reuniones	Docentes y secretarias
Sistema Reservar Salas	Docentes, secretarias y DST
Sistema ARA	Docentes, secretarias y estudiantes
Sistema SATT	Docentes, secretarias y estudiantes
Repositorio de Software vario	DST
Sistema CONTROLPC	DST y estudiantes
Portal Cautivo	Comunidad dela FIEC
Recursos compartidos	Previa solicitud y autorización

- Los usuarios podrán acceder a los equipos asignados por el DST con usuario y contraseña configurados en el momento de asignar el mismo.

- Los usuarios de los equipos de laboratorios podrán acceder de acuerdo a lo siguiente:
  - Si el equipo se administra con el sistema ControlPC, deberá ingresar con las credenciales de FIEC.
  - Si el equipo no usa el sistema ControlPC, deberá usar las credenciales que se configuren al momento de entregar el mismo.

- *Control de acceso a las redes y servicios asociados. (9.1.2)*
  - El DST debe asegurar que la red inalámbrica cuente con un método de autenticación para evitar accesos no autorizados.
  - El DST debe verificar al término de cada semestre los controles de acceso para los usuarios, con el objetivo de revisar que dichos usuarios tengan acceso únicamente a los recursos de red y servicios que le fueron autorizados.
  - Los equipos de los usuarios que se conecten o deseen conectarse a las redes de datos de la FIEC podrán realizar únicamente las tareas y tener acceso a recursos para las que fueron autorizados.
  - Los usuarios, antes de contar con acceso a servicios y recursos de la red de datos de la FIEC, deben solicitar la

creación de una cuenta a la máxima autoridad y una vez autorizado, deberá firmar un Acuerdo de Confidencialidad.

Gestión de acceso de usuario. (9.2)

- El DST establecerá un procedimiento para asignar privilegios de acceso lógico a los usuarios. Adicionalmente, asignará acceso únicamente a la información necesaria para que pueda realizar sus labores.
- El DST establecerá un procedimiento formal para la administración de los usuarios en la red de datos y los recursos informáticos de la FIEC, que contemple la creación o eliminación de las cuentas de usuario.

Controles aplicados:

- *Gestión de altas/bajas en el registro de usuarios. (9.2.1)*
    - El DST, previa autorización de la máxima autoridad o Jefes inmediatos de los solicitantes de las cuentas de usuario, procederá a crear, modificar, bloquear o *eliminar dicha cuenta.*

- *Gestión de los derechos de acceso asignados a usuarios. (9.2.2)*
    - El DST deberá asignar derechos de acceso a recursos informáticos, a los usuarios que lo soliciten, previa autorización del Jefe inmediato o máxima autoridad.
    - El DST procederá a revocar derechos de acceso a recursos informáticos, cuando sea solicitado por el jefe inmediato o máxima autoridad.

- *Revisión de los derechos de acceso de los usuarios. (9.2.5)*
    - El DST procederá a revisar los derechos de acceso a los recursos informáticos al término de cada semestre o después de que un usuario haya cambiado de lugar de trabajo o funciones, para evitar que existan privilegios sin autorización.
    - El DST al final de cada semestre procederá a revisar los derechos de acceso a los recursos informáticos con el fin de revocarlos según los siguientes casos:
        - Usuario que se desvinculen de la institución.
        - Usuario no tiene tareas relacionadas con el recurso informático asociado.
        - Petición de máxima autoridad o Jefe inmediato.

Responsabilidades del usuario. (9.3)

Controles aplicados:

- *Uso de información confidencial para la autenticación. (9.3.1)*
  - Los usuarios de los recursos informáticos y de los sistemas que administra el DST, deberán usarlo adecuadamente de forma responsable, salvaguardando la información a la cual se les ha permitido acceder.
  - Los usuarios de los recursos informáticos, servicios de red y los sistemas que administra el DST deben hacerse responsables de las acciones realizadas sobre estos, así como el uso de las credenciales asignadas para el acceso de los mismos.
  - Los usuarios no deben compartir sus cuentas de usuario y contraseñas con otros.
  - En el caso de los estudiantes podrán crear su cuenta y registrar su contraseña desde el sitio web de la FIEC, siempre que sean estudiantes de la FIEC y posean la cuenta en ESPOL.

- En el caso de los docentes y administrativos, deben tener cuenta de ESPOL para proceder a solicitar la cuenta de FIEC.

Control de acceso a sistemas y aplicaciones. (9.4)

Controles aplicados:

- *Restricción del acceso a la información. (9.4.1)*
  - El DST restringe el acceso a recursos informáticos y sistemas de acuerdo con al grupo de usuario al que pertenece, necesidad de uso y/o bajo autorización de máxima autoridad o jefe inmediato.
  - El DST es responsable de la administración de los sistemas informáticos, por lo tanto velará para que estos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico. Además, velará que los desarrolladores, se acojan a buenas prácticas de desarrollo en lo que corresponde al acceso lógico y evitar accesos no autorizados a los sistemas administrados.

- *Control de acceso al código fuente de los programas. (9.4.5)*

- El DST asignará acceso al código fuente de los sistemas que se desarrollan al Asistente técnico de desarrollo.
- El acceso debe restringir acceso a equipos que no sean de uso del Asistente Técnico de desarrollo.
- El DST debe establecer ambientes separados para desarrollo (pruebas y producción), tanto a nivel físico como lógico, procurando que las actividades de desarrollo y pruebas no pongan en riesgo la integridad de la información que se encuentra en ambiente de producción.
- El DST debe proporcionar repositorios para mantener los archivos fuente de los sistemas informáticos, los cuales contaran con control de acceso.

Desarrollo

- El DST asegurará que los sistemas informáticos que se desarrollen requieran autenticación, excepto aquellas que son considerados de acceso público.
- El DST asegurará que no se almacenen contraseñas, cadenas de conexión u otra información sensible en texto plano.
- El DST deberá establecer controles de autenticación de tal forma que cuando fallen, deben evitar especificar cuál

fue la falla durante el proceso de autenticación y, en su lugar, deberá mostrar un mensaje general de falla.

- El Asistente Técnico de Desarrollo del DST, debe asegurar que los sistemas informáticos no muestren en pantalla las contraseñas ingresadas.
- El Asistente Técnico de Desarrollo del DST, debe certificar que los mensajes de fallo no muestren información relacionada con el servidor, ip. Versiones de sistemas o software.
- El Asistente Técnico de Desarrollo del DST, deben asegurar acceso a archivos u otros recursos, direcciones URL protegidas, a funciones protegidas, servicios, información de los sistemas, configuración, solamente a usuarios autorizados.

V. De la Seguridad Física y ambiental.

Áreas seguras. (11.1)

- EL DST velará por que se cumplan los procedimientos de seguridad física y control de acceso que aseguren el perímetro de las instalaciones de red y servidores. Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de los centro de datos.

- Se consideran áreas de acceso restringido a todas las áreas que son destinadas para el procesamiento o almacenamiento de información sensible/crítica, así como en las que se encuentran equipos y demás infraestructura de soporte a los sistemas informáticos y red de comunicaciones.

Controles aplicados:

- *Perímetro de seguridad física. (11.1.1)*
  - El DST, define como perímetro de seguridad la delimitación de una pared y puerta con acceso controlado al menos por una llave o sistema de control de acceso a los centros de datos/cableado.
  - El DST, mantendrá a equipos que realizan procesamiento de información o equipos de enrutamiento dentro del perímetro de un edificio o área de construcción sólida y las puertas que comuniquen con el exterior deben estar protegidas contra accesos no autorizados, al menos por una cerradura en el caso que se encuentren en el Edificio 16-C

- El DST mantendrá identificado la Salida de Emergencia en caso de escenarios catastróficos dentro del área donde se encuentre el centro de datos principal.

- *Controles físicos de entrada. (11.1.2)*
  - Los centros de cableado y cómputo (cuarto de servidores) deben contar con mecanismos de control de acceso tales como puertas de seguridad, cerradura, sistemas de control de acceso con tarjetas y sistema de alarmas.
  - El ingreso de terceros a los Centros de cableado y cómputo (cuarto de servidores), debe estar debidamente registrado mediante una bitácora ubicada en la entrada de estos lugares de forma visible.
  - Las solicitudes de acceso al centro de cómputo (cuarto de servidores) o a los centros de cableado deben ser notificadas al Jefe del DST para autorizar el acceso y que al menos una persona del DST esté presente durante la visita en los lugares señalados anteriormente.
  - El DST, debe modificar de manera inmediata los privilegios de acceso físico al centro de cómputo (cuarto de servidores) o a los centros de cableado que

administra, a quien tenga autorizado el ingreso pero se desvincule o cambie de labores.

Seguridad de Las Oficinas

- Personal del DST, administrativos y docentes deberán mantener los puestos de trabajo limpios y sin documentos importantes fuera del horario de trabajo o en ausencia prolongada de su puesto, con el fin de evitar el acceso no autorizado a la información y equipos.
- Personal del DST, administrativos y docentes deben colocar las pantallas de sus computadores en una posición en la que evite que personal no autorizado pueda visualizar información importante.
- Todos los usuarios son responsables de bloquear la sesión de su equipo de trabajo en el momento en que no se encuentren en su puesto de trabajo, la cual podrá desbloquear con su contraseña.
- Todos los usuarios cuando finalicen la jornada de trabajo/actividades, debe dejar sus equipos de trabajo apagados.

- Todos los usuarios, deben evitar dejar olvidado en las impresoras información importante/confidencial, una vez que hayan sido impresas.

- *Protección contra las amenazas externas y ambientales. (11.1.4)*
  - Los centros de cableado, cómputo (cuarto de servidores), laboratorios de computación deben contar con sistemas de alarmas y cámaras de seguridad, sistema de detección de fuego y extintores.
  - Los equipos deben mantenerse ubicados en un buen lugar, aislándolos de amenazas como fuego, agua, vibración, polvo, interferencia electromagnética y vandalismo, etc.
  - Los centros de cableado, cómputo (cuarto de servidores), laboratorios de computación deben estar climatizados y mantener los niveles de temperatura y humedad dentro de los límites requeridos por la infraestructura informática instalada.
  - No se permite comer, beber y fumar dentro de las instalaciones de los centros de cableado, cómputo (cuarto de servidores), laboratorios de computación.

- Personal del DST deber monitorear las condiciones físicas y medioambientales de forma continua en los centros de cableado, cómputo (cuarto de servidores) y laboratorios de computación, con el fin de asegurar la protección y correcta operación de infraestructura informática que administra
- El DST debe asegurar que las trabajos de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal competente y autorizado; de igual forma, se debe llevar control de la planificación de los mantenimientos preventivos.
- Los equipos auxiliares tales como cintas magnéticas, discos duros de respaldo, etc. deben ser ubicados en lugares seguros para evitar que sufran daños ambientales.

Seguridad de los equipos. (11.2)

o En caso de pérdida o robo de un equipo informático, se debe reportar al DST para que as u vez se informe a la máxima autoridad y se inicie el trámite interno correspondiente, el cual consiste en poner la denuncia ante

la autoridad competente por parte del custodio de la facultad.

Controles aplicados:

- *Instalaciones de suministro. (11.2.2)*
    - Los centros de datos deberán disponer de múltiples tomas de corrientes para evitar un único punto de falla en el suministro de energía.
    - Los centros de datos deben contar con sistema de suministro de energía ininterrumpiere (UPS) para asegurar el apagado regulado.
    - Los equipos de UPS serán inspeccionados y probados al menos una vez al año para asegurar que funcionen correctamente y que tengan la autonomía requerida que es de 30 minutos.

- *Seguridad del cableado. (11.2.3)*
    - El cableado de red que se encuentra en laboratorios y centro de datos, deberá de tener acceso restringido.
    - En el caso de que un área requiera de cableado estructurado deberá cumplir mínimo el estándar ANSI/TIA/EIA-568-B.2-1.

- Los puntos de red deben estar etiquetados.

- *Mantenimiento de los equipos. (11.2.4)*
  - El DST debe realizar mantenimientos preventivos y correctivos de los recursos informáticos de la FIEC para asegurar su disponibilidad e integridad, teniendo en cuenta lo siguiente:
    - Se realizarán 2 mantenimientos preventivos en el año en lo que refiere a los Laboratorios de computación de la FIEC.
    - Se realizará 1 mantenimiento preventivo en el año en los centros de datos y servidores.
    - Sólo el personal del DST está autorizado para realizar el mantenimiento, retirarlo y llevar a cabo reparaciones o cambios de partes de los equipos.
    - El personal del DST, registrarán las fallas supuestas o reales y además llevará un registro de instalación, registro del mantenimiento preventivo y correctivo realizado.
    - La información que se encuentre en los equipos que se retiren de alguna oficina o laboratorio, se tendrá

que realizar una copia de respaldo en caso de que éste requiera ser formateado.

- Cuando un equipo presente una falla/problema de hardware o software, el usuario responsable debe informar al DST a través del CRM, correo o teléfono, con el fin de realizar una asistencia adecuada.
- El mantenimiento que corresponde a equipamiento auxiliar debe ser solicitado a la persona encargada de la FIEC al menos 2 veces en el año.

- *Salida de activos fuera de las dependencias de la empresa. (11.2.5)*
  - Si un equipo sale de las instalaciones de la FIEC, deberá ser previa autorización de la máxima autoridad y bajo la responsabilidad del solicitante del equipo, mediante un acta de entrega/recepción del mismo.

- *Reutilización o retirada segura de dispositivos de almacenamiento. (11.2.7)*
  - El DST debe asegurar que los equipos que entrega no deben contener instaladores o licencias que puedan verse comprometidas.

- Los equipos que tienen conteniendo/información sensible serán formateados, sobrescritos o destruidos, según sea el medio de almacenamiento, con el fin de no comprometer información sensible cuando ese equipo sea retirado o reubicado. Ver Procedimiento de cambio de equipo o reubicación.

- *Equipo informático de usuario desatendido. (11.2.8)*
  - Los equipos informáticos requieren una protección contra accesos no autorizados cuando se encuentran desatendidos, por lo que los usuarios deben cumplir con las siguientes pautas:
    - Cerrar las sesiones activas al finalizar sus tareas.
    - Proteger las estaciones de trabajo contra usos/accesos no autorizados mediante un bloqueo de seguridad, por ejemplo, contraseña de acceso cuando no se utilizan.
  - Los equipos informáticos, no deben ser dejados desatendidos en lugares públicos o a la vista, en el caso de que estén siendo movilizados.

- *Política de puesto de trabajo despejado y bloqueo de pantalla*. (11.2.9)
    - Los usuarios deben almacenar bajo llave, o según corresponda, los documentos en papel y los medios informáticos de almacenamiento, que sean considerados de tipo crítico o sensible, en un mobiliario seguro cuando estos no estén siendo utilizados.
    - Los equipos informáticos que se han asignados deben ser protegidos mediante contraseñas u otros controles cuando no están en uso, por ejemplo, utilización de protectores de pantalla con contraseña o bloqueo de pantalla.
    - Retirar de la impresora documentos con información sensible o confidencial, una vez que han sido impresos.

VI. De la Seguridad en la Operativa

Responsabilidades y procedimientos de operación. (12.1)

- El DST proporcionará manuales de configuración y operación relacionados con la administración de la infraestructura informática (sistemas, servicios de red, bases de datos) al personal que conforma el departamento de acuerdo a sus funciones.

- El DST deberá realizar una estimación de los recursos informáticos que se necesitan de acuerdo a la demanda y crecimiento de la facultad, con el fin de asegurar el correcto desempeño, ya sea en lo referente a ancho de banda, equipos informáticos, suministros y repuestos.

Controles aplicados:

- *Documentación de procedimientos de operación. (12.1.1)*
  - El DST es responsable de documentar y mantener actualizados los procedimientos operativos que se han identificados en esta Política.
  - El responsable de las redes y servidores deberá disponer de documentación sobre procedimientos relacionados con el puesto.
  - El responsable de los sistemas informáticos deberá disponer de documentación sobre procedimientos relacionados con las actividades del puesto.
  - El responsable de soporte técnico deberá disponer de documentación sobre procedimientos relacionados con las actividades que realiza el puesto.

- *Gestión de cambios. (12.1.2)*

- El DST definirá el procedimiento de control cambios para la parte operativa, de comunicaciones y de desarrollo, es decir, que dicho cambio deberá ser evaluado previamente en lo relacionado con aspectos técnicos y de seguridad, con el fin de que no afecte la seguridad de la infraestructura informática.

Protección contra código malicioso. (12.2)

Control aplicado:

- *Controles contra el código malicioso. (12.2.1)*
  - El DST proveerá de mecanismos para ayudar a garantizar la protección de la información y los recursos informáticos que administra, aplicando controles para evitar la divulgación, modificación o daño que pueden ser ocasionados por el contagio de software malicioso.
  - Todos los equipos informáticos que son administrados por el DST deberán tener instalado el antivirus institucional, actualizado, con licencia y configurado con la política del antivirus.
  - El DST asegurará que la información almacenada en la plataforma tecnológica será escaneada por el antivirus,

incluyendo la información que es transmitida por correo electrónico.

- El DST configurará con contraseña el acceso al antivirus para evitar que usuarios puedan modificarlo.
- El DST debe asegurar que los equipos informáticos que administra tengan instalada la última versión del software antivirus y actualizaciones del sistema operativo.
- EL DST deberá revisar periódicamente los servidores con el fin de prevenir contagios de virus informáticos.

o Los usuarios que hagan uso de equipos que no poseen inventario de ESPOL, deberán tener instalado un antivirus, para mitigar las vulnerabilidades.

o Los usuarios no pueden instalar antivirus adicionales o intentar cambiar la configuración del software de antivirus institucional en equipos con inventario de ESPOL.

o .Los usuarios deberán escanear todas las unidades de almacenamiento que se conecten al equipo que se les ha asignado.

o Los usuarios deben asegurarse que los archivos adjuntos de los correos electrónicos, archivos descargados de internet o que han sido copiados de un medio de

almacenamiento sean escaneados con el fin de evitar infección de virus informáticos.

- Los usuarios que detecten o sospechen de alguna infección por software malicioso deben notificar al DST, para que se tomen las medidas de control correspondientes.

Copias de seguridad. (12.3)

Control aplicado:

- *Copias de seguridad de la información. (12.3.1)*
  - El DST debe tener definido un procedimiento de respaldo de la información y datos críticos, con el fin preservar la integridad y disponibilidad de los mismos.
  - El DST deberá probar que las copias de respaldo que se han realizado funcionan correctamente, para comprobar su integridad.
  - El DST debe definir quién o quienes deben de realizar las copiar de seguridad, y según el caso, quien debe transportarlas.
  - El DST definirá repositorios para almacenar copias de respaldo.

- Los usuarios son responsables de identificar los datos críticos que deben ser respaldados, para incluirlos dentro de las copias de seguridad, siempre y cuando estén alojados dentro de los servidores de la facultad.

Registro de actividad y supervisión. (12.4)

Controles aplicados:

- *Registro y gestión de eventos de actividad. (12.4.1)*
  - El DST, realizará un monitoreo continuo de la red, servicios, sistemas y demás recursos informáticos, con el objetivo de asegurar que la infraestructura tecnológica funcione correctamente.
  - Los sistemas deberán generar logs de actividades de los usuarios y administradores, los mismos que deberán ser monitoreados en el caso de ocurrir algún evento que afecte los mismos.
  - Los servidores deberán generar logs de los sistemas y servicios que alojen, los mismos que deberán ser monitoreados periódicamente para evitar que afecten la disponibilidad e integridad de los mismos.
  - El personal del DST deberán registrar y documentar los eventos de los logs que afecten los sistemas y servicios.

- El Asistente Técnico de Desarrollo del DST, evitará guardar datos innecesarios de los sistemas y en los logs, solo deberá almacenar información estrictamente requerida.

- *Protección de los registros de información. (12.4.2)*
  - Los logs serán protegidos de que personas no autorizadas puedan revisarlos.
  - El administrador de servidores y redes podrá tener acceso a los logs de los servidores, equipos de red, bases de datos; y en el caso de los sistemas informáticos será el desarrollador.

- *Sincronización de relojes. (12.4.4)*
  - Con el objetivo de garantizar la exactitud de los registros y logs de accesos y demás eventos, los equipos que forman parte de la administración del DST, deberán tener configurados un servidor de reloj, en especial aquellos que almacenan registros.

Control del software en explotación. (12.5.1)

Controles aplicados:

- *Instalación del software en sistemas en sistemas operativos. (12.5.2)*
    - Los equipos de laboratorios deberán tener configuradas las políticas de seguridad definidas por el DST, con el objetivo de evitar que usuarios realicen instalaciones de software sin autorización.

Gestión de la vulnerabilidad técnica. (12.6)

Control aplicado:

- *Restricciones en la instalación de software. (12.6.1)*
    - Los usuarios deberán solicitar al DST instalación de software que tenga licencia o sea libre.
    - El DST no se hace responsable por software instalado y que no conste en los registros de instalación que se generan al momento de la entrega del equipo.

4.3 Definición de los Procedimientos

Los procedimientos considerados importantes que se definen en este esquema de seguridad son los siguientes:

- ✓ Procedimiento de eliminación de soportes.
- ✓ Procedimiento para gestionar usuarios y privilegios.

- ✓ Procedimiento de cambio de equipo o reubicación
- ✓ Procedimiento de respaldo de la información y datos críticos
- ✓ Procedimiento de revisión estado de servidores y red.
- ✓ Procedimiento de mantenimiento de equipos.
- ✓ Procedimiento de control cambios.

Ver anexo K.

4.4 Difusión de la Política

El propósito de este documento es dar a conocer el esquema de seguridad que está conformado por la política de seguridad y procedimientos. Para poder difundirla se ha determinado que a través del correo y sitio web de la Facultad es la forma de llegar a que tengan conocimiento de la misma. Adicionalmente al personal nuevo que ingresa a laborar en la facultad se le facilitará la política, todo esto para lograr que dentro de la FIEC se forme una cultura de seguridad de informática.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones:

1. Después de realizar el análisis de la situación actual que presenta el DST, se puede concluir que dentro de las tareas que realizan, no contemplan tareas de seguridad informática relacionas con la infraestructura que administran, al igual que las actividades que involucren seguridad informática no se encuentran definidas dentro de las funciones del personal que labora en el departamento.

2. A partir de la identificación de los activos que administra el DST, se pudieron detectar las amenazas a los que están expuestos con la ayuda de la metodología Magerit, obteniendo como resultado que casi todos los activos presentan un nivel de riesgo.

3. El activo que corresponde a las redes de comunicaciones LAN es el que se demuestra estar más afectado, debido al alto nivel de riesgo que presentaron las amenazas que se definieron para ese activo, sin

embargo, se espera que los controles que se usaron para definir la política de seguridad ayuden reducir dicho riesgo.

4. Basados en los resultados del análisis de riesgo de los activos que administra el DST, se realizó el diseño de un esquema de seguridad de informática, el cual está conformado por políticas y controles seleccionados de la norma ISO 27002. Los dominios que se consideraron para este diseño fueron: Aspectos organizativos de la seguridad de la información, Gestión de activos, Control de Accesos, Seguridad Física y Ambiental y Seguridad en la operativa, abarcando seguridad física y lógica.

5. A partir del desarrollo de esta tesis se identificaron riesgos en activos que antes no se consideraban tan relevantes como es el caso de las herramientas para dar soporte, base datos del crm, entre otras, los que fueron evaluados con un valor medio en las dimensiones de seguridad, elevando así la importancia que constituyen todos los activos y la necesidad de definir controles que minimícenlos riesgos a los que pueden estar expuestos.

6. La difusión de la política dentro del DST ayuda a mejorar el manejo de los incidentes de seguridad que se presenten y proyecta evitar que dichas eventualidades ocurran nuevamente, aplicando controles y procedimientos definidos en dicha política.

7. Los documentos resultantes son específicos para la FIEC y representan una primera fase de controles y procedimientos que se definen en el DST para gestionar la seguridad. Uno de los documentos más importantes definidos es el de los roles y responsabilidades para cada uno de los integrantes del DST en lo que a seguridad informática se refiere.

8. Actualmente la tecnología permite a los usuarios acceder desde cualquier parte a un sistema informático, por lo que la seguridad informática juega un rol muy importante, es decir, que no se debe dejar sin monitorear o desatendidos aquellos activos que no presentaron un riesgo puesto que siempre existe un nivel de riesgo.

Recomendaciones:

1. En futuros trabajos o modificaciones a esta política, se debe contemplar controles que no se consideraron en el alcance de esta tesis.

2. El personal del DST debería ser capacitado en las áreas donde se presenta mayor riesgo como en el caso de los activos relacionados con la red de comunicaciones.

3. El DST debería realizar capacitaciones al personal administrativo y docente acerca de las amenazas a las que podrían estar expuestos y contemplar el uso correcto de los sistemas, servicios y equipos que tienen a disposición.

BIBLIOGRAFÍA

[1] http://lema.rae.es/drae/srv/search?key=seguro, RAE, 2014

[2] http://lema.rae.es/drae/srv/search?key=inform%C3%A1tica, RAE, 2014

[3] Gollmann Dieter, Computer Security, Febrero 2011, página 39.

[4] Astudillo Karina, Hacking Ético 101, Septiembre 2013, pág. 8.

[5] Astudillo Karina, Hacking Ético 101, Septiembre 2013, pág. 189.

[6] http://www.27000.org/, 2013

[7] http://www.27000.org/iso-27002.htm, 2013

[8] Carmen de Pablos Heredero,José Joaquín López Hermoso Agius,Santiago Martín Romo Romero,Sonia Medina Salgado, Organización y transformación de los sistemas de información en la empresa, 2011, pág. 286-287.

[9] https://es.scribd.com/doc/36343741/Tabla-Comparativa-Magerit-Nist, 2012

[10] Ministerio de hacienda y administraciones públicas S. de E. de administraciones públicas dirección de tecnologías de la información y las comunicaciones, MAGERIT – versión 3.0, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Octubre 2012, pág. 22.

[11] Ministerio de hacienda y administraciones públicas S. de E. de administraciones públicas dirección de tecnologías de la información y las comunicaciones, MAGERIT – versión 3.0, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Octubre 2012, pág. 27.

[12] Ministerio de hacienda y administraciones públicas S. de E. de administraciones públicas dirección de tecnologías de la información y las comunicaciones, MAGERIT – versión 3.0, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Octubre 2012, pág. 31.

[13] Ministerio de hacienda y administraciones públicas S. de E. de administraciones públicas dirección de tecnologías de la información y las comunicaciones, MAGERIT – versión 3.0, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Octubre 2012, pág. 9.

[14] Ministerio de hacienda y administraciones públicas S. de E. de administraciones públicas dirección de tecnologías de la información y las comunicaciones, MAGERIT – versión 3.0, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Octubre 2012, pág. 22.

[15] Ministerio de hacienda y administraciones públicas S. de E. de administraciones públicas dirección de tecnologías de la información y las comunicaciones, MAGERIT – versión 3.0, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Octubre 2012, pág. 27.

[16] Ministerio de hacienda y administraciones públicas S. de E. de administraciones públicas dirección de tecnologías de la información y las comunicaciones, MAGERIT – versión 3.0, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Octubre 2012, pág. 31.

[17] Ministerio de hacienda y administraciones públicas S. de E. de administraciones públicas dirección de tecnologías de la información y las

comunicaciones, MAGERIT – versión 3.0, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Octubre 2012, pág. 31.

[18]https://www.blackhat.com/latestintel/07152015-attendee-survey.html, 2015 Black Hat Attendee Survey: Time to Rethink Enterprise IT Security, Julio 2015.

[19] https://business.kaspersky.com/it-security-risks-survey-2014-none-is-spared/2339/, Kaspersky Lab, It Security Risks Survey, A Business Approach To Managing Data Security Threats, 2014

[20] http://www.pwc.co.uk/services/audit-assurance/insights/2015-information-security-breaches-survey.html, Information Security Breaches Survey, 2015

ANEXO A

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.
5.1 Directrices de la Dirección en seguridad de la información.
5.1.1 Conjunto de políticas para la seguridad de la información.
5.1.2 Revisión de las políticas para la seguridad de la información.
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
6.1 Organización interna.
6.1.1 Asignación de responsabilidades para la segur. de la información.
6.1.2 Segregación de tareas.
6.1.3 Contacto con las autoridades.
6.1.4 Contacto con grupos de interés especial.
6.1.5 Seguridad de la información en la gestión de proyectos.
6.2 Dispositivos para movilidad y teletrabajo.
6.2.1 Política de uso de dispositivos para movilidad.
6.2.2 Teletrabajo.
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
7.1 Antes de la contratación.
7.1.1 Investigación de antecedentes.
7.1.2 Términos y condiciones de contratación.
7.2 Durante la contratación.
7.2.1 Responsabilidades de gestión.
7.2.2 Concienciación, educación y capacitación en segur. de la informac.
7.2.3 Proceso disciplinario.
7.3 Cese o cambio de puesto de trabajo.
7.3.1 Cese o cambio de puesto de trabajo.
8. GESTIÓN DE ACTIVOS.
8.1 Responsabilidad sobre los activos.
8.1.1 Inventario de activos.
8.1.2 Propiedad de los activos.
8.1.3 Uso aceptable de los activos.
8.1.4 Devolución de activos.
8.2 Clasificación de la información.
8.2.1 Directrices de clasificación.
8.2.2 Etiquetado y manipulado de la información.
8.2.3 Manipulación de activos.
8.3 Manejo de los soportes de almacenamiento.
8.3.1 Gestión de soportes extraíbles.
8.3.2 Eliminación de soportes.
8.3.3 Soportes físicos en tránsito.
9. CONTROL DE ACCESOS.
9.1 Requisitos de negocio para el control de accesos.
9.1.1 Política de control de accesos.
9.1.2 Control de acceso a las redes y servicios asociados.
9.2 Gestión de acceso de usuario.
9.2.1 Gestión de altas/bajas en el registro de usuarios.
9.2.2 Gestión de los derechos de acceso asignados a usuarios.
9.2.3 Gestión de los derechos de acceso con privilegios especiales.
9.2.4 Gestión de información confidencial de autenticación de usuarios.
9.2.5 Revisión de los derechos de acceso de los usuarios.
9.2.6 Retirada o adaptación de los derechos de acceso
9.3 Responsabilidades del usuario.
9.3.1 Uso de información confidencial para la autenticación.
9.4 Control de acceso a sistemas y aplicaciones.
9.4.1 Restricción del acceso a la información.
9.4.2 Procedimientos seguros de inicio de sesión.
9.4.3 Gestión de contraseñas de usuario.
9.4.4 Uso de herramientas de administración de sistemas.
9.4.5 Control de acceso al código fuente de los programas.
10. CIFRADO.
10.1 Controles criptográficos.
10.1.1 Política de uso de los controles criptográficos.
10.1.2 Gestión de claves.
11. SEGURIDAD FÍSICA Y AMBIENTAL.
11.1 Áreas seguras.
11.1.1 Perímetro de seguridad física.
11.1.2 Controles físicos de entrada.
11.1.3 Seguridad de oficinas, despachos y recursos.
11.1.4 Protección contra las amenazas externas y ambientales.
11.1.5 El trabajo en áreas seguras.
11.1.6 Áreas de acceso público, carga y descarga.
11.2 Seguridad de los equipos.
11.2.1 Emplazamiento y protección de equipos.
11.2.2 Instalaciones de suministro.
11.2.3 Seguridad del cableado.
11.2.4 Mantenimiento de los equipos.
11.2.5 Salida de activos fuera de las dependencias de la empresa.
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
11.2.8 Equipo informático de usuario desatendido.
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.
12. SEGURIDAD EN LA OPERATIVA.
12.1 Responsabilidades y procedimientos de operación.
12.1.1 Documentación de procedimientos de operación.
12.1.2 Gestión de cambios.
12.1.3 Gestión de capacidades.
12.1.4 Separación de entornos de desarrollo, prueba y producción.
12.2 Protección contra código malicioso.
12.2.1 Controles contra el código malicioso.
12.3 Copias de seguridad.
12.3.1 Copias de seguridad de la información.
12.4 Registro de actividad y supervisión.
12.4.1 Registro y gestión de eventos de actividad.
12.4.2 Protección de los registros de información.
12.4.3 Registros de actividad del administrador y operador del sistema.
12.4.4 Sincronización de relojes.
12.5 Control del software en explotación.
12.5.1 Instalación del software en sistemas en producción.
12.6 Gestión de la vulnerabilidad técnica.
12.6.1 Gestión de las vulnerabilidades técnicas.
12.7 Consideraciones de las auditorías de los sistemas de información.
12.7.1 Controles de auditoría de los sistemas de información.
13. SEGURIDAD EN LAS TELECOMUNICACIONES.
13.1 Gestión de la seguridad en las redes.
13.1.1 Controles de red.
13.1.2 Mecanismos de seguridad asociados a servicios en red.
13.1.3 Segregación de redes.
13.2 Intercambio de información con partes externas.
13.2.1 Políticas y procedimientos de intercambio de información.
13.2.2 Acuerdos de intercambio.
13.2.3 Mensajería electrónica.
13.2.4 Acuerdos de confidencialidad y secreto.
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
14.1 Requisitos de seguridad de los sistemas de información.
14.1.1 Análisis y especificación de los requisitos de seguridad.
14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
14.1.3 Protección de las transacciones por redes telemáticas.
14.2 Seguridad en los procesos de desarrollo y soporte.
14.2.1 Política de desarrollo seguro de software.
14.2.2 Procedimientos de control de cambios en los sistemas.
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
14.2.4 Restricciones a los cambios en los paquetes de software.
14.2.5 Uso de principios de ingeniería en protección de sistemas.
14.2.6 Seguridad en entornos de desarrollo.
14.2.7 Externalización del desarrollo de software.
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
14.2.9 Pruebas de aceptación.
14.3 Datos de prueba.
14.3.1 Protección de los datos utilizados en pruebas.
15. RELACIONES CON SUMINISTRADORES.
15.1 Seguridad de la información en las relaciones con suministradores.
15.1.1 Política de seguridad de la información para suministradores.
15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
15.2 Gestión de la prestación del servicio por suministradores.
15.2.1 Supervisión y revisión de los servicios prestados por terceros.
15.2.2 Gestión de cambios en los servicios prestados por terceros.
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
16.1 Gestión de incidentes de seguridad de la información y mejoras.
16.1.1 Responsabilidades y procedimientos.
16.1.2 Notificación de los eventos de seguridad de la información.
16.1.3 Notificación de puntos débiles de la seguridad.
16.1.4 Valoración de eventos de seguridad de la información y toma

ANEXO B

TIPOS DE ACTIVOS QUE DEFINE MAGERIT

[arch] Arquitectura del sistema
[sap] punto de [acceso al] servicio [ip] punto de interconexión [ext] proporcionado por terceros
[D] Datos / Información
[source] código fuente [exe] código ejecutable [test] datos de prueba
[keys] Claves criptográficas
[info] protección de la información [encrypt] claves de cifra [shared_secret] secreto compartido (clave simétrica) [public_encryption] clave pública de cifra [public_decryption] clave privada de descifrado [sign] claves de firma [shared_secret] secreto compartido (clave simétrica) [public_signature] clave privada de firma [public_verification] clave pública de verificación de firma [com] protección de las comunicaciones [channel] claves de cifrado del canal [authentication] claves de autenticación [verification] claves de verificación de autenticación [disk] cifrado de soportes de información [encrypt] claves de cifra [x509] certificados de clave pública
[S] Servicios
[anon] anónimo (sin requerir identificación del usuario) [pub] al público en general (sin relación contractual) [ext] a usuarios externos (bajo una relación contractual) [int] interno (a usuarios de la propia organización) [www] world wide web [telnet] acceso remoto a cuenta local [email] correo electrónico [file] almacenamiento de ficheros [ftp] transferencia de ficheros [edi] intercambio electrónico de datos [dir] servicio de directorio [idm] gestión de identidades [ipm] gestión de privilegios [pki] PKI - infraestructura de clave pública
[SW] Aplicaciones (software)
[prp] desarrollo propio (in house) [sub] desarrollo a medida (subcontratado) [std] estándar (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 [file] servidor de ficheros [dbms] sistema de gestión de bases de datos [tm] monitor transaccional [office] ofimática

[av] anti virus [os] sistema operativo
[hypervisor] gestor de máquinas virtuales
[ts] servidor de terminales
[backup] sistema de backup

[HW] Equipos informáticos (hardware)

[host] grandes equipos
[mid] equipos medios
[pc] informática personal
[mobile] informática móvil
[pda] agendas electrónicas
[vhost] equipo virtual
[backup] equipamiento de respaldo
[peripheral] periféricos
[print] medios de impresión
[scan] escáneres
[crypto] dispositivos criptográficos
[bp] dispositivo de frontera
[network] soporte de la red
[modem] módems
[hub] concentradores
[switch] conmutadores
[router] encaminadores
[bridge] pasarelas
[firewall] cortafuegos
[wap] punto de acceso inalámbrico
[pabx] centralita telefónica
[ipphone] teléfono IP

[COM] Redes de comunicaciones

[PSTN] red telefónica
[ISDN] rdsi (red digital)
[X25] X25 (red de datos)
[ADSL] ADSL
[pp] punto a punto
[radio] comunicaciones radio
[wifi] red inalámbrica
[mobile] telefonía móvil
[sat] por satélite
[LAN] red local
[MAN] red metropolitana [Internet] Internet

[Media] Soportes de información

[electronic] electrónicos
[disk] discos
[vdisk] discos virtuales
[san] almacenamiento en red
[disquette] disquetes
[cd] cederrón (CD-ROM)
[usb] memorias USB
[dvd] DVD
[tape] cinta magnética
[mc] tarjetas de memoria
[ic] tarjetas inteligentes
[non_electronic] no electrónicos
[printed] material impreso
[tape] cinta de papel
[film] microfilm
[cards] tarjetas perforadas

[AUX] Equipamiento auxiliar

[power] fuentes de alimentación
[ups] sistemas de alimentación ininterrumpida
[gen] generadores eléctricos
[ac] equipos de climatización
[cabling] cableado
[wire] cable eléctrico
[fiber] fibra óptica
[robot] robots
[tape] ... de cintas
[disk] ... de discos
[supply] suministros esenciales
[destroy] equipos de destrucción de soportes de información
[furniture] mobiliario: armarios, etc
[safe] cajas fuertes

[L] Instalaciones

[site] recinto
[building] edificio
[local] cuarto
[mobile] plataformas móviles
[car] vehículo terrestre: coche, camión, etc.
[plane] vehículo aéreo: avión, etc.
[ship] vehículo marítimo: buque, lancha, etc.
[shelter] contenedores
[channel] canalización
[backup] instalaciones de respaldo

[P] Personal

[ue] usuarios externos
[ui] usuarios internos
[op] operadores
[adm] administradores de sistemas
[com] administradores de comunicaciones
[dba] administradores de BBDD
[sec] administradores de seguridad
[des] desarrolladores / programadores
[sub] subcontratas
[prov] proveedores

ANEXO C

AMENAZAS QUE DEFINE MAGERIT

	AMENAZAS	[D]	[I]	[C]
DATOS	[E.1] Errores de los usuarios	x	x	x
	[E.2] Errores del administrador	x	x	x
	[E.3] Errores de monitorización (log)		x	
	[E.4] Errores de configuración		x	
	[E.14] Escapes de información			x
	[E.15] Alteración accidental de la información		x	
	[E.18] Destrucción de información	x		
	[E.19] Fugas de información			x
	[A.3] Manipulación de los registros de actividad (log)		x	
	[A.4] Manipulación de la configuración	x	x	x
	[A.5] Suplantación de la identidad del usuario	x	x	x
	[A.6] Abuso de privilegios de acceso	x	x	x
	[A.8] Difusión de software dañino (virus, spyware, troyanos, gusanos, etc)	x	x	x
	[A.11] Acceso no autorizado		x	x
	[A.12] Análisis de tráfico			
	[A.13] Repudio		x	
	[A.15] Modificación deliberada de la información		x	
	[A.18] Destrucción de información	x		
	[A.19] Divulgación de información			x
SERVICIOS	[E.1] Errores de los usuarios	x	x	x
	[E.2] Errores del administrador	x	x	x
	[E.19] Fugas de información			x
	[E.9] Errores de [re-]encaminamiento		x	
	[E.24] Caída del sistema por agotamiento de recursos	x		
	[A.5] Suplantación de la identidad del usuario	x	x	x
	[A.6] Abuso de privilegios de acceso	x	x	x
	[A.7] Uso no previsto	x	x	x
	[A.9] [Re-]encaminamiento de mensajes			x
	[A.10] Alteración de secuencia		x	
	[A.11] Acceso no autorizado			x
	[A.13] Repudio		x	
	[A.15] Modificación deliberada de la información		x	
	[A.18] Destrucción de información	x		
	[A.19] Divulgación de información			x
	[A.24] Denegación de servicio	x		

SOFTWARE	[I.5] Avería de origen físico o lógico	x		
	[E.1] Errores de los usuarios	x	x	x
	[E.2] Errores del administrador	x	x	x
	[E.8] Difusión de Software dañino	x	x	x
	[E.19] Fugas de información			x
	[E.9] Errores de [re-]encaminamiento		x	
	[E.19] Fugas de información			x
	[E.20] Vulnerabilidades de los programas (software)	x	x	x
	[E.21] Errores de mantenimiento / actualización de programas (software)	x	x	
	[A.5] Suplantación de la identidad del usuario	x	x	x
	[A.6] Abuso de privilegios de acceso	x	x	x
	[A.7] Uso no previsto	x	x	x
	[A.8] Difusión de software dañino (virus, spyware, troyanos, gusanos, etc)	x	x	x
	[A.9] [Re-]encaminamiento de mensajes			x
	[A.10] Alteración de secuencia		x	
	[A.11] Acceso no autorizado	x		
	[A.15] Modificación deliberada de la información		x	
	[A.18] Destrucción de información	x		
	[A.19] Divulgación de información			x
	[A.22] Manipulación de programas	x	x	x
HARDWARE	[N.1]Fuego	x		
	[N.2] Daños por agua	x		
	[I.1] Fuego	x		
	[I.2] Daños por agua	x		
	[I.*] Desastres industriales	x		
	[I.3] Contaminación mecánica	x		
	[I.4] Contaminación electromagnética	x		
	[I.5] Avería de origen físico o lógico	x		
	[I.6] Corte de suministro eléctrico	x		
	[I.7] Condiciones inadecuadas de temperatura o humedad	x		
	[E.2] Errores del administrador	x	x	x
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	x		
	[E.25] Pérdida de equipos	x		x
	[A.6] Abuso de privilegios de acceso	x	x	x
	[A.7] Uso no previsto	x	x	x
	[A.11] Acceso no autorizado		x	x
	[A.23] Manipulación de los equipos	x	x	x

	[A.24] Denegación de servicio	x		
	[A.25] Robo	x		x
	[A.26] Ataque destructivo	x		
MEDIA	[N.1]Fuego	x		
	[N.2] Daños por agua	x		
	[I.1] Fuego	x		
	[I.2] Daños por agua	x		
	[I.*] Desastres industriales	x		
	[I.3] Contaminación mecánica	x		
	[I.4] Contaminación electromagnética	x		
	[I.5] Avería de origen físico o lógico	x		
	[I.6] Corte de suministro eléctrico	x		
	[I.7] Condiciones inadecuadas de temperatura o humedad	x		
	[I.10] Degradación de los soportes de almacenamiento de información	x		
	[E.1] Errores de los usuarios	x	x	x
	[E.2] Errores del administrador	x	x	x
	[E.19] Fugas de información			x
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	x		
	[E.24] Caída del sistema por agotamiento de recursos			
	[E.25] Pérdida de equipos	x		x
	[A.7] Uso no previsto	x	x	x
	[A.11] Acceso no autorizado		x	x
	[A.15] Modificación deliberada de la información		x	
	[A.18] Destrucción de información	x		
	[A.19] Divulgación de información			x
	[A.25] Robo	x		x
	[A.26] Ataque destructivo	x		
AUXILIARES	[N.1]Fuego	x		
	[N.2] Daños por agua	x		
	[I.1] Fuego	x		
	[I.2] Daños por agua	x		
	[I.*] Desastres industriales	x		
	[I.3] Contaminación mecánica	x		
	[I.4] Contaminación electromagnética	x		
	[I.5] Avería de origen físico o lógico	x		
	[I.6] Corte de suministro eléctrico	x		
	[I.7] Condiciones inadecuadas de temperatura o humedad	x		
	[I.9] Interrupción de otros servicios y suministros esenciales	x		

	[E.2] Errores del administrador	x	x	x
	[E.19] Fugas de información			x
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	x		
	[E.24] Caída del sistema por agotamiento de recursos			
	[E.25] Pérdida de equipos	x		x
	[A.7] Uso no previsto	x	x	x
	[A.11] Acceso no autorizado		x	x
	[A.25] Robo	x		x
	[A.26] Ataque destructivo	x		
INSTALACIONES	[N.1]Fuego	x		
	[N.2] Daños por agua	x		
	[I.1] Fuego	x		
	[I.2] Daños por agua	x		
	[I.*] Desastres industriales	x		
	[E.19] Fugas de información			x
	[A.7] Uso no previsto	x	x	x
	[A.11] Acceso no autorizado		x	x
	[A.15] Modificación deliberada de la información		x	
	[A.18] Destrucción de información	x		
	[A.19] Divulgación de información			x
	[A.26] Ataque destructivo	x		
	[A.27] Ocupación enemiga	x		x
COMUNICACIONES	[E.19] Fugas de información			x
	[A.5] Suplantación de la identidad del usuario	x	x	x
	[A.6] Abuso de privilegios de acceso	x	x	x
	[A.9] [Re-]encaminamiento de mensajes			x
	[A.10] Alteración de secuencia		x	
	[A.11] Acceso no autorizado		x	x
	[A.12] Análisis de tráfico			x
	[A.14] Interceptación de información (escucha)			x
	[A.18] Destrucción de información	x		
	[A.19] Divulgación de información			x
	[A.24] Denegación de servicio	x		
PERSONAL	[E.7]Deficiencias en la organización	x		
	[E.19] Fugas de información			x
	[E.28] Indisponibilidad del personal	x		
	[A.28] Indisponibilidad del personal	x		
	[A.29] Extorsión	x	x	x
	[A.30] Ingeniería social (picaresca)	x	x	x

ANEXO D

SALVAGUARDAS QUE DEFINE MAGERIT

Protecciones generales u horizontales
H Protecciones Generales H.IA Identificación y autenticación H.AC Control de acceso lógico H.ST Segregación de tareas H.IR Gestión de incidencias H.tools Herramientas de seguridad H.tools.AV Herramienta contra código dañino H.tools.IDS IDS/IPS: Herramienta de detección / prevención de intrusión H.tools.CC Herramienta de chequeo de configuración H.tools.VA Herramienta de análisis de vulnerabilidades H.tools.TM Herramienta de monitorización de tráfico H.tools.DLP DLP: Herramienta de monitorización de contenidos H.tools.LA Herramienta para análisis de logs H.tools.HP Honey net / honey pot H.tools.SFV Verificación de las funciones de seguridad H.VM Gestión de vulnerabilidades H.AU Registro y auditoría
Protección de los datos / información
D Protección de la Información D.A Copias de seguridad de los datos (backup) D.I Aseguramiento de la integridad D.C Cifrado de la información D.DS Uso de firmas electrónicas D.TS Uso de servicios de fechado electrónico (time stamping)
Protección de las claves criptográficas
K Gestión de claves criptográficas K.IC Gestión de claves de cifra de información K.DS Gestión de claves de firma de información K.disk Gestión de claves para contenedores criptográficos K.comms Gestión de claves de comunicaciones K.509 Gestión de certificados
Protección de los servicios
S.A Aseguramiento de la disponibilidad S.start Aceptación y puesta en operación S.SC Se aplican perfiles de seguridad S.op Explotación S.CM Gestión de cambios (mejoras y sustituciones) S.end Terminación S.www Protección de servicios y aplicaciones web S.email Protección del correo electrónico S.dir Protección del directorio S.dns Protección del servidor de nombres de dominio (DNS) S.TW Teletrabajo S.voip Voz sobre IP
Protección de las aplicaciones (software)
SW Protección de las Aplicaciones Informáticas SW.A Copias de seguridad (backup) SW.start Puesta en producción SW.SC Se aplican perfiles de seguridad

SW.op Explotación / Producción SW.CM Cambios (actualizaciones y mantenimiento) SW.end Terminación
Protección de los equipos (hardware)
HW Protección de los Equipos Informáticos HW.start Puesta en producción HW.SC Se aplican perfiles de seguridad HW.A Aseguramiento de la disponibilidad HW.op Operación HW.CM Cambios (actualizaciones y mantenimiento) HW.end Terminación HW.PCD Informática móvil HW.print Reproducción de documentos HW.pabx Protección de la centralita telefónica (PABX)
Protección de las comunicaciones
COM Protección de las Comunicaciones COM.start Entrada en servicio COM.SC Se aplican perfiles de seguridad COM.A Aseguramiento de la disponibilidad COM.aut Autenticación del canal COM.I Protección de la integridad de los datos intercambiados COM.C Protección criptográfica de la confidencialidad de los datos intercambiados COM.op Operación COM.CM Cambios (actualizaciones y mantenimiento) COM.end Terminación COM.internet Internet: uso de ? acceso a COM.wifi Seguridad Wireless (WiFi) COM.mobile Telefonía móvil COM.DS Segregación de las redes en dominios
Protección en los puntos de interconexión con otros sistemas
IP Puntos de interconexión: conexiones entre zonas de confianza IP.SPP Sistema de protección perimetral IP.BS Protección de los equipos de frontera
Protección de los soportes de información
MP Protección de los Soportes de Información MP.A Aseguramiento de la disponibilidad MP.IC Protección criptográfica del contenido MP.clean Limpieza de contenidos MP.end Destrucción de soportes
Protección de los elementos auxiliares
AUX Elementos Auxiliares AUX.A Aseguramiento de la disponibilidad AUX.start Instalación AUX.power Suministro eléctrico AUX.AC Climatización AUX.wires Protección del cableado
Seguridad física – Protección de las instalaciones
L Protección de las Instalaciones L.design Diseño L.depth Defensa en profundidad L.AC Control de los accesos físicos L.A Aseguramiento de la disponibilidad L.end Terminación

Salvaguardas relativas al personal
PS Gestión del Personal PS.AT Formación y concienciación PS.A Aseguramiento de la disponibilidad
Salvaguardas de tipo organizativo
G Organización G.RM Gestión de riesgos G.plan Planificación de la seguridad G.exam Inspecciones de seguridad
Continuidad de operaciones
BC Continuidad del negocio BC.BIA Análisis de impacto (BIA) BC.DRP Plan de Recuperación de Desastres (DRP)

ANEXO E

CRITERIOS DE VALORIZACIÓN DE ACTIVOS DEFINIDOS EN MAGERIT

[pi] Información de carácter personal		
6	6.pi1	probablemente afecte gravemente a un grupo de individuos
	6.pi2	probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
5	5.pi1	probablemente afecte gravemente a un individuo
	5.pi2	probablemente quebrante seriamente leyes o regulaciones
4	4.pi1	probablemente afecte a un grupo de individuos
	4.pi2	probablemente quebrante leyes o regulaciones
3	3.pi1	probablemente afecte a un individuo
	3.pi2	probablemente suponga el incumplimiento de una ley o regulación
2	2.pi1	pudiera causar molestias a un individuo
	2.pi2	pudiera quebrantar de forma leve leyes o regulaciones
1	1.pi1	pudiera causar molestias a un individuo
[lpo] Obligaciones legales		
9	9.lro	probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
7	7.lro	probablemente cause un incumplimiento grave de una ley o regulación
5	5.lro	probablemente sea causa de incumplimiento de una ley o regulación
3	3.lro	probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
1	1.lro	pudiera causar el incumplimiento leve o técnico de una ley o regulación
[si] Seguridad		
10	10.si	probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios
9	9.si	probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
7	7.si	probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
3	3.si	probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
1	1.si	pudiera causar una merma en la seguridad o dificultar la investigación de un incidente
[cei] Intereses comerciales o económicos		
9	9.cei.a	de enorme interés para la competencia
	9.cei.b	de muy elevado valor comercial

	9.cei.c	causa de pérdidas económicas excepcionalmente elevadas
	9.cei.d	causa de muy significativas ganancias o ventajas para individuos u organizaciones
	9.cei.e	constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
7	7.cei.a	de alto interés para la competencia
	7.cei.b	de elevado valor comercial
	7.cei.c	causa de graves pérdidas económicas
	7.cei.d	proporciona ganancias o ventajas desmedidas a individuos u organizaciones
	7.cei.e	constituye un serio incumplimiento de obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
3	3.cei.a	de cierto interés para la competencia
	3.cei.b	de cierto valor comercial
	3.cei.c	causa de pérdidas financieras o merma de ingresos
	3.cei.d	facilita ventajas desproporcionadas a individuos u organizaciones
	3.cei.e	constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros
2	2.cei.a	de bajo interés para la competencia
	2.cei.b	de bajo valor comercial
1	1.cei.a	de pequeño interés para la competencia
	1.cei.b	de pequeño valor comercial
0	0.3	supondría pérdidas económicas mínimas
[da] Interrupción del servicio		
9	9.da	Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
	9.da2	Probablemente tenga un serio impacto en otras organizaciones
7	7.da	Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones
	7.da2	Probablemente tenga un gran impacto en otras organizaciones
5	5.da	Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones
	5.da2	Probablemente cause un cierto impacto en otras organizaciones
3	3.da	Probablemente cause la interrupción de actividades propias de la Organización
1	1.da	Pudiera causar la interrupción de actividades propias de la Organización
[po] Orden público		
9	9.po	alteración sería del orden público

6	6.po	probablemente cause manifestaciones, o presiones significativas
3	3.po	causa de protestas puntuales
1	1.po	pudiera causar protestas puntuales
[olm] Operaciones		
10	10.olm	Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
9	9.olm	Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
7	7.olm	Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
5	5.olm	Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local
3	3.olm	Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local)
1	1.olm	Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local)
[adm] Administración y gestión		
9	9.adm	probablemente impediría seriamente la operación efectiva de la Organización, pudiendo llegar a su cierre
7	7.adm	probablemente impediría la operación efectiva de la Organización
5	5.adm	probablemente impediría la operación efectiva de más de una parte de la Organización
3	3.adm	probablemente impediría la operación efectiva de una parte de la Organización
1	1.adm	pudiera impedir la operación efectiva de una parte de la Organización
[lg] Pérdida de confianza (reputación)		
9	9.lg.a	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con otras organizaciones
	9.lg.b	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con el público en general
7	7.lg.a	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con otras organizaciones
	7.lg.b	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general
5	5.lg.a	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con otras organizaciones
	5.lg.b	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con el público

3	3.lg	Probablemente afecte negativamente a las relaciones internas de la Organización
2	2.lg	Probablemente cause una pérdida menor de la confianza dentro de la Organización
1	1.lg	Pudiera causar una pérdida menor de la confianza dentro de la Organización
0	0.4	no supondría daño a la reputación o buena imagen de las personas u organizaciones
[**crm] Persecución de delitos**		
8	8.crm	Impida la investigación de delitos graves o facilite su comisión
4	4.crm	Dificulte la investigación o facilite la comisión de delitos
[rto] Tiempo de recuperación del servicio		
7	7.rto	RTO < 4 horas
4	4.rto	4 horas < RTO < 1 día
1	1.rto	1 día < RTO < 5 días
0	0.rto	5 días < RTO
[lbl.nat] Información clasificada (nacional)		
10	10.lbl	Secreto
9	9.lbl	Reservado
8	8.lbl	Confidencial
7	7.lbl	Confidencial
6	6.lbl	Difusión limitada
5	5.lbl	Difusión limitada
4	4.lbl	Difusión limitada
3	3.lbl	Difusión limitada
2	2.lbl	Sin clasificar
1	1.lbl	Sin clasificar

ANEXO F

DEPENDENCIAS ENTER ACTIVOS

	[D]	[S]	[SW]	[HW]	[COM]	[Media]	[AUX]	[L]	[P]
[bd_crm]		[servi_support]	[sis_crm]	[srv_db] [srv_web]	[wifi] [LAN]	[tape]			[adm] [com] [ast] [des] [wm]
[bd_reservar]		[servi_labs]	[sis_reservar]	[srv_db] [srv_web]	[wifi] [LAN]	[tape]			[ast] [des]
[bd_controlac]		[servi_dev]	[sis_controlac]	[srv_db] [srv_web]	[wifi] [LAN]	[tape]			[des]
[bd_reunion]		[servi_dev]	[sis_reunion]	[srv_db] [srv_web]	[wifi] [LAN]	[tape]			[des]
[bd_ara]		[servi_dev]	[sis_ara]	[srv_db] [srv_web]	[wifi] [LAN]	[tape]			[des]
[bd_satt]		[servi_dev]	[sis_satt]	[srv_db] [srv_web]	[wifi] [LAN]	[tape]			[des]
[backup]		[servi_support] [servi_mante] [servi_file]				[disk]			[adm] [com] [ast] [des] [wm]
[source]		[servi_dev]	[sis_crm] [sis_controlac] [sis_creacion] [sis_reunion] [sis_reservar] [sis_ara] [sis_satt] [sis_controlpc]	[srv_db] [srv_web]	[wifi] [LAN]	[disk]			[com] [des] [wm]
[files]		[servi_file]		[serv_file]	[wifi] [LAN]	[disk]			[com]
[bd_controlpc]		[servi_labs]	[sis_controlpc]	[srv_control]	[wifi] [LAN]	[tape]			[com] [des]

[conf]		[servi_acco] [servi_dev] [servi_wifi] [email] [servi_mante] [servi_file] [servi_labs]	[sis_crm] [sis_controlac] [sis_creacion] [sis_reunion] [sis_reservar] [sis_ara] [sis_satt] [sis_controlpc] [av]	[print] [scan] [cam] [mobile] [srv_strmg] [wap] [pc] [srv_control] [srv_dhcp] [srv_radius] [switch] [router] [srv_mail] [srv_db] [srv_web] [srv_ant]	[wifi] [LAN]	[disk]			[com] [des]
[log]		[servi_support]	[sis_crm] [sis_controlac] [sis_creacion] [sis_reunion] [sis_reservar] [sis_ara] [sis_satt] [sis_controlpc] [av]	[print] [scan] [cam] [mobile] [srv_strmg] [wap] [pc] [srv_control] [srv_dhcp] [srv_radius] [switch] [router] [srv_mail] [srv_db] [srv_web] [srv_ant]	[wifi] [LAN]	[disk] [log] [nas]			[com] [des]
[bd_ldap]		[servi_acco] [servi_wifi] [email] [servi_labs]	[sis_crm] [sis_creacion] [sis_reservar] [sis_controlpc]	[wap] [pc] [srv_radius]	[wifi] [LAN]	[disk]			[com]
[bd_sitiobFiec]		[servi_dev]	[sis_crm] [sis_controlac] [sis_creacion] [sis_reunion] [sis_reservar] [sis_ara] [sis_satt]	[srv_db] [srv_web]	[LAN]	[disk] [tape]			[wm] [com]
[servi_a/v]	[conf]			[cam] [mobile] [srv_strmg] [wap] [pc]	[wifi] [LAN]				[ast]
[servi_equi]	[files]			[srv_files]					[adm] [ast]
[servi_support]	[bd_crm] [backup]		[sis_crm]	[srv_db] [srv_web]	[wifi] [LAN]				[adm] [com] [ast] [des] [wm]

[servi_acco]	[bd_ldap]		[sis_creacion]	[srv_db] [srv_web]	[wifi] [LAN]				[com] [des]
[servi_dev]	[bd_crm] [bd_reservar] [bd_controlac] [bd_reunion] [bd_ara] [bd_satt] [source] [bd_controlpc] [conf] [log] [bd_ldap] [bd_sitioFiec]		[sis_crm] [sis_controlac] [sis_creacion] [sis_reunion] [sis_reservar] [sis_ara] [sis_satt] [sis_controlpc]	[srv_db] [srv_web]	[wifi] [LAN]				[com] [des] [wm]
[servi_wifi]	[conf] [log] [bd_ldap]		[sis_portal]	[wap] [pc] [srv_control] [srv_dhcp] [srv_radius] [switch] [router]	[wifi] [LAN]				[com]
[email]	[conf] [log] [bd_ldap]		[av]	[srv_mail]	[wifi] [LAN]				[com]
[servi_mante]	[bd_crm] [backup]		[sis_crm] [pkt] [av]	[print] [scan] [cam] [mobile] [wap] [pc]	[wifi] [LAN]				[adm] [com] [ast] [des] [wm]
[servi_file]	[backup] [source] [files] [bd_ldap]		[pkt] [av]	[srv_files]	[wifi] [LAN]				[com]
[servi_labs]	[bd_reservar] [bd_ldap]		[sis_reservar]	[print] [scan] [cam] [mobile] [pc]	[wifi] [LAN]				[adm] [ast]
[sis_crm]		[servi_support] [servi_mante] [servi_dev]		[srv_db] [srv_web]					[adm] [com] [ast] [des] [wm]
[sis_controlac]		[servi_dev]		[srv_db] [srv_web]					[com] [des]
[sis_creacion]		[servi_acco] [servi_dev]		[srv_db] [srv_web]					[com] [des]

[sis_reunion]		[servi_dev]		[srv_db] [srv_web]					[com] [des]
[sis_reservar]		[servi_labs] [servi_dev]		[srv_db] [srv_web]					[adm] [com] [ast] [des] [wm]
[sis_ara]		[servi_dev]		[srv_db] [srv_web]					[com] [des]
[sis_satt]		[servi_dev]		[srv_db] [srv_web]					[com] [wm]
[pkt]		[servi_support] [servi_mante] [servi_files]		[srv_files]					[adm] [com] [ast] [des] [wm]
[sis_controlpc]		[servi_dev]		[srv_control]					[com] [des]
[av]		[servi_support] [servi_mante]		[srv_ant]					[adm] [com] [ast] [des] [wm]
[sis_portal]		[servi_wifi]		[srv_dhcp] [srv_radius]					[adm] [com]
[print]	[conf] [log]	[servi_support] [servi_mante]						[building]	[adm] [com] [ast]
[scan]		[servi_support] [servi_mante]						[building]	[adm] [com] [ast]
[cam]		[servi_support] [servi_mante]						[building]	[adm] [com] [ast]
[mobile]	[backup] [files]	[servi_support] [servi_mante] [servi_labs] [servi_equi]						[building]	[adm] [com] [ast] [des] [wm]
[srv_strmg]	[conf] [log]	[servi_a/v]						[building] [local]	[com]

[wap]	[conf] [log]	[servi_wifi]						[building]	[com]
[pc]	[backup] [files] [conf] [log]	[servi_support] [servi_mante] [servi_labs] [servi_equi]						[building]	[adm] [com] [ast] [des] [wm]
[srv_files]	[backup] [source] [files]	[servi_file]						[building] [local]	[com]
[srv_control]	[bd_controlpc]	[servi_dev]						[building] [local]	[com] [des]
[srv_dhcp]	[conf] [log]	[servi_wifi]						[building] [local]	[com]
[srv_radius]	[conf] [log]	[servi_wifi]						[building] [local]	[com]
[switch]	[conf] [log]	[servi_a/v] [servi_acco] [servi_wifi] [email] [servi_file] [servi_labs]						[building] [local]	[com]
[router]	[conf] [log]	[servi_a/v] [servi_acco] [servi_wifi] [email] [servi_file] [servi_labs]						[building] [local]	[com]
[srv_mail]	[conf] [log]	[email]						[building] [local]	[com]
[srv_db]	[bd_crm] [bd_reservar] [bd_controlac] [bd_reunion] [bd_ara] [bd_satt] [log] [conf] [bd_ldap] [bd_sitioFiec]	[servi_dev]						[building] [local]	[com]
[srv_web]	[conf] [log]	[servi_dev]						[building] [local]	[com] [wm]
[srv_ant]	[conf] [log]	[servi_support] [servi_mante] [servi_labs]						[building] [local]	[com]

[wifi]		[servi_wifi]	[sis_portal]					[building] [local]	[adm] [com]
[LAN]		[servi_a/v] [servi_support] [servi_dev] [servi_acco] [servi_wifi] [email] [servi_mante] [servi_file] [servi_labs]	[sis_crm] [sis_controlac] [sis_creacion] [sis_reunion] [sis_reservar] [sis_ara] [sis_satt] [pkt] [sis_controlpc] [av] [sis_portal]					[building] [local]	[adm] [com]
[disk]	[bd_crm] [bd_reservar] [bd_controlac] [bd_reunion] [bd_ara] [bd_satt] [backup] [source] [files] [bd_controlpc] [conf] [log] [bd_ldap] [bd_sitioFiec]							[local]	[adm] [com] [ast] [des] [wm]
[san]	[files] [conf] [log]							[local]	[adm] [com] [ast]
[tape]	bd_crm] [bd_reservar] [bd_controlac] [bd_reunion] [bd_ara] [bd_satt] [backup] [source] [conf] [log] [bd_ldap] [bd_sitioFiec]							[local]	[com]
[furniture]		[servi_a/v] [servi_wifi] [servi_file] [servi_labs]			[wifi] [LAN]				[adm] [com]
[tools]		[servi_mante] [servi_support]							[adm] [com] [ast]
[tools_networK]		[servi_mante] [servi_support]			[wifi] [LAN]				[adm] [com]
[ss]					[wifi] [LAN]				[adm] [ast]

[ups]		[servi_a/v] [servi_dev] [servi_acco] [servi_wifi] [email] [servi_file] [servi_labs]			[wifi] [LAN]				[adm] [com] [ast]
[ac]		[servi_a/v] [servi_dev] [servi_acco] [servi_wifi] [email] [servi_file] [servi_labs]			[wifi] [LAN]				[adm] [com] [ast]
[building]				[print] [scan] [cam] [mobile] [wap] [pc]					[adm] [com] [ast]
[local]				pc] [srv_strmg] [srv_files] [srv_control] [srv_dhcp] [srv_radius] [switch] [router] [srv_mail] [srv_db] [srv_web] [srv_ant]					[adm] [com]
[adm]	[conf]	[servi_a/v] [servi_equi] [servi_support] [servi_dev] [servi_acco] [servi_wifi] [email] [servi_mante] [servi_file] [servi_labs]	[sis_crm] [pkt] [sis_reservar]	[print] [scan] [cam] [mobile] [pc] [switch] [router]					
[com]	[bd_crm] [bd_reservar] [bd_controlac] [bd_reunion] [bd_ara] [bd_satt] [backup] [source] [files] [bd_controlpc] [conf] [log] [bd_ldap] [bd_sitioFiec]	[servi_acco] [servi_wifi] [email] [servi_file]	[sis_crm] [pkt] [av] [sis_portal]	[print] [srv_strmg] [wap] [srv_files] [srv_control] [srv_dhcp] [srv_radius] [switch] [router] [srv_mail] [srv_db] [srv_web] [srv_ant]					
[ast]	[conf]	[servi_a/v] [servi_support] [servi_mante]	[sis_crm] [pkt] [sis_reservar]	[print] [scan] [cam] [mobile] [pc]					

[des]	[bd_crm] [bd_reservar] [bd_controlac] [bd_reunion] [bd_ara] [source] [bd_controlpc] [conf] [log]	[servi_dev]	[sis_crm] [pkt] [sis_controlac] [sis_creacion] [sis_reunion] [sis_reservar] [sis_ara] [sis_controlpc]	[srv_control]					
[wm]	[bd_satt] [backup] [source] [conf] [log] [bd_sitioFiec]	[servi_dev]	[sis_crm] [sis_satt] [pkt]						

ANEXO G

ROLES Y ASIGNACION DE RESPONSABILIDADES

PERSONAL DEL DST

Nombre	Correo	Cargo
Katherine Campos	admredes@fiec.espol.edu.ec	Asistente Técnico de Redes
Diana Ordoñez	admintec@fiec.espol.edu.ec	Asistente Técnico de Soporte
Xavier Villacrés	admlab@fiec.espol.edu.ec	Asistente Técnico de Soporte
Carlos Bustamante	asistec@fiec.espol.edu.ec	Asistente Técnico de Soporte
Dalton Gutierrez	admdev@fiec.espol.edu.ec	Asistente Técnico de Desarrollo
Christian Vergara	admweb@fiec.espol.edu.ec	Webmaster
Margarita Filián	mfilian@fiec.espol.edu.ec	Jefe del DST

Objetivo:

Este documento tiene como objetivo definir los roles y responsabilidades en el esquema de seguridad informática definido para el DST, así como también las habilidades y competencias necesarias para cumplir con las mismas

Roles definidos:

- ✓ Responsable de servicios e infraestructura tecnológica
- ✓ Responsable de seguridad

- ✓ Responsable de sistemas
- ✓ Responsable de soporte
- ✓ Responsable de sitio web

ROLES: FUNCIONES Y RESPONSABILIDADES

A continuación se describen las responsabilidades y funciones que requiere cada rol que se ha definido para el esquema de seguridad de informática:

Responsable de servicios e infraestructura tecnológica
El Jefe del DST tendrá el rol de responsable de los servicios informáticos y de los activos que forman la infraestructura tecnológica de la FIEC. Teniendo por funciones las siguientes: • Establecer los requisitos de los servicios en materia de seguridad. • Trabajar con el responsable de seguridad, sistemas y soporte en el mantenimiento y revisión de los servicios, equipos y sistemas alineándolos al esquema de seguridad. • Coordinar las actividades con los demás responsables para lograr la adecuada y oportuna implementación del esquema de seguridad. • Realizar revisiones y estado de las incidencias ocurridas. • Verificar que los sistemas desarrollados no presenten vulnerabilidades, realizando pruebas sobre los mismos.

Responsables de Seguridad

El Jefe del DST y el Asistente Técnico de Redes tienen el rol de responsable de seguridad.

- El Jefe del DST tiene por funciones las siguientes:
- Mantener la seguridad de la información y los servicios que administra
- Realizar revisiones periódicas que permitan verificar el cumplimiento del esquema de seguridad.
- Difundir y promover la concienciación de la seguridad informática dentro de su ámbito de responsabilidad.
- Coordinar reuniones con los demás responsables de seguridad para verificar que las medidas y esquema de seguridad establecidas son adecuadas para la protección de los activos.
- Analizar, modificar y completar la documentación relacionada con el esquema de seguridad.
- Aprobar los procedimientos de seguridad elaborados por los demás responsables.
- Revisar que el sistema de control de acceso y CCTV funcione correctamente.

El Asistente Técnico de Redes tiene por funciones las siguientes:

- Monitorear el estado de la red y servidores.
- Sugerir herramientas o mecanismos que ayuden en el análisis de logs y eventos.
- Investigar a cerca de los incidentes de seguridad desde que son notificados hasta que sean resueltos.
- Llevar una bitácora de incidentes ocurridos.
- Realizar hardening en los sistemas para reducir vulnerabilidades y posibles amenazas.
- Asegurar que la red inalámbrica ingresen a través del portal cautivo.
- Realizar copias de seguridad de la información de los principales servidores de la FIEC.
- Revisar periódicamente el estado de las bases y sus usuarios.
- Determinar la configuración de hardware y software a utilizar en el sistema.
- Configuración y puesta a punto de las bases de datos.

Responsable de Sistemas

El Asistente Técnico de Desarrollo en el rol de responsable de los sistemas. Tiene por funciones, dentro de sus áreas de trabajo, las siguientes:

- Desarrollar, administrar y mantener los sistemas que desarrollo o se le asignen durante todo su ciclo de vida, realizando tareas de instalación configuración y verificación de su correcto funcionamiento.
- Definir como se conectan los usuarios a los sistemas, ya sea a través de credenciales de FIEC o ESPOL.
- Sugerir y documentar los cambios que afecten a la seguridad de los sistemas en el modo que operan.
- Sugerir y aplicar las medidas de seguridad al momento de desarrollar los sistemas.
- Considerar todos los escenarios posibles de posibles vulnerabilidades en los sistemas y corregirlos.
- Determinar la configuración de hardware y software a utilizar en el sistema.
- Documentar los cambios realizados en los sistemas.
- Definir perfiles de acceso para cada sistema.
- Investigar acerca de incidentes de seguridad que afecten los sistemas en lo relacionado con versiones de software, sistema operativo y código; documentarlo y comunicarlo a las personas responsables de seguridad.
- Realizar las pruebas necesarias de los sistemas desarrollados con el fin de evitar posibles vulnerabilidades.
- Revisar que los sistemas que desarrolle no presenten información de dirección ip, versión de base de datos o sistema operativo donde es alojado, es decir información del servidor.

Responsables de Soporte

Los Asistentes Técnico de Soporte en el rol de responsable de soporte. Tienen por funciones, dentro de sus áreas de trabajo, las siguientes:

- Realizar mantenimiento preventivo y correctivos al finalizar un semestre.
- Deben mantener y actualizar el inventario de los equipos a su cargo.
- Instalar antivirus en todos los equipos con inventario ESPOL.
- Realiza configuraciones necesarias para evitar que ejecución de código malicioso mediante el autorun.
- Los equipos a su cargo deben tener configuradas contraseñas.
- Deben sugerir y realizar actualizaciones de paquetes de programas, sistemas operativos y parches.

Responsable de sitio web

El webmaster en el rol de responsable de sitio web. Tienen por funciones, dentro de sus áreas de trabajo, las siguientes:

- Realizar mantenimiento al sitio web de la FIEC.
- Sugerir y realizar cambios de los componentes o plugins que presenten vulnerabilidades.
- Sugerir el cambio de versión del administrador de contenido.
- Revisar que el sitio web no presente información de dirección ip, versión de base de datos o sistema operativo.

ANEXO H

INVENTARIO DE EQUIPOS DE COMPUTACIÓN

Laboratorio/Oficina:
Ubicación:
Fecha:
Realizado por:

No.	Uso	Marca/ Modelo Cpu	Marca/ Modelo Monitor	Marca/ Modelo Teclado	Marca/ Modelo mouse	Serie CPU	Serie Monitor	Serie Teclado	Serie Mouse	Inventario CPU	Inventario Monitor	Inventario Teclado	Inventario Mouse
1													
2													

RESUMEN EJECUTIVO						
Procesador	**Velocidad (Ghz)**	**Cantidad PCs**	**Disco Duro**	**Memoria**	**Inventario**	**Año inventario**

ANEXO I

¨Personal del DST responsables del inventario y mantenimiento de activos de la FIEC.

Laboratorio / Oficina / Rack	Responsable
Laboratorio de Computación 1	Asistente Técnico de Soporte I
Laboratorio de Computación 2	Asistente Técnico de Soporte I
Laboratorio de Computación 3	Asistente Técnico de Soporte I
Laboratorio de Computación 4	Asistente Técnico de Soporte I
Laboratorio de Computación 5	Asistente Técnico de Soporte I
Laboratorio de Computación 6	Asistente Técnico de Soporte I
Laboratorio de Computación 7	Asistente Técnico de Soporte I
Laboratorio Móvil	Asistente Técnico de Soporte I
Lab. Programas Utilitarios 1	Asistente Técnico de Soporte I
Lab. Programas Utilitarios 2	Asistente Técnico de Soporte I
Lab. de Sistemas Multimedia	Asistente Técnico de Soporte I
Lab. de Ingeniería de Software	Asistente Técnico de Soporte I
Lab. de Realidad Virtual	Asistente Técnico de Soporte I
Lab. de Automatización Industrial 1	Asistente Técnico de Soporte II
Lab. de Automatización Industrial 2	Asistente Técnico de Soporte II
Lab. de Computación de Potencia	Asistente Técnico de Soporte II
Lab. de Control Automático	Asistente Técnico de Soporte II
Lab. de Controles Industriales Eléctricos	Asistente Técnico de Soporte II
Lab. de Electrónica A	Asistente Técnico de Soporte II
Lab. de Electrónica B	Asistente Técnico de Soporte II
Lab. de Instrumentación Industrial	Asistente Técnico de Soporte II
Lab. de Maquinarias	Asistente Técnico de Soporte II
Lab. de Microcontroladores	Asistente Técnico de Soporte II
Lab. de Microprocesadores	Asistente Técnico de Soporte II
Lab. de Redes Eléctricas	Asistente Técnico de Soporte III
Lab. de Robótica	Asistente Técnico de Soporte III
Lab. de Simulación de Redes	Asistente Técnico de Soporte III
Lab. de Sistemas Telemáticos	Asistente Técnico de Soporte III
Lab. de Sistemas Digitales	Asistente Técnico de Soporte III
Lab. de Telecomunicaciones	Asistente Técnico de Soporte III
Lab. de Circuitos Impresos	Asistente Técnico de Soporte III
Lab. de Electrónica Médica	Asistente Técnico de Soporte III
Lab. de Electrónica de Potencia	Asistente Técnico de Soporte III
Lab. de Sistemas de Potencia	Asistente Técnico de Soporte III
Lab. de Proyectos Eléctricos y Electrónicos	Asistente Técnico de Soporte III
Grupos estudiantiles	Asistente Técnico de Soporte I, II y III
Docentes	Asistente Técnico de Soporte I, II y III
Redes y Servidores	Asistente Técnico de Redes y Jefe del DST
Sistemas	Asistente Técnico de Desarrollo
Sitio Web	Webmaster
Control de Acceso y CCTV	Jefe del DST

ANEXO J

Acuerdo de Confidencialidad.

ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE INFORMACIÓN.

En _____ (ciudad) a ____ de _____ de 20__.

De un lado, _____ (nombre y apellidos del USUARIO), en su propio nombre y derecho, con domicilio a efectos del presente Acuerdo en _____ (domicilio), _____ (ciudad), en adelante “EL USUARIO”.

Y el Departamento de Soporte Técnico, en su propio nombre y derecho / en nombre, con domicilio a efectos del presente Acuerdo en el Campus Km 3.5 vía perimetral, Campus Gustavo Galindo de la Escuela Superior Politécnica del Litoral en la Facultad de Ingeniería en Electricidad y Computación, edificio 16C, Guayaquil, en adelante “EL DST”.

Ambas partes se reconocen recíprocamente con capacidad para obligarse y, al efecto, suscriben el presente Acuerdo de Confidencialidad y de No Divulgación de Información en base a las siguientes ESTIPULACIONES:

PRIMERA.- Objeto. El presente Acuerdo se refiere a la información que EL USUARIO tiene acceso y que el DST le ha asignado ya sea para que la administre o haga uso de ella de acuerdo a las funciones del cargo que ocupa, esta información puede ser entregada de forma oral, gráfica o escrita.

SEGUNDA.- 1. EL DST únicamente utilizará la información que involucra a la FIEC para fines académicos y administrativos dentro de la institución, por lo que EL USUARIO se compromete a mantener la más estricta confidencialidad respecto de dicha información.

2. EL USUARIO no podrá reproducir, modificar, hacer pública o divulgar a terceros la información objeto del presente Acuerdo sin previa autorización.

3. De igual forma, EL DST protegerá la información objeto de este Acuerdo en las dimensiones de seguridad que corresponde a confidencialidad e integridad, evitando en la medida de lo posible su pérdida, robo o sustracción.

TERCERA.- Sin perjuicio de lo estipulado en el presente Acuerdo, ambas partes aceptan que la obligación de confidencialidad no se aplicará en los siguientes casos:

a) Cuando la información sea considera de dominio público.

b) Cuando la información ya estuviera en el conocimiento de EL USUARIO con anterioridad a la firma del presente Acuerdo y sin obligación de guardar confidencialidad.

c) Cuando la máxima autoridad de la FIEC indique que de acuerdo a una eventualidad se dé a conocer dicha información.

d) En caso de que EL USUARIO pueda probar que la información fue desarrollada o recibida por terceros, independiente de la relación con EL DST.

CUARTA.- Los derechos de propiedad de la información objeto de este Acuerdo pertenecen a EL DST y el hecho de revelarla a EL USUARIO no cambiará tal situación de que debe ser confidencial.

En caso de que la información sea revelada, divulgada o utilizada por EL USUARIO de forma distinta al objeto de este Acuerdo, ya sea de forma dolosa o por mera negligencia, se aplicarán las sanciones de acuerdo a lo que indique la máxima autoridad de la Facultad si llega a causar daños o perjuicios.

QUINTA.- Las partes se obligan a devolver cualquier documentación que se les haya facilitado en cualquier tipo de soporte, en el supuesto de que cese la relación entre las partes por cualquier motivo.

SEXTA.- El presente Acuerdo entrará en vigor en el momento de la firma del mismo por ambas partes, extendiéndose su vigencia hasta 3 meses después del momento que finalizase la relación entre las partes.

SÉPTIMA.- En caso de cualquier conflicto o discrepancia que pueda surgir en relación con la interpretación y/o cumplimiento del presente Acuerdo, las partes se someten ante la máxima autoridad de la Facultad.

Y en señal de expresa conformidad y aceptación de los términos recogidos en el presente Acuerdo, lo firman las partes por duplicado ejemplar y a un solo efecto en el lugar y fecha al comienzo indicados.

_____ _____

EL USUARIO EL DST

ANEXO K

Procedimiento de eliminación de soportes.

Para la eliminación de soportes de información se debe tener la autorización del dueño de la información mediante un correo, ticket mediante el sistema CRM u oficio. Y se deberá seguir el siguiente procedimiento de acuerdo a tipo de soporte.

En el caso de:

Cintas magnéticas, se borran mediante software y se procede a dar de baja en caso de que no se las requiera.

Discos duros, se debe dar formato a bajo nivel para asegurarnos que se borre todo la información. Y en caso de considerarse obsoleto se realizará el trámite de baja correspondiente.

Recurso compartido, se elimina el contenido del recurso.

USB, se formatea a bajo nivel para asegurar que se borre toda la información que está contenida en el mismo.

Procedimiento para gestionar usuarios y privilegios.

El DST establecerá accesos a la red, recursos y sistemas de acuerdo al grupo que se encuentren el usuario:

Docentes y técnicos docentes, tendrán accesos a los sistemas que usa la facultad y al recurso compartido en la red previa autorización del dueño de la información.

Estudiantes, podrán acceder al correo, sistemas destinados para estudiantes y uso de equipos.

Administrativos, tendrán accesos a los sistemas que usa la facultad y al recurso compartido en la red previa autorización del dueño de la información.

1. Deberán solicitar acceso a los sistemas y recursos que requieran y dependiendo del acceso que requiere deberá ser autorizado por la máxima autoridad.

2. Personal del DST debe realizar las configuraciones en: ldap, sistemas y recursos para otorgar accesos.

3. Notificará al usuario que ha solicitado los accesos el momento que ya puede hacer uso de los mismos.

El personal del DST encargado de la gestión de los usuarios deberá revisar al término de cada semestre que los accesos a los recursos estén asignados correctamente.

En lo relacionado con la gestión de usuarios, el personal del DST debe tomar en consideración lo siguiente:

Creación de cuentas

1. Los estudiantes de la FIEC pueden crear su usuario a través del sitio web de la facultad, siempre y cuando exista su usuario de ESPOL.

2. El DST puede crear una cuenta de la FIEC a los docentes que posean una cuenta de ESPOL y deberán notificarle al correo de ESPOL lo siguiente:

    a. La cuenta ha sido creada.

    b. Tienen una contraseña temporal y que debe cambiarla a través del siguiente link: https://www.fiec.espol.edu.ec/servicios/password/app/password.php

    c. Tiene acceso al correo de la Facultad en el siguiente enlace: https://www.fiec.espol.edu.ec/mail

3. El DST puede crear una cuenta de la FIEC al personal administrativo que posea una cuenta de ESPOL y deberán notificarle al correo de ESPOL lo siguiente:

    a. La cuenta ha sido creada.

    b. Tienen una contraseña temporal y que debe cambiarla a través del siguiente link: https://www.fiec.espol.edu.ec/servicios/password/app/password.php

    c. Tiene acceso al correo de la Facultad en el siguiente enlace: https://www.fiec.espol.edu.ec/mail

Eliminación de cuentas

El DST deberá de dar de baja las cuentas de usuarios que se desvinculen con la facultad, previa autorización de la máxima autoridad de la FIEC.

Procedimiento de cambio de equipo o reubicación

El personal del DST podrá cambiar o reubicar equipos de acuerdo a lo siguiente:

- Si el equipo en cuestión presenta falla en alguno de sus periféricos o componentes, procederá a cambiar esa parte.

- Si después de cambiar una parte el equipo sigue presentando problemas, se procederá a cambiar el mismo.

- Si un usuario solicita cambio o reubicación de equipo, se deberá analizar el motivo de la solicitud y comunicar al Jefe del DST.

- Un equipo se podrá reubicar de acuerdo a las necesidades y previa solicitud y autorización de la máxima autoridad o jefe inmediato.

Procedimiento de respaldo de la información y datos críticos

El personal del DST realizará los respaldos de información y datos críticos de acuerdo a lo siguiente:

Equipos u unidades de almacenamiento externas.

- Si un equipo debe ser reinstalado o formateado, deberá realizarse antes un respaldo de la información.

Servidores y recursos compartidos.

- El administrador de redes y servidores deberá realizar una tarea programada que se ejecute al menos 3 veces en la semana, por lo cual se debe colocar las cintas magnéticas en cada uno de los dispositivos de respaldo en el orden que se detalla a continuación:

	Día 1	Día 2	Día 3
SRV1	x	x	x
SRV2	x	x	x
SRV3	x	x	x

Procedimiento de revisión estado de servidores y red.

Servidores

- El administrador de la red y servidores debe verificar periódicamente el espacio en disco de los servidores principales, memoria en uso y procesamiento haciendo uso de software o comandos según sea el caso.

Red

- Si existe un problema en la red el administrador de redes debe proceder a revisar los nodos principales dependiendo del área donde no hay acceso a internet.

- Revisar servidores: DNS, DHCP o Radius.

- En caso de que el problema no se genere en la FIEC deberá escalar o preguntar a la GTySI.

En el caso de que existe un corte de energía debe proceder a revisar el estado de los servidores, red inalámbrica y servicios.

Procedimiento de mantenimiento de equipos.

El procedimiento para dar mantenimiento a equipos es el siguiente:

- Se solicita a los docentes el software que requieren mediante un correo.
- Planifica un cronograma de actividades.
- Se inicia el mantenimiento que comprende lo siguiente:
    - Limpieza completa del hardware.
    - Formatear el equipo y reinstalar los sistemas operativos con las aplicaciones actualizadas y necesarias para el semestre.
- Se verifica el inventario,
- Se actualizan los documentos de registros de instalación de los equipos, ejecución de mantenimiento e inventario.

El mantenimiento preventivo se lo realiza una vez por semana en el caso de laboratorios. Comprende la limpieza de registros y de archivos temporales, la ejecución del antivirus, descarga e instalación de actualizaciones del sistema operativo y limpieza externa.

Procedimiento de control de cambios para la parte operativa, de comunicaciones y de desarrollo.

Para realizar un cambio que involucre para parte operativa, comunicaciones y de desarrollo se debe considerar lo siguiente:

- Definir quiénes son los afectados
- Aprobar o negar el cambio propuesto.
- Planificar cuando se realizará el cambio.
- Probar el cambio en un ambiente de prueba.
- Comunicar detalles del cambio a las personas pertinentes.