PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

MAESTRÍA EN REDES DE COMUNICACIÓN

INFORME FINAL CASO DE ESTUDIO PARA UNIDAD DE TITULACIÓN ESPECIAL

TEMA:

"ELABORACIÓN DE POLITICAS Y NORMAS DE SEGURIDAD DE LA INFORMACIÓN EN BASE A LA NORMA DE SEGURIDAD ISO/IEC 27001, Y AL ANÁLISIS DE RIESGOS REALIZADO APLICANDO LA METODOLOGÍA MAGERIT Y LA HERRAMIENTA PILAR."

CASO DE ESTUDIO: UNIVERSIDAD POLITÉCNICA SALESIANA SEDE QUITO CAMPUS SUR

Tixilima Cisneros Viviana de los Angeles

Quito – 2015

AUTORÍA

Yo, Viviana de los Angeles Tixilima Cisneros, portadora de la cédula de ciudadanía No. 171759669-4, declaro bajo juramento que la presente investigación es de total responsabilidad del autor, y que se he respetado las diferentes fuentes de información realizando las citas correspondientes. Esta investigación no contiene plagio alguno y es resultado de un trabajo serio desarrollado en su totalidad por mi persona.

_____

Tixilima Cisneros Viviana de los Angeles

Contenido

Índice de Figuras

Índice de Tablas

CAP. I: INTRODUCCIÓN

1.1 Introducción

"La tendencia, cada vez más dominante, hacia la interconectividad y la interoperabilidad de las redes, de las máquinas de computación, de las aplicaciones, e incluso de las empresas, ha situado a la seguridad de los sistemas de información como un elemento central en todo el desarrollo de la sociedad." (AREITIO, 2008).

Este trabajo presenta la creación de políticas de Seguridad basadas en las normas ISO/IEC 27001 para la red de la Universidad Politécnica Salesiana Sede Quito Campus Sur, mediante la utilización de la metodología MAGERIT para el Análisis y Gestión de Riesgos. Su principal fin es conocer el estado actual de red, definir los activos y el valor que estos tienen para la empresa, identificar amenazas, evaluar riesgos, ya que la información es un recurso vital para toda institución; y esta es generada en función de las actividades que se llevan a cabo en cada área o departamento, por lo que se busca establecer e implementar políticas de seguridad, que permitan controlar el acceso a recursos en la red, mismas que permitan asegurar la disponibilidad, integridad y confidencialidad en el manejo de la información, minimizando e identificando los riesgos de ocurrencia.

1.2 Justificación

En la actualidad ha comenzado a ser de suma importancia el manejo que se le da a la información, y a la forma como es utilizada la red; debido a ello son muchas las funciones por las cuales se debe velar por su seguridad.

"Las tecnologías de la información actualmente son elementos fundamentales para la superación y desarrollo de un país, la información que en ellas se maneja es considerada un activo cada vez más valioso el cual puede hacer que una organización triunfe o quiebre." (Seguridad Informatica, 2014).

"Las empresas, instituciones u organizaciones que se jactan de tener una red: "ágil" y "receptiva", a menudo alcanzan altas prestaciones mediante el uso de estandarizaciones, de procesos maduros y de planeamiento de contingencias; "por lo que estas entidades y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo." (El portal de ISO 27001 en Español, 2005).

En los ambientes universitarios usualmente es notoria la aparición de virus, gusanos, spyware y malware y a menudo funcionan con malas prácticas globales de seguridad, donde los equipos portátiles tanto de docentes, como de estudiantes, que no tengan antivirus y antispyware pueden verse comprometidos al ponerse en contacto con la red universitaria.

Así mismo es común encontrar en los ambientes universitarios puntos de acceso inalámbricos conllevando a riesgos y a más vulnerabilidades, donde los atacantes comúnmente acceden inalámbricamente para rastrear los paquetes, identificando información sensible para los usuarios tales como docentes, estudiantes y administrativos, información como: datos personales, claves de acceso, documentación privada, exámenes, notas, etc.

Para poder identificar las vulnerabilidades de los activos de un ambiente universitario como lo es el Campus Sur de la Universidad Politécnica Salesiana, se va hacer uso de la herramienta PILAR.

En función de los resultados obtenidos se procederá a realizar un análisis de cada dato obtenido para diseñar un Modelo de Política de Seguridad en base a las normas de Seguridad ISO/IEC 27001, a través de la utilización de la metodología Magerit.

Por lo indicado el presente proyecto se justifica ya que se pretende identificar la información que siempre debe estar disponible, manteniendo su integridad y confidencialidad, para esto es importante identificar las vulnerabilidades de los activos del Campus Sur de la Universidad

Politécnica Salesiana, realizando un análisis de riesgos, una evaluación de servicios lo cual permite identificar las áreas que no cumplen los niveles de servicio propuestos; chequeo de la autenticidad de la información con el propósito de garantizar que la información no sea modificada en el tránsito, manteniendo un control de acceso a la información y evaluando un acceso no autorizado a datos.

1.3 Antecedentes

"En la actualidad, las organizaciones hacen uso de tecnologías de la información para su operación diaria. El logro de sus objetivos se debe en gran medida a su utilización. Sin embargo, existen riesgos inherentes a ellas, es decir, la posibilidad de que una debilidad sea aprovechada por una amenaza y sus consecuencias: divulgación, modificación, pérdida o interrupción de información sensible." (Miguel Ángel Mendoza López, 2013).

Ha comenzado a ser de suma importancia el manejo que se le da a la información y la forma como es utilizada la red y sus dispositivos de interconexión. Por lo que la creación de un Modelo de Políticas de Seguridad se ha vuelto en un aspecto fundamental y necesario, debido a su alta sistematización, tornándose importante la necesidad de saber que sucede con los activos de información de una Universidad, anticipándose a los posibles fallos y a detectar su posible impacto en la prestación de un servicio.

La seguridad actual de toda organización, es un proceso de mejora continua, en la que han de estar implicados todos los departamentos de una empresa, que debe estar bajo un modelo de madurez eficaz que monitorice, con valores cuantitativos y cualitativos, los riesgos de seguridad para poder actuar, no sólo de forma reactiva, sino proactiva y preventiva (AREITIO, 2008).

"La gestión de seguridad hace referencia a la habilidad para supervisar y controlar la disponibilidad de facilidades de seguridad, y a reportar amenazas y rupturas en la seguridad." (MATUTE MACIAS, 2006) *, su objetivo es "asegurar la protección de la información en las redes y la protección de la infraestructura de soporte, permite abarcar los límites de las organizaciones,*

requiere de la cuidadosa consideración del flujo de la data, implicancias legales, monitoreo y protección." (ISO, 2005).

"Las políticas de seguridad de la Información dictan el cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico del organismo. Así mismo las políticas de seguridad de la información protegen a la misma de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riegos de daño y asegurar el eficiente cumplimento del organismo." (PUBLICA, 2005)

Las políticas así como la gestión de seguridad aparecen para proveer de herramientas, procedimientos y recursos que protejan la información de ataques; ya que en sus inicios, los ataques involucraban poca sofisticación técnica, los ataques internos se basaban en utilizar los permisos para alterar la información, los externos se basaban en acceder a la red simplemente averiguando una clave valida; a través del avance de la tecnología en los actuales tiempos los ataques se han hecho mucho más sofisticados capaces de explotar vulnerabilidades en el diseño, configuración y operación de los sistemas; Por ejemplo los ataques comunes en la capa de aplicación son:

- *DNS Spoofing para suplantar una identidad por nombre de dominio y acceder a la red.*
- *Sniffing para obtener una enorme cuantía de información sensible transmitida sin encriptar mediante sniffers o espías de red basados en difusión.*
- *Eavesdropping contempla la detención del tráfico que transita por la red de forma pasiva.*
- *Snooping que consiste en almacenar información extraída de un sistema o solo de tráfico en el ordenador del atacante.*
- *DoS denegación de servicios se producen desde el exterior de un sistema, a través de la red.*

Por el lado de la capa transporte también se presenta algunas vulnerabilidades tales como: Fingerprinting que permite obtener información de un sistema concreto.

- *Escaneo de Puertos con el propósito de hallar puertas traseras en las aplicaciones.*
- *UDP Flood y TCP SYN Flood que consisten en una denegación se servicios mediante el uso de UDP y TCP correspondientemente.*
- *Land que bloquea un sistemas mediante él envió de un paquete SYN.*
- *Sesión Hijaking para poder apoderarse de una sesión ya establecida.*

En la capa Red también se puede detectar las siguientes vulnerabilidades:

- *ICMP Echo para identificar todos los equipos existentes en una red.*
- *IP Bad Headers Fields la cual genera un error ICMP.*
- *IP Spoofing consiste en la generación IP con una dirección de origen falsa.*
- *SMURF provoca que todos los sistemas que forman parte de la red respondan simultáneamente.*
- *Ping of Death que puede ocasionar que el buffer de memoria se desborde.*

A nivel de capa Enlace de Datos las vulnerabilidades que se puede presentar son:

- *Hijacking para redirigir el flujo de tramas entre dos dispositivos hacia el equipo del atacante.*
- *ARP Spoofing para infiltrarse en una red Ethernet conmutada.*

Así también se puede citar ciertas vulnerabilidades relacionadas a los sistemas por ejemplo: Caballos de Troya los cuales son utilizados para implantar servicios no anhelados en sistemas y poder ejecutar ataques remotos.

- *Finger Bomb obliga al sistema a un elevado consumo de CPU.*
- *Buffers Overflobs que consiste en el desbordamiento de un buffer; gusanos, virus, etc.*

Todas estas vulnerabilidades afectan y ponen en riesgo a la información de una organización. (CESAR MEJIA, 2012)

En la red del Campus Sur de la Universidad Politécnica Salesiana, las principales vulnerabilidades están enmarcadas en los segmentos inalámbricos, ya que, es esta sección donde se producen Instalaciones por defecto de sistemas y aplicaciones en equipos externos a la institución pero que se conectan a la red. También otro problema es el gran número de puertos abiertos e insuficiente filtrado de paquetes con direcciones de inicio y destino inadecuadas.

1.4 Objetivos

Objetivo General:

Elaborar políticas y normas de Seguridad de la información en base a la norma de Seguridad ISO/IEC 27001, y al análisis de riesgos realizado aplicando la metodología MAGERIT y la herramienta PILAR, para el Campus Sur de la Universidad Politécnica Salesiana.

Objetivos Específicos:

1. *Analizar el estado actual de la red de la Universidad Politécnica Salesiana e identificar sus principales activos.*
2. *Identificar los potenciales riesgos a los que están expuestos los activos mediante la utilización del software PILAR.*
3. *Clasificar los tipos riesgos existentes sobre los activos para valorar su nivel de vulnerabilidad.*
4. *Diseñar un Modelo de Políticas de Seguridad adecuado para la realidad del Campus Sur de la Universidad Politécnica Salesiana en base a la metodología de análisis de riesgos* Magerit.

CAP. II: DESARROLLO CASO DE ESTUDIO

2.1 ESTADO DEL ARTE

2.1.1 Sistema de gestión de seguridad de la información.

Entendiéndose por información a todo aquel grupo organizado de datos en poder de una organización, que tengan valor para la misma, independientemente de la forma en que se almacene, procese o transmita, de su origen o de la fecha de elaboración. La seguridad de la información se basa en tres términos fundamentales:

- "Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran." (iso27000, 2012)

"El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir. Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente." (EL PORTAL DE ISO 27001 EN ESPAÑOL, 2012)

2.1.2 Políticas de seguridad de la información.

"Las Políticas de Seguridad de la Información mantienen como propósito constituir las normas y requisitos de seguridad que garanticen la confidencialidad, integridad y disponibilidad de todos los sistemas de inform.ación que forman parte de la empresa." (iso27000, 2012).

Los aspectos más trascendentales que se debe asumir en las Políticas de Seguridad son:

Tabla 1 Aspectos trascendentales en las políticas de seguridad

ACCIÓN	PROPÓSITO
Garantizar en los sistemas de información	Confidencialidad Integridad Disponibilidad
Designar un responsable de seguridad	Delegado la gestión de la seguridad Debe estar dentro de las estructuras organizacionales de la empresa
Efectuar requisitos legales	Deben ser aplicable dentro de la empresa.
Gestionar incidencias	Todas las incidencias posibles de forma adecuada
Disponer de un plan de contingencia	El plan permite a la empresa recuperarse en caso de desastre.
Informar a lo empleados	Difundir entre los empleados sus obligaciones con respecto a la seguridad de los sistemas.

Fuente: (iso27000, 2012).

Las Políticas de Seguridad están respaldadas por el Manual de Seguridad que incluye un grupo de normas de seguridad y procedimientos. Este manual puede estructurase de diversas formas. Las propuestas más usuales son las utilizadas en las certificaciones ISO 27001:

- “Gestión de los activos.

- Seguridad ligada a los recursos humanos.
- Seguridad física y ambiental.
- Gestión de las comunicaciones y operaciones.
- Control de acceso lógico.
- Gestión de incidentes.
- Planes de contingencia
- Cumplimiento de requisitos legales" (iso27000, 2012)

La Política de Seguridad debe ser:

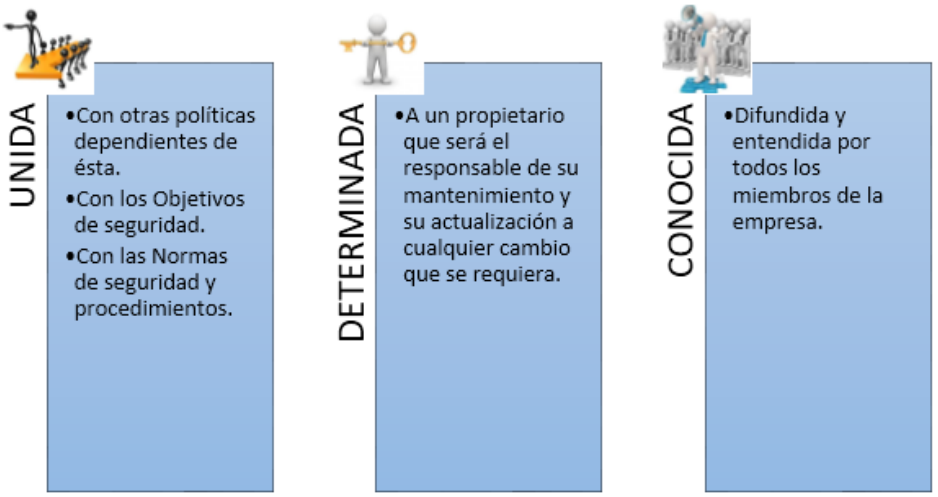

Figura 1 Características de una política
Elaborado por: Ing. Viviana Tixilima

2.1.3 Implementación de un Sistema de Gestión de Seguridad de la información SGSI.

"Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información SGSI en base a la norma ISO 27001, se utiliza el ciclo continuo PDCA, tradicional en los sistemas de gestión de la calidad; este ciclo PDCA sirve como modelo para implantación de SGSI, permanece en una constante revaluación, de las medidas de prevención, corrección y evaluación, manteniendo un constante ciclo que por sus características no podría terminar." (iso27000, 2012).

Figura 2 Ciclo PDCA

Fuente: (iso27000, 2012)

Donde:

- Plan : Planificar
- Do : Hacer
- Check : Verificar
- Act : actuar

2.1.3.1 Plan: Esta etapa se encarga de Establecer con planificación.

- "*Establecer las políticas, objetivos, procesos y procedimientos relativos a la gestión del riesgo y mejoramiento de la seguridad de la información de la organización.*
- *Definir el alcance del SGSI en términos del negocio, la organización, su localización, activos y tecnologías.*
- *Definir una metodología de evaluación del riesgo apropiada para el SGSI y los requerimientos del negocio, además de establecer los criterios de aceptación del riesgo y especificar los niveles de riesgo aceptable.*" (iso27000, 2012).
- Identificar los riesgos:

Figura 3 Ciclo para identificar riesgos
Elaborado por: Ing. Ing. Viviana Tixilima

Donde:

- 1: Identifica los activos que están dentro del alcance del SGSI;
- 2: Identifica y descubre amenazas con relación a los activos;
- 3: Identifica vulnerabilidades que puedan ser aprovechadas por amenazas;
- 4: identifica los impactos en la integridad, confidencialidad y disponibilidad de los activos.

- Analizar y evaluar los riesgos:

Figura 4 Proceso de análisis y evaluación de riesgos
Elaborado por: Ing. Ing. Viviana Tixilima

Donde:

- 1: Evalúa el impacto de un fallo de seguridad, tomando en cuenta la pérdida de confidencialidad, e integridad o disponibilidad de un activo;
- 2: Evalúa la probabilidad de ocurrencia de un fallo de seguridad;
- 3: Estima los niveles de riesgo de los activos de información;
- 4: Determina criterios de aceptación para la tolerancia de riesgo.

- Identificar y evaluar las distintas opciones de tratamiento de los riesgos para:
  - Aplicar controles adecuados;
  - Aceptar el riesgo,
  - Evitar el riesgo, y
  - Transferir el riesgo a terceros.

Figura 5 Gestión de riesgos de una empresa

Fuente: (iso27000, 2012)

2.1.3.2 Do: Esta etapa se encarga de Implementar y utilizar el SGSI:

- *"Definir un plan de tratamiento de riesgos que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.*
- *Implantar el plan de tratamiento de riesgos, con el fin de alcanzar los objetivos de control identificados, incluyendo la asignación de recursos, responsabilidades y prioridades.*
- *Definir un sistema de métricas que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles o grupos de controles.*
- *Procurar programas de formación y concienciación en relación a la seguridad de la información a todo el personal.*

- *Gestionar los recursos necesarios asignados al SGSI para el mantenimiento de la seguridad de la información.*
- *Implantar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.*
- *Desarrollo del marco normativo necesario: normas, manuales, procedimientos e instrucciones.*" (iso27000, 2012).

2.1.3.3 Check: En esta etapa se Monitoriza y revisa el SGSI.

- Ejecutar procedimientos de monitorización y revisión para:

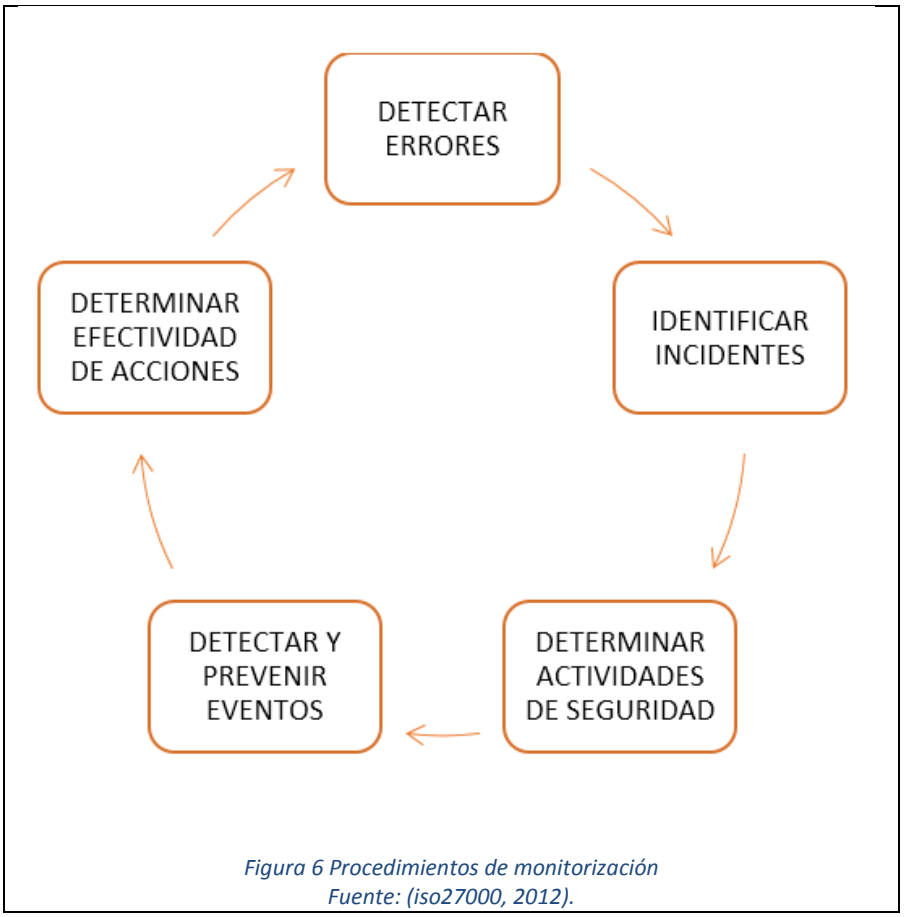

Figura 6 Procedimientos de monitorización
Fuente: (iso27000, 2012).

Donde:

Se debe detectar los errores encontrados e identificar los incidentes, para determinar qué actividades de seguridad de la información se desarrollan en relación a lo establecido, con esto se puede detectar y prevenir eventos

mediante el uso de indicadores, y así determinar la efectividad de las acciones.

- Revisar periódicamente la efectividad del SGSI.
- Evaluar la efectividad de los controles.
- Examinar periódicamente en intervalos planificados las evaluaciones de riesgo.
- "Realizar periódicamente auditorías internas del SGSI en intervalos planificados para determinar si los controles, procesos y procedimientos del SGSI mantienen la conformidad con los requisitos de ISO 27001:2005, el entorno legal y los requisitos y objetivos de seguridad de la organización, están implementados y mantenidos con eficacia y tienen el rendimiento esperado." (iso27000, 2012).
- Revisar periódicamente el SGSI, para garantizar que el alcance definido sigue siendo el adecuado este proceso esta delegado por parte de la dirección.
- "Actualizar los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitorización y revisión.
- Registrar acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del SGSI." (iso27000, 2012)

2.1.3.4 Act: La organización deberá regularmente *Mantener y Mejorar:*

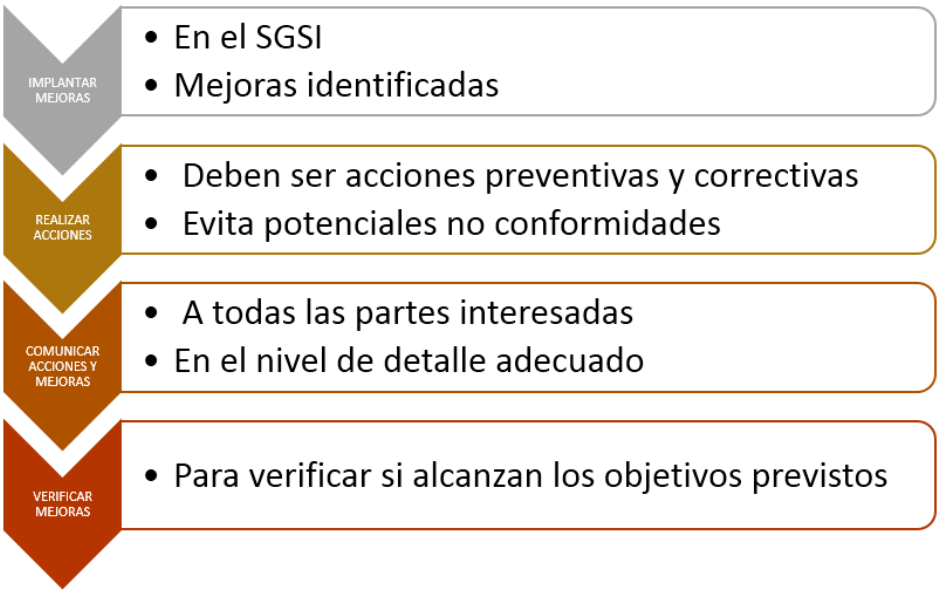

Figura 7 Procesos de ACT, para mantener y mejorar
Elaborado por: Ing. Viviana Tixilima

2.1.4 Elementos de gestión de la seguridad de los sistemas de información.

2.1.4.1 Identificación de activos.

"Se denominan Activos de Información a todos aquellos recursos de valor para una organización que generan, procesan, almacenan o transmiten información." (UNIVERSIDAD NACIONAL DE LUJAN).

Activos de información son:

Figura 8 Activos de un organización
Elaborado por: Ing. Viviana Tixilima

2.1.4.2 Identificación de amenazas a los activos.

Una amenaza puede ocasionar incidentes no deseados, provocando daños o pérdidas de todo tipo en una organización. Este tipo de amenazas puede proceder de:

- Ataques directos e indirectos sobre los sistemas de información
- medioambientales (inundaciones, rayos, terremotos)
- Robo de contraseñas

2.1.4.3 Identificación de vulnerabilidades.

Una vulnerabilidad se considera como una posibilidad de ocurrencia de una amenaza afectando a un activo. Las vulnerabilidades incluyen las debilidades en el nivel físico sobre la organización, los procedimientos, el personal, la gestión, la administración, los equipos, el software o la información.

"Las vulnerabilidades provocan debilidades en el sistema que pueden explotarse y dar lugar a consecuencias no deseadas" (Gaona Vásquez, 2013)

Las vulnerabilidades se clasifican:

- Físicas (presentes en los ambientes en los cuales la información se está almacenando o manejando)
- Naturales (relacionados con las condiciones de la naturaleza)
- Hardware (posibles defectos en la fabricación o configuración de los equipos de la empresa)
- Software (puntos débiles de aplicaciones que permitan que ocurran accesos indebidos a los sistemas informáticos)
- Medios de almacenaje (soportes físicos o magnéticos que se utilizan para almacenar la información)
- Comunicación (abarca el tránsito de la información)
- Humanas (personas que puedan causar daños a la información a al ambiente tecnológico que la soporta)

2.1.4.4 Identificación de impactos.

"El impacto es la consecuencia de la materialización de una amenaza sobre un activo, como la destrucción de ciertos activos, el peligro de integridad del sistema de información, la perdida de autenticidad o de disponibilidad." (AREITIO, 2008)

2.1.4.5 Identificación de riesgos.

"El riesgo es la posibilidad de que se produzca un impacto determinado en un activo, o en toda la organización. Este impacto se puede producir debido a que una amenaza explote vulnerabilidades para causar pérdidas o daños. El riesgo se caracteriza por una combinación de dos factores: la probabilidad de que ocurra el incidente no deseado y su impacto." (AREITIO, 2008).

2.1.4.6 Identificación de riesgos residuales.

"El nivel de riesgo existente después de la implantación de salvaguardas se denomina riesgo residual; esto implica un análisis de si este tipo de riesgos son aceptables,

como parte del proceso en el que se establece el equilibrio entre la seguridad y las necesidades de una organización.” (AREITIO, 2008).

2.1.4.7 Aplicación de salvaguardas.

Las salvaguardas son contras medidas que se definen como aquellos procedimientos o mecanismos tecnológicos protegiendo contra una amenaza, reduciendo las vulnerabilidades; reduciendo así el riesgo.

2.1.4.8 Identificación de las limitaciones de aplicaciones de seguridad.

"Consiste en conocer las restricciones que existen en el entorno, que pueden afectar a las contramedidas y sistema de seguridad especialmente a las amenazas, a los riesgos ya a las salvaguardas. Las limitaciones son establecidas y reconocidas por la dirección de la organización y dependen del entorno en el que funcionan. Pueden ser organizativas, financieras, ambientales, de personal, de tiempo legales, técnicas, etc.” (AREITIO, 2008)

2.1.5 Norma ISO 27001.

“Es el modelo estándar desarrollado por ISO para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI de una organización.” (MOGUERZA, 2010).

La norma define claramente las pautas para poder diseñar un sistema de gestión de seguridad de la información; esta norma contempla diez dominios: (MELO, 2008).

Tabla 2 Dominios de la Norma ISO27001

1. **Política de seguridad de la información**
2. **Organización de la seguridad de la información**
3. **Gestión de activos**
4. **Seguridad de recursos humanos**
5. **Seguridad física y del entorno**
6. **Gestión de comunicaciones y operaciones**
7. **Control de acceso**
8. **Adquisición, desarrollo y mantenimiento de Sistemas de información**
9. **Gestión de Incidentes de la Seguridad de la Información**
10. **Cumplimiento**

Fuente: (MELO, 2008)

2.1.6 Metodología Magerit.

"Magerit es una metodología de Análisis de Riesgos de carácter público elaborada por el ministerio de administraciones públicas de España, cuyo objetivo es descubrir los riesgos a los que se encuentran expuestos los sistemas de información y recomendar las medidas apropiadas que se debería adoptarse para controlar estos riesgos." (GALINDO & MORALES, 2008)

La aplicación de Magerit permite:

- "Aportar racionalidad en el conocimiento del estado de seguridad de los Sistemas de Información.
- Garantizar una adecuada cobertura para que no haya elementos del sistema de información se queden fuera del análisis.
- Atenuar las insuficiencias de los sistemas vigentes

- Asegurar el desarrollo de cualquier tipo de sistema desde la planificación hasta la implantación y mantenimiento." (GALINDO & MORALES, 2008)

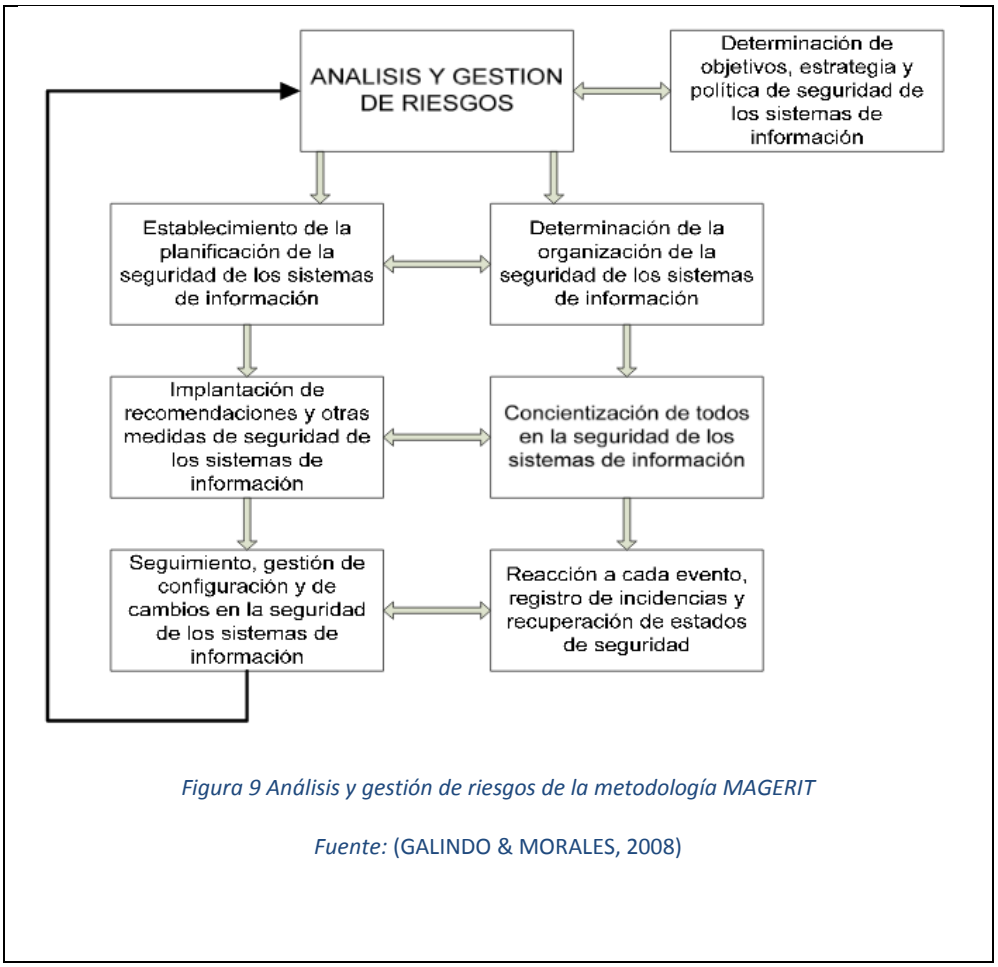

Figura 9 Análisis y gestión de riesgos de la metodología MAGERIT

Fuente: (GALINDO & MORALES, 2008)

2.1.7 Vulnerabilidades en una red LAN

"Una vulnerabilidad hace referencia a la debilidad de un sistema, donde se puede permitir a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones." (MÓNICA, 2014)

Tabla 3 Vulnerabilidades de una Red LAN

Integridad	
Amenazas	**Consecuencias**
• Datos modificados	• Información perdida

• Caballo de Troya • Memoria cambiada • Mensajes modificados (en tránsito)	• Máquina penetrada • Vulnerabilidad a otras amenazas

Confidencialidad

Amenazas	**Consecuencias**
• Mensajes escuchados en la red • Datos robados de servidores • Análisis de Tráfico • Detecta configuración de la red	• Perdida de privacidad • Revela contraseñas • Identifica patrones de acceso • Facilita otros ataques

Denial of Service

Amenazas	**Consecuencias**
• Procesos matados • Inundación con paquetes • Llenado de discos • Aislamiento de máquinas (DNS)	• Molestias • Interferencia con trabajo

Autentificación

Amenazas	**Consecuencias**
• Identidades falsas • Datos falsos	• Acciones atribuidas al usuario • Daño al nombre institucional

Realizado por: Ing. Ing. Viviana Tixilima

2.2 ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA RED DE LA UNIVERSIDAD POLITÉCNICA SALESIANA CAMPUS SUR

2.2.1 Análisis de la situación actual

"La Universidad Politécnica Salesiana creada mediante Ley N° 63 expedida por el Congreso Nacional y publicada en el registro oficial N° 499 del 5 de agosto de 1994,

es una institución de derecho privado sin fines de lucro, con personería jurídica propia y autonomía responsable, académica, administrativa, financiera, y orgánica. Su domicilio se hallar en la ciudad de Cuenca, con sedes en las ciudades de Quito y Guayaquil." (UNIVERSIDAD POLITECNICA SALESIANA, 2012).

La Universidad está conformado por un cuerpo colegiado que está estructurado de la siguiente forma:

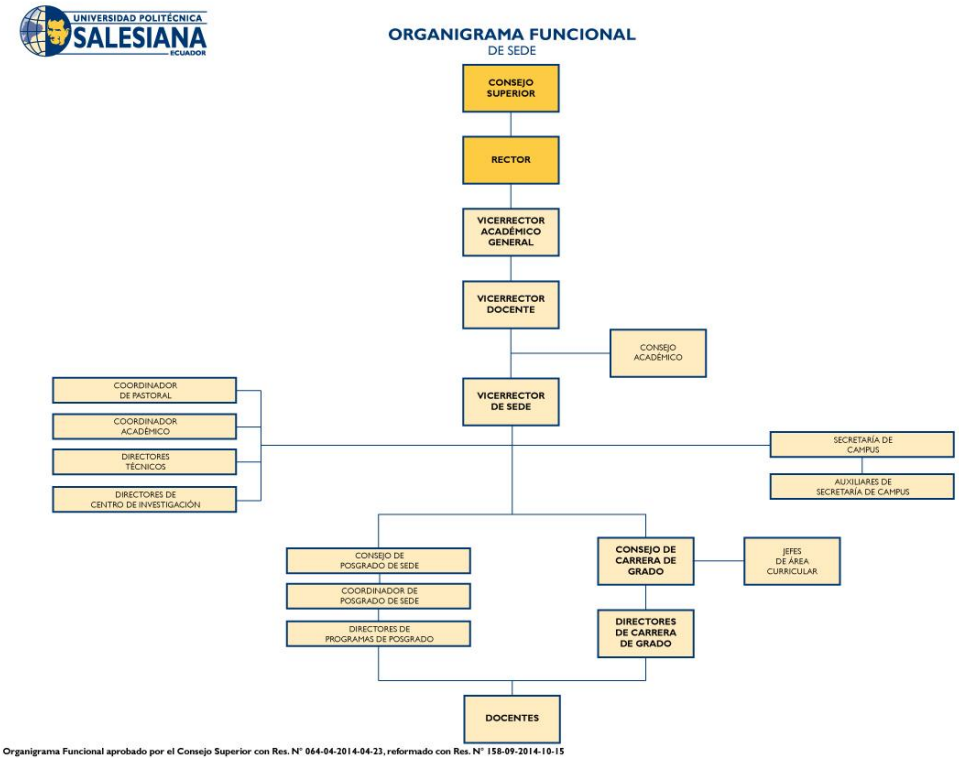

Figura 10 Organigrama Funcional aprobado por consejo superior
Fuente: (UPS, 2014)

La sede Quito está constituida por tres Campus: Campus Kennedy, Campus El Girón, y Campus Sur. Dentro de los cuales el flujo de tráfico que circular a través de la su infraestructura es:

- Telefonía IP
- Ambientes virtuales de aprendizaje AVAC
- Portal Institucional.
- Video de Cámaras IP
- Sistema Nacional Académico SNA

- Sistema de Talento Humano SIGAG
- Sistema Financiero SQUAD.

El campus Sur está conformado por 8 bloques identificados desde la A hasta el H: Bloque A, Bloque B, Bloque C, Bloque D, Bloque E, Bloque F, Bloque G y Bloque H. (ALEJANDRO & LUIS, 2015). En este campus se desarrollan las carreras técnicas tales como:

- Ingeniería Ambiental
- Ingeniería Civil
- Ingeniería Electrónica
- Ingeniería Eléctrica
- Ingeniería en Gerencia y Liderazgo
- Ingeniería Mecánica
- Ingeniería de Sistemas

Dichas carreras al periodo de evaluación Octubre 2015 – Marzo 2016 cuentan con la siguiente población de estudiantes y cuerpo de docentes:

Tabla 4 Población de estudiantes del Campus Sur

CARRERAS	**Número de Estudiantes**	**Número de docentes**
Ingeniería de Sistemas	551	40
Ingeniería Civil	520	36
Ingeniería Electrónica	772	53
Ingeniería Ambiental	432	36
Ingeniería Mecánica	138	17
Ingeniería Eléctrica	168	14

Ingeniería en Gerencia y Liderazgo	357	31

Fuente: datos extraídos del SNA

Teniendo una población total de 2938 estudiantes de los cuales aproximadamente el 70.45% es decir 2070 estudiantes,

La planta docente que labora en el Campus Sur es de 227 docentes, de los cuales aproximadamente el 80% es decir 182 docentes laboran en el horario de lunes a viernes de 07:00 am a 07:30 pm, mientras que aproximadamente el 20%, es decir 45 docentes laboran en el horario nocturno de lunes a viernes de 7:30 pm a 9:30 pm, y los sábados de 07:00 am a 03:00 pm.

Por otro lado el personal administrativo está constituido por los departamentos de Secretaria, Tesorería, Biblioteca, Laboratorios, Informática, Bienestar Estudiantil y Administrativo, su población está conformada de la siguiente forma:

Tabla 5 Personal administrativo del Campus Sur

Departamentos	**Número de personal**
Secretaría	12
Tesorería	2
Biblioteca	5
Laboratorios	10
Informática	3
Bienestar estudiantil	4
Administrativo	6

Fuente: Datos obtenidos de GTH

La población del personal administrativo es de 38 personas aproximadamente, de las cuales el 97.48% laboran en el horario de 08:30 a 17:30 y el 2.52% restante en el horario de 13:30 a 21:30.

2.2.2 Identificación de recursos.

EL Campus Sur al estar conformado por varios bloques, requiere de una infraestructura capaz de brindar el servicio de acceso a la red, razón por la cual mantiene los siguientes equipos de conmutación de paquetes, tal como se describe en la Tabla 4.

Tabla 6 Identificación de recursos de la red del Campus Sur

RECURSO	**UBICACIÓN**	**NOMBRE**	**FUNCIÓN**
Switch cisco WS-C6506-E	MDF - Bloque A	MSF-SUR	Switch de Core,
Switch cisco WS-C2960S	IDF - Bloque D IDF - Bloque A Piso 4 IDF - Bloque A Piso 5	IDF-PB-CISCO IDF-A-P4 IDF-A-P5	Switch de Distribución
Switch cisco WS-C3750 POE	SDF - Bloque A Piso 4 SDF – Bloque A Planta Baja SDF – Bloque A Planta Baja SDF – Bloque A Biblioteca SDF - Bloque B Piso 1 SDF - Bloque B Planta Baja SDF - Bloque F Piso 1 SDF - Bloque C	SDF-A-P4-1 SDF-A-PB SDF-A-PB-24p SDF-A-SB SDF-BB-P1-2 SDF-BB-PB SDF-BF-P1-1 SDF-BLOQUE-C	Switch de acceso

Switch cisco WS-C3750	SDF - Bloque H	SDF-BLOQUE-H	Switch de acceso
Switch cisco WS-C2960	SDF - Bloque A Piso 4 SDF - Bloque B	SDF-A-P4-1 SDF-BB-P1	Switch de acceso
Switch 3com SS3-3226	SDF - Bloque E	SDF-LAB-SUELOS	Switch de acceso

Fuente: (ALEJANDRO & LUIS, 2015)

El Backbone principal del Sistema de cableado vertical del Campus Sur, está conformado por fibra óptica multimodo 62.5/125 micrones, trabajando a 1300 nm, con un ancho de banda de 500 MHz/Km y atenuación máxima de 1.5 dB/Km

La red del Campus Sur también está integrada por puntos de acceso inalámbricos, ya que tanto docentes como estudiantes, acceden cada vez más, a la red a través de sus equipos móviles tales como: laptos, tablets, celulares, etc. mediante la red WIFI. En la actualidad se cuenta con 34 Access Point distribuidos en los bloques del campus Sur.

2.2.3 Infraestructura de la seguridad de la información.

La Red del Campus Sur cuenta con un CISCO ASA 5515-x, dispositivo que proporciona servicios de seguridad altamente integrados, posee las siguientes características:

- Peers VPN IPSec: 250
- Peers VPN SSL: 2
- Sesiones concurrentes: 250000
- Interfaces virtuales (VLAN): 100
- Contexto de seguridad: 2
- Capacidad del cortafuegos: 1.2 Gbps
- Capacidad de VPN (3DES/AES): 250 Mbps

2.2.4 Principales funciones del campus.

EL Campus de la Universidad Politécnica mantiene dentro de sus funciones las siguientes:

- La docencia
- La investigación
- La extensión
- La planificación
- La administración

Todas estas funciones se apoyan mediante la utilización de herramientas de Tecnologías de la Información y Comunicación TIC´s. tales como: SNA, SIGAG, SQUAD y portal institucional.

CAP. III: ANÁLISIS Y GESTIÓN DE RIESGOS DE LA UNIVERSIDAD POLITÉCNICA SALESIANA

3.1 Análisis de Riesgos

3.1.1 Identificación de Activos

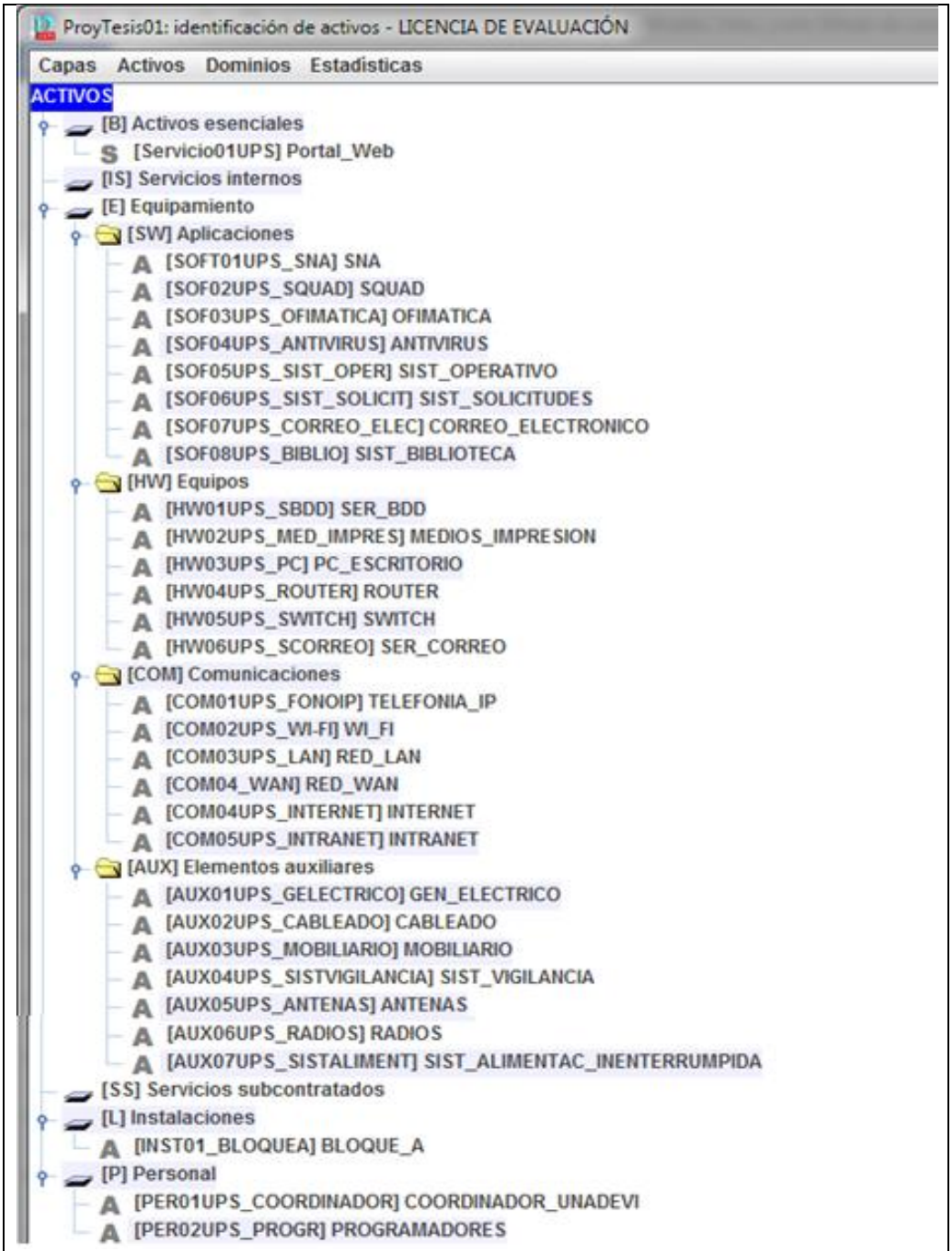

Figura 11 Identificación de activos. Realizado en PILAR 5.4.7

Realizado por: Ing. Viviana Tixilima

3.1.1.1 Dependencia entre activos

"Las dependencias se usan para propagar el valor (es decir, los requisitos de seguridad) desde los activos valiosos (arriba) a los activos que soportan el valor por delegación (abajo)." (PILAR / ayuda, s.f.)

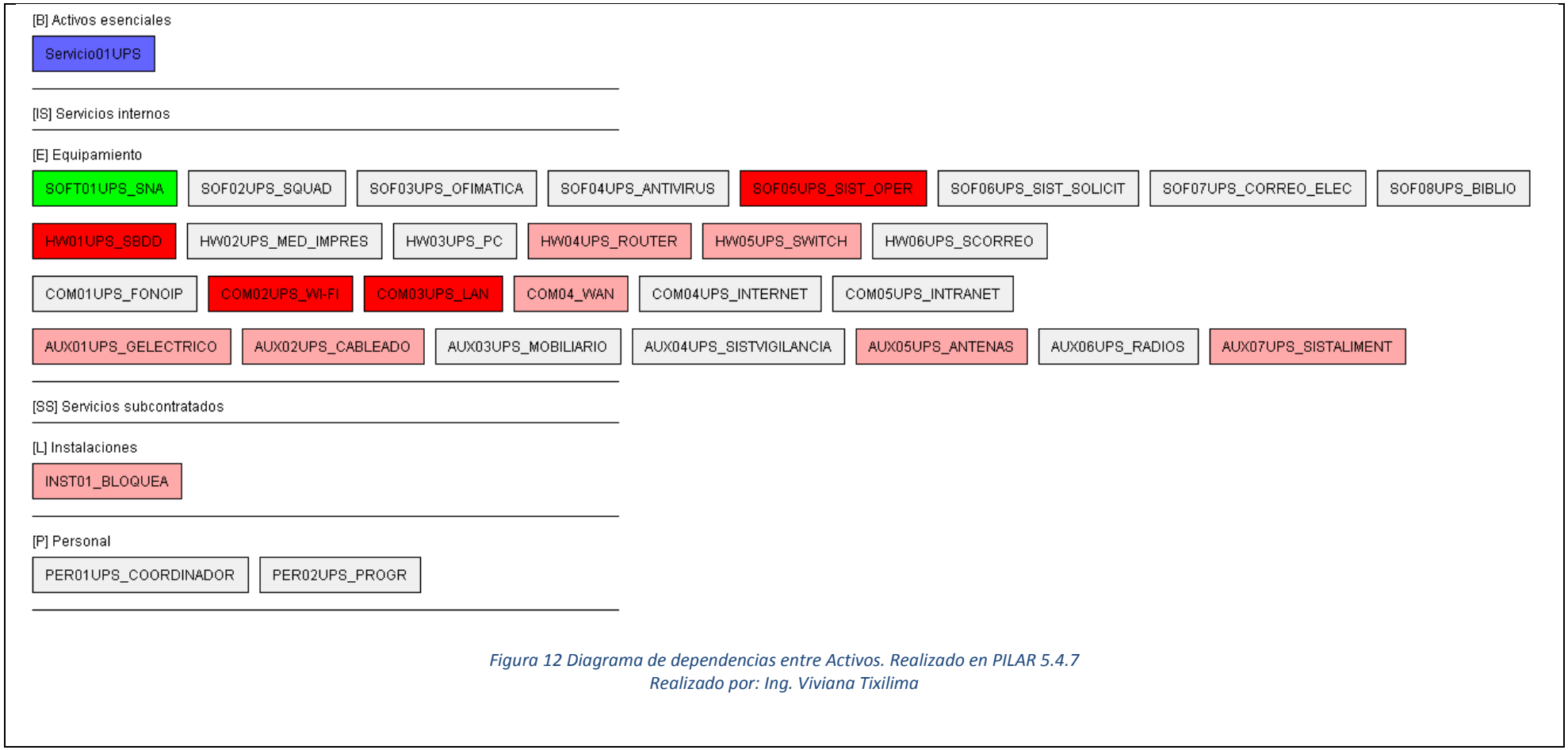

Figura 12 Diagrama de dependencias entre Activos. Realizado en PILAR 5.4.7
Realizado por: Ing. Viviana Tixilima

Donde los activos están evaluados bajos los siguientes criterios:

Tabla 7 Criterios de evaluación

COLOR	DESCRIPCIÓN
azul claro	activos superiores relacionados indirectamente
azul fuerte	activos superiores relacionados directamente
Verde	el activo seleccionado
rojo fuerte	activos inferiores relacionados directamente
rojo claro	activos inferiores relacionados indirectamente
Gris	sin relación

Realizado por: Ing. Viviana Tixilima

3.1.1.2 Valoración de los Activos

Para la valoración de activos se debe establecer algunos criterios de Valoración, los mismos que van a ser evaluados dentro de un rango de 10 a 0, donde el nivel más alto representa un alto riesgo, mientras que el nivel 0 presenta un riesgo despreciable, tal como se muestra en la siguiente tabla:

Tabla 8 Criterios de Valoración

Nivel	Criterio
10	Nivel 10
9	Nivel 9
8	Nivel 8 (+)
7	Alto
6	Alto (-)
5	Medio (+)
4	Medio
3	Medio (-)
2	Bajo (+)
1	Bajo
0	Despreciable

Fuente: herramienta PILAR 5.4.7

Dimensiones

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

- [T] trazabilidad del servicio y de los datos

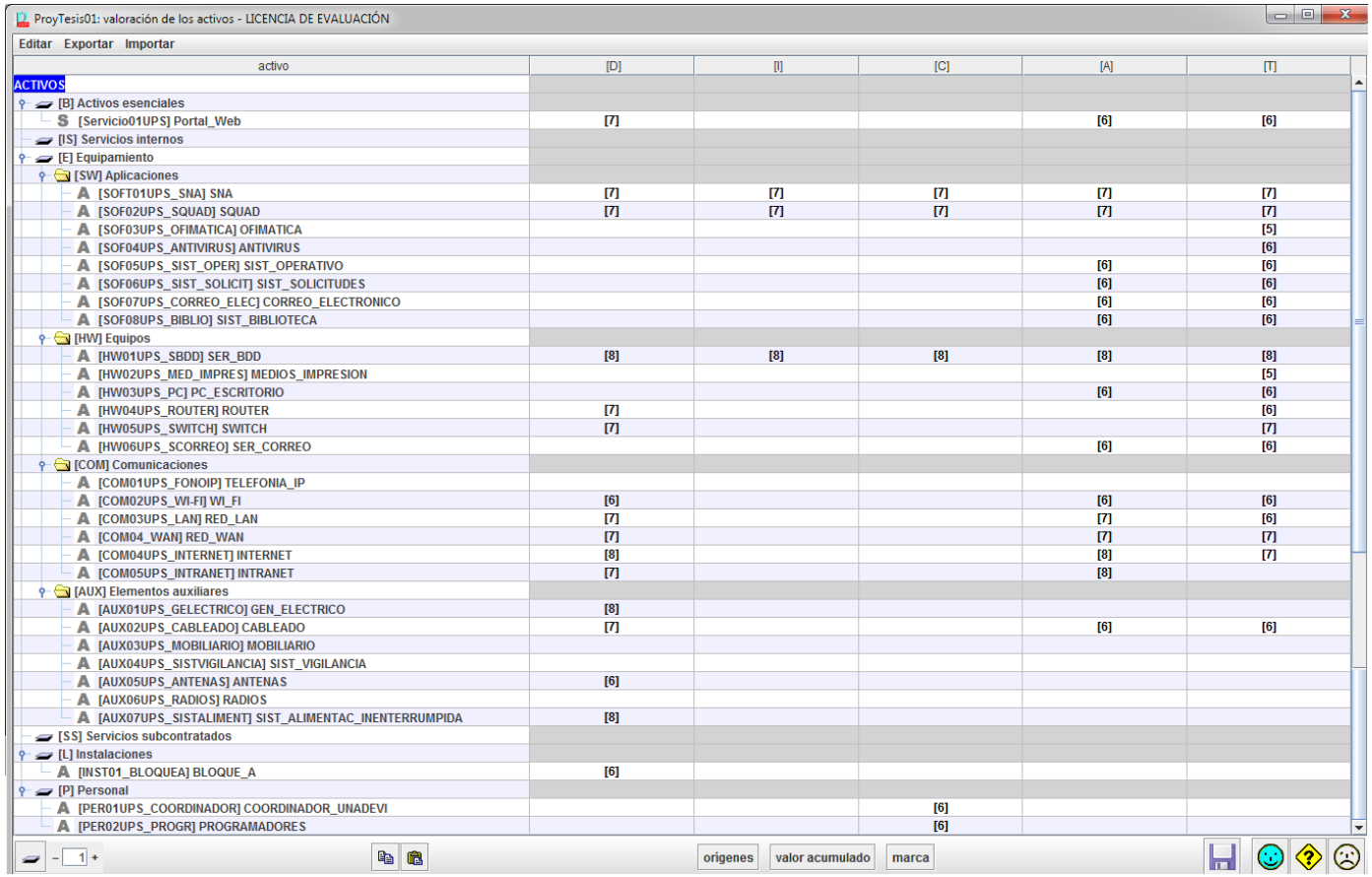

Figura 13 Valoración de activos. Realizado en PILAR 5.4.7

Realizado por: Ing. Viviana Tixilima

3.2 DISEÑO DEL MODELO DE POLITICAS

3.2.1 Diseño del modelo de políticas.

El Modelo de Políticas de Seguridad está basado en el Anexo A de la Norma ISO 27001

Tabla 9 Políticas de seguridad para el Campus Sur

"A.5 Políticas de seguridad de la información"			
"A.5.1 Gestión de la Gerencia para la seguridad de la información "			
"Objetivo: Brindar orientación y apoyo por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes."			
Cód.	**Nombre**	**Control**	**Actividades necesarias**
"A.5.1.1"	"Políticas de seguridad de la información"	"La gerencia debe definir, aprobar, publicar y comunicar a los trabajadores y partes externas involucradas, una serie de políticas para la seguridad de la información."	• Identificar claramente los activos y los procesos de seguridad asociados con cada sistema específico • Nombrar al responsable de cada activo o proceso de seguridad • Documentar los detalles de cada responsabilidad • Definir y documentar claramente los niveles de autorización • Aprobar y respaldar el documento por parte de la Dirección • Las políticas deben ser conocidas y aceptadas por los afectados • Todo el personal de la organización tiene acceso al documento
"A.5.1.2"	"Revisión de las políticas de seguridad de la información"	"Las políticas de seguridad de la información deben ser revisadas en intervalos planificados o	• Identificar no conformidades e incumplimientos

		si ocurren cambios significativos, para garantizar su idoneidad, adecuación, y efectividad continuos."	• Revisar periódicamente el cumplimiento por parte del personal
"A.6.1 Organización interna"			
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.			
Cód.	**Nombre**	**Control**	**Actividades necesarias**
A.6.1.1	Funciones y responsabilidades de la seguridad de la información	Se deberían definir y asignar todas las responsabilidades de la seguridad de la información.	• Definir un comité de seguridad de la información y que está respaldado por la dirección • Definir claramente las funciones de seguridad • Aprobar las designaciones de responsables de seguridad • Identificar los objetivos de seguridad • Revisar, evaluar y aprobar la normativa de seguridad
A.6.1.2	Segregación de tareas	Tareas y áreas de responsabilidad en conflicto deben ser segregadas para reducir las posibilidades de modificación no autorizada o involuntaria, o el uso indebido de los activos de la organización	• Definir responsable(s) de la información, responsable(s) de los servicios, responsable de la seguridad de la información y responsable del sistema • Asignar responsabilidades para la seguridad de la información • Identificar claramente los activos y los procesos de seguridad asociados con cada sistema específico • Nombrar al responsable de cada activo o proceso de seguridad • Documentar los detalles de cada responsabilidad

			• Definir y documentar claramente los niveles de autorización
A.6.1.3	Contacto con las autoridades	Se deben mantener los contactos adecuados con las autoridades pertinentes.	• Mantener contactos con los organismos reguladores • Mantener contactos con los proveedores de servicios de información • Mantener contactos con los operadores de telecomunicaciones
A.6.1.4	Contacto con grupos de especial interés	Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	• Mantener contactos con los organismos reguladores • Mantener contactos con los proveedores de servicios de información • Mantener contactos con los operadores de telecomunicaciones • Participar en foros de seguridad
A.6.2 Equipos móviles y trabajo a distancia			
Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.			
Cód.	**Nombre**	**Control**	**Actividades necesarias**
A.6.2.1	Política para dispositivos móviles	Se debe adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	• Los dispositivos móviles activados se configuran de forma segura • Se comprueba que son compatibles con los demás dispositivos del sistema • Los dispositivos se identifican y autentican antes de conectarse al sistema. • Se requiere autorización para que medios y dispositivos tengan acceso a redes y servicios. • Se desactiva el modo de conexión ad-hoc en los dispositivos de usuario

			• Se autentican los dispositivos wireless (filtrado MAC, servidor de autenticación, etc.)
A.6.2.2	Trabajo a distancia	Se debe implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza a distancia.	• Restringir la administración remota • Emplear protocolos seguros para la administración remota • Emplear autenticación fuerte para administración remota
A.7 Seguridad de los recursos humanos			
A.7.1 Antes de asumir el empleo			
Objetivo: Asegurar que los empleados y contratistas comprendan sus responsabilidades y son idóneos en los roles para los que se consideran.			
Cód.	**Nombre**	**Control**	**Actividades necesarias**
A.7.1.1	Selección	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberían llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.	• Comprobar previamente que el personal cumple los requisitos del puesto • Comprobar periódicamente que el personal con puestos de gran responsabilidad cumple con los requisitos del puesto • Habilitar seguridad de acuerdo al grado de clasificación de la información que se maneja
A.7.1.2	Términos y condiciones del empleo	Los acuerdos contractuales con empleados y contratistas, deberían establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	• Realizar una inclusión del ámbito, el alcance y el periodo de las responsabilidades en materia de seguridad • Realizar un compromiso escrito del cumplimiento de la política y la normativa correspondiente
A.7.2 Durante el trabajo			
Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.			

Cód.	Nombre	Control	Actividades necesarias
A.7.2.1	Responsabilidades de la dirección	La dirección debe exigir a todos los empleados y contratistas a aplicar la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización	• Definir claramente las funciones de seguridad • Aprobar las designaciones de responsables de seguridad • Identificar los objetivos de seguridad • Asegurar la coordinación en materia de seguridad dentro de la organización
A.7.2.2	Concientización, educación y capacitación sobre la seguridad de la información	Todos los empleados de la organización y los contratistas, si así lo requiriesen, deben recibir una adecuada educación de concientización y capacitación, así como actualizaciones regulares sobre las políticas y procedimientos organizacionales, de acuerdo a las funciones de trabajo que desempeñen.	• Dar a conocer los contenidos de las normativas de seguridad mediante medios y actividades como: Charlas, paneles de difusión, foros • Programar un curso formal de Capacitación
A.7.2.3	Procesos disciplinarios	Se debe contar con un proceso disciplinario formal el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información	• Establecer un régimen sancionador por incumplimiento • Realizar una difusión del procedimiento sancionador
A.7.3 Término y cambio de empleo			
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o término del empleo.			
Cód.	**Nombre**	**Control**	**Actividades necesarias**
A.7.3.1	Terminación o cambio de responsabilidades de empleo	Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de contrato se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	• Realizar una entrevista previa a la finalización o cambio del contrato • Recuperar los elementos de seguridad a devolver (llaves, tarjetas, etc.) • Comunicar de la baja o cambio a los responsables de seguridad, y administradores del sistema

A.8 Gestión de los Activos			
A.8.1 Responsabilidades sobre los activos			
Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.			
Cód.	**Nombre**	**Control**	**Actividades necesarias**
A.8.1.1	Inventario de activos	Se deben identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos	• Actualizar regularmente el inventario cuando: • Cuando entran nuevos sistemas de información • Cuando se retiran sistemas de información • Cuando entran aplicaciones • Cuando hay cambios en las aplicaciones • Cuando se retiran aplicaciones • Cuando entra equipamiento • Cuando hay cambios en el equipamiento • Cuando se retira equipamiento • Cuando entran servicios de comunicaciones • Cuando hay cambios en los servicios de comunicaciones • Cuando se retiran servicios de comunicaciones de producción • Cuando se estrenan nuevas instalaciones • Cuando hay cambios en las instalaciones • Cuando se cierran instalaciones
A.8.1.2	Propiedad de los activos	Los activos mantenidos en el inventario deben tener un propietario.	• Identificar claramente los activos y los procesos de seguridad asociados con cada sistema específico • Nombrar al responsable de cada activo o proceso de seguridad

			• Documentar los detalles de cada responsabilidad • Definir y documentar claramente los niveles de autorización
A.8.1.3	Uso aceptable de los activos	Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	• Identificar claramente los activos y los procesos de seguridad asociados con cada sistema específico • Nombrar al responsable de cada activo o proceso de seguridad • Documentar los detalles de cada responsabilidad
A.8.1.4	Devolución de activos	Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	• Realizar una entrevista previa a la finalización o cambio del contrato • Recuperar los elementos de seguridad a devolver (llaves, tarjetas, etc.) • Asegurar que la persona que recibe los activos, es la responsable y que al momento de la entrega estén en perfectas condiciones, exceptuando las salidas para fines de reparación.
A.8.2 Clasificación de la información			
Objetivo: Garantizar que la información reciba un nivel adecuado de protección de acuerdo a su importancia dentro de la organización			
Cód.	**Nombre**	**Control**	**Actividades necesarias**
A.8.2.1	Clasificación de la información	La información se debe ser clasificada en términos de los requisitos y valores legales, siendo crítica y sensible ante la divulgación y modificación no autorizada.	• Se requiere una habilitación de seguridad de acuerdo al grado de clasificación de la información que se maneja

A.8.2.2	Etiquetado de la información	Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	• Disponer de normativas sobre el manejo de información compartida • Disponer de normativas de manejo de información sensible en función de la seguridad que proporcionan los medios
A.8.2.3	Manejo de activos	Se debe desarrollar e implementar procedimientos para el manejo de activos, Se deberían desarrollar e implementar procedimientos para el manejo de activos, información adoptada por la organización.	• Identificar: • Cuáles son los sistemas y activos críticos. • Cómo se regula cada uno de ellos. • Cómo se comporta cada uno de estos sistemas y activos.
A.8.3 Manejo de los medios de comunicación			
Objetivo: Prevenir la divulgación, modificación, retiro o destrucción no autorizada de la información almacenada en los medios de comunicación			
Cód.	**Nombre**	**Control**	**Actividades necesarias**
A.8.3.1	Gestión de medios removibles	Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	• Definir estándares a utilizar para los distintos medios removibles, evaluar y autorizar el uso proponer configuraciones de seguridad para los medios removibles • Formatear medios externos y pendrive a solicitud del usuario • Todo medio removible debe ser escaneado mediante antivirus cada vez que sea conectado a un equipo de la red • Almacenar información sensible mediante herramientas de cifrado • Los medios removibles deben almacenarse en un ambiente seguro, de acuerdo a las especificaciones de los fabricantes • La información almacenada en medios removibles que requiera estar disponible

			después del tiempo de vida del medio, debe ser almacenada en cualquier otro medio de manera de garantizar que no exista perdida de información
A.8.3.2	Disposición de los medios	Los medios de comunicación deben ser desechados de manera segura cuando ya no sean necesarios, utilizando procedimientos formales.	• Destruir los medios removibles bajo las normas ambientales vigentes
A.8.3.3	Transferencia física de los medios de comunicación	Los medios que contienen información se deberían proteger contra acceso no autorizado, uso indebido o corrupción durante su transporte.	• Disponer de normativas sobre el manejo de los medios que contienen información • Disponer de normativas de manejo de información sensible en función de la seguridad que proporcionan los medios
A.9 Control de Acceso			
A.9.1 Requisitos del negocio sobre el control de acceso			
Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.			
Cód.	**Nombre**	**Control**	**Actividades necesarias**
A.9.1.1	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	• Impedir el acceso no autorizado a los sistemas de información, base datos y servicios de información. • Implementar seguridad en los accesos a usuarios por medio de técnicas de autenticación y autorización • Controlar la seguridad en la conexión entre la red de la institución y otras redes • Registrar y revisar eventos y actividades criticas llevadas a cabo por los usuarios en los sistemas

			• Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos
A.9.1.2	Acceso a las redes y a los servicios de las redes	Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	• Establecer políticas de uso de los servicios de red • Crear autenticaciones para conexiones externas • Realizar identificación de equipos en la red • Proteger puertos de diagnóstico remoto y configuración • Segregar las redes • Controlar la conexión a las redes
A.9.2 Gestión del acceso al usuario			
Objetivo: Garantizar el acceso al usuario autorizado para evitar el acceso no autorizado a los sistemas y servicios.			
Cód.	**Nombre**	**Control**	**Actividades necesarias**
A.9.2.1	Registro y cancelación del registro de usuarios	Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, los derechos de acceso.	• Crear nuevas cuentas de usuarios • Activar cuentas de usuario • Modificar cuentas de usuario • Suspender temporalmente las cuentas de usuario • Las cuentas que ya no son necesarias se eliminan o se bloquean • No reutilizar los identificadores
A.9.2.2	Provisión de acceso al usuario	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.	• Comprobar la identidad de los usuarios y los privilegios requeridos antes de entregar el autenticador • Limitar el número de autenticadores necesarios por usuario • Distribuir los autenticadores de forma segura

			• Comprometer por escrito al usuario a mantener la confidencialidad del autenticador • El usuario debe confirmar la recepción del autenticador • El usuario se hace cargo personalmente del control del autenticador
A.9.2.3	Gestión de derechos de acceso privilegiado	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	• Crear cuentas específicas para administradores del sistema • Crear cuentas específicas para administradores de seguridad • Crear cuentas específicas para actividades de auditoría • Crear cuentas especiales sujetas a procesos específicos de gestión
A.9.2.4	Gestión de información de autenticación secreta de usuarios	La asignación de la información secreta se debe controlar por medio de un proceso de gestión formal.	• Crear un proceso de gestión formal para controlar la asignación de información de autenticación secreta de usuarios.
A.9.2.5	Revisión de los derechos de acceso de usuarios	Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares.	• Disponer de mecanismo(s) de control de los derechos de acceso (privilegios) • Disponer de derechos de acceso para auditar la calidad y exactitud del trabajo realizado; por parte de los propietarios de los activos

A.9.2.6	Retiro o ajuste de los derechos de acceso	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	• Quitar los derechos de acceso a la información y a las instalaciones de procesamiento de la información al término de la relación laboral • Remover o suspender los activos asociados con instalaciones y servicios de procesamiento de información al termino de la relación laboral • Eliminar los derechos de acceso incluyendo accesos físicos y lógicos. • Cambiar las contraseñas conocidas para los identificadores de usuario que permanezcan activas
A.9.3 Responsabilidades del usuario			
Objetivo: Hacer a los usuarios responsables de salvaguardar la autenticación de su información.			
Cód.	**Nombre**	**Control**	**Actividades necesarias**
A.9.3.1	Uso de información secreta de autenticación	Se debe solicitar a los usuarios seguir las prácticas de la organización sobre el uso de la información secreta de autenticación.	• Comprometer a los usuarios al cumplimiento de las políticas de seguridad en el uso de la información de autenticación secreta.
A.9.4 Control de acceso a sistemas y aplicaciones			
Objetivo: Evitar el acceso no autorizado a los sistemas y aplicaciones			
Cód.	**Nombre**	**Control**	**Actividades necesarias**
A.9.4.1	Restricción del acceso a la información	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	• Solicitar autorización previa • No acceder a la información sin una verificación previa de los derechos de acceso

			• Establecer menús específicos para controlar los accesos a las funciones de las aplicaciones • Controlar los privilegios de los usuarios (lectura, escritura, modificación, borrado, ejecución)
A.9.4.2	Procedimiento de ingreso seguro	Se así lo requiere la política de control del acceso, se debe controlar el acceso a los sistemas y a las aplicaciones, mediante un procedimiento seguro de logueo.	• Identificar los perfiles de acceso y sus privilegios asociados • Aprobar los derechos de acceso el propietario del servicio o de la información • Los usuarios reconocen por escrito que conocen y aceptan sus derechos • Separar las responsabilidades de administración y operación • Mantener un registro de los privilegios de acceso • Mantener los privilegios asociados a cada usuario • Anular los privilegios cuando termina la autorización • Revisar los privilegios cuando el usuario cambia de responsabilidades o de función • Anular los privilegios cuando el usuario abandona la organización

A.9.4.3	Sistema de gestión de contraseñas	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	• Seleccionar contraseñas fáciles de recordar pero de difícil conjetura • Responsabilizar a los usuarios de la confidencialidad de las contraseñas • Disponer de un mecanismo para la comprobación de la robustez de las contraseñas • No se reciclar contraseñas usadas con anterioridad • Las contraseñas deben tener una duración limitada • Las contraseñas de usuarios administradores se deben cambian con mayor frecuencia • Las contraseñas deben ser modificadas al ser comprometidas o existir sospecha de ello
A.9.4.4	Uso de programas utilitarios privilegiados	Se debe restringir y controlar severamente el uso de programas utilitarios que puedan controlar manualmente el sistema y los controles de aplicación.	• Restringir y controlar el uso de los programas de utilidad que tengan la capacidad de sobrepasar los controles del sistema y de la aplicación • Usar procedimientos de identificación, autorización y autenticación para los programas utilitarios • Segregar los programas de aplicación de los programas utilitarios • Limitar el uso de programas a usuarios confiables y autorizados

A.9.4.5	Control de acceso a códigos fuente de programas	Se debe restringir el acceso al programa de código fuente.	• Controlar el acceso al código fuente • Nombrar un responsable del código fuente para cada aplicación • Requerir autorización previa para la actualización y entrega de código fuente a programadores • Proteger físicamente los listados de programas • Registrar el acceso al código fuente • Controlar la realización de copias de seguridad del código fuente • El código fuente no está accesible en los sistemas en producción
A.10 Criptografía			
A.10.1 Controles de la criptografía			
Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger a confidencialidad, la autenticidad y/o la integridad de la información.			
Cód.	**Nombre**	**Control**	**Actividades necesarias**
A.10.1.1	Política sobre el uso de controles criptográficos	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	• Tomar en cuenta los requisitos de aplicabilidad (confidencialidad, integridad, autenticidad y no repudio) • Identificar el nivel requerido de protección (basado en la asignación de riesgos) • Tomar en cuenta el uso de encriptación para la información transmitida por líneas de comunicación públicas, o para la información transportada en dispositivos de medios removibles o móviles.

A.10.1.2	Gestión de las claves	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las claves criptográficas durante todo su ciclo de vida.	• Incluir requisitos para la gestión de claves criptográficas • Incluir la generación, almacenamiento, distribución, retiro y destrucción de claves
A.11 Seguridad física y medioambiental			
A.11.1 Áreas seguras			
Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.			
Cód.	**Nombre**	**Control**	**Actividades necesarias**
A.11.1.1	Perímetro de seguridad física	Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o crítica, e instalaciones de manejo de información.	• Definir los perímetros de seguridad, la ubicación y la fuerza de cada uno de ellos • Contar con una zona de recepción atendida por una o más personas, u otros medios para controlar el acceso físico al lugar o edificio • El acceso a ciertos sitios y edificios debe restringirse sólo al personal autorizado • Construir barreras físicas para impedir el acceso físico no autorizado y la contaminación ambiental • Contar con un sistema de alarma contra incendios • Instalar sistemas de detección de intrusos, adecuados de acuerdo con normativas nacionales, regionales o internacionales

A.11.1.2	Controles físicos de los ingresos	Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.	• Registrar la fecha y la hora de entrada y salida de las visitas • Supervisar a todas las visitas a menos que su acceso haya sido aprobado anteriormente • Autenticar la identidad de las visitas con un medio adecuado • Restringir el acceso a las áreas donde se procesa o almacena la información confidencial • Mantener y monitorear de manera segura un libro de registro físico o una auditoría de seguimiento electrónica de todo los accesos • Portar algún tipo de identificación todos los empleados, contratistas y visitas externas • Otorgar acceso restringido al personal de servicio y de apoyo a las áreas seguras o a las instalaciones de procesamiento de información confidencial
A.11.1.3	Seguridad de oficinas, salas e instalaciones	Se debería diseñar y aplicar seguridad física a oficinas, salas e instalaciones.	• Disponer de una normativa relativa a la protección de las instalaciones • Establecer normas de conducta (prohibición de fumar, beber, comer, etc)
A.11.1.4	Protección contra amenazas externas y medioambientales	Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	• Contar con protección contra daños causados por desastres naturales (inundación, terremoto, tsunami, tormenta eléctrica, etc.)

			• Contar con protección contra daños causados por ataque malicioso (explosión, revuelta civil, etc.) • Contar con protección contra accidentes u otras formas de desastres por causa humana.
A.11.1.5	Trabajo en áreas seguras	Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	• Impartir lineamientos para trabajar en áreas seguras.
A.11.1.6	Distribución de las zonas de carga	Se deben controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	• Controlar la utilización de las áreas de carga / descarga • Separar las áreas de carga / descarga de las áreas de seguridad • Separar las áreas de entrada y salida • Realizar una inspección del material entrante • La entrega o recepción de material fuera de las horas de trabajo deben estar justificadas y sujetas a procedimientos rigurosos de control
A.11.2 Equipos			
Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.			
Cód.	**Nombre**	**Control**	**Actividades necesarias**
A.11.2.1	Ubicación y protección de los equipos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.	• Ubicar o proteger el equipamiento de forma que se reduzcan los riesgos provocados por amenazas y peligros ambientales, y accesos no autorizados. • Impartir instrucciones relativas al consumo de alimentos, bebidas y tabaco en las

			cercanías de los medios de procesan y soportan información.
A.11.2.2	Servicios públicos de soporte	Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	• El equipamiento institucional debe estar protegido contra fallas en el suministro de energía y otras interrupciones causadas por fallas en los elementos de soporte.
A.11.2.3	Seguridad del cableado	Se debe proteger de cualquier interferencia, intercepción o daño al cableado de energía o telecomunicaciones que transfiere datos o que sirve de apoyo en los servicios de información.	• Disponer de planos actualizados del cableado • Etiquetar todos los elementos de cableado • Seguir un procedimiento para la modificación del cableado • Realizar un mantenimiento regular del cableado • Segregar el cableado de alimentación del de comunicaciones para evitar interferencias • Instalar filtros de protección frente a rayos • Emplear recubrimientos que no son inflamables ni tóxicos • Disponer de medidas frente a posibles robos
A.11.2.4	Mantenimiento de los equipos	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	• Canalizar el mantenimiento preventivo y correctivo de los equipos de cómputo, a través del área de Gestión Tecnológica
A.11.2.5	Retiro de los activos	Los equipos, información o software no se deben retirar de su sitio sin autorización previa.	• Solicitar una autorización formal previa al retiro del equipamiento, información o software.

A.11.2.6	Seguridad de los equipos y bienes fuera de las instalaciones	Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	• Requerir una autorización previa para el uso de equipos para tratamiento de información fuera de los locales de la Organización • Identificar a las personas autorizadas • Disponer de un registro de activos fuera de las instalaciones en cada momento • Registrar la salida • Registrar el retorno • Revisar regularmente la relación de equipos ausentes • Proteger técnicamente el activo antes de su salida • Revisar el activo a su regreso • Disponer de una póliza de seguro para los equipos fuera de su lugar de trabajo
A.11.2.7	Disposición o re-uso seguros de los equipos	Todos los equipos que contienen medios de comunicación la información deben ser revisados para garantizar que se haya extraído o que se haya sobre-escrito la información sensible y la licencia del software antes de desechar o re-usar el mismo.	• Verificar el equipo para asegurarse de que contiene o no medios de almacenamiento antes de su eliminación o reutilización. • Destruir, eliminar o sobrescribir mediante técnicas, los medios de almacenamiento que contienen información sensible o con derecho de autor para hacer que la información original no se pueda recuperar
A.11.2.8	Usuario de equipo abandonado	Los usuarios deben garantizar una adecuada protección a los equipos abandonados.	• Generar conciencia en los usuarios acerca de los requisitos de seguridad y los procedimientos para proteger los equipos desatendidos.

A.11.2.9	Política de escritorio y pantallas limpias	Se debe adoptar la política de escritorio limpio de papales y de medios de almacenamiento removibles y una política de pantalla limpia en las instalaciones de procesamiento de la información.	• Bloquear la estación de trabajo cada vez que un usuario se ausente de su lugar de trabajo • Guardar en un lugar seguro cualquier documento, medio magnético u óptico removible que contenga información confidencial • Retirar inmediatamente de las impresoras la información clasificada o sensible cuando esta sea impresa
A.12 Seguridad de las operaciones			
A.12.1 Procedimientos operacionales y responsabilidades			
Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.			
Cód.	**Nombre**	**Control**	**Actividades necesarias**
A.12.1.1	Procedimientos de operación documentados	Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesiten.	• Crear procedimientos documentados para las actividades operacionales asociadas con las instalaciones de procesamiento y comunicación de información, como procedimientos de inicio y cierre de sesión de computadores, respaldo, mantenimiento de equipos, manejo de medios, salas de computación y administración y seguridad de manejo de correo.
	Cambios en la gerencia	Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	• Identificar y registrar cambios significativos • Evaluar los posibles impactos, incluidos los impactos de seguridad en la información

			• Comunicar los detalles de los cambios a todas las personas pertinentes
A.12.1.3	Gestión de la capacidad	Para asegurar el desempeño requerido del sistema se debe hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.	• Identificar los requisitos de capacidad, considerando la criticidad para el negocio de cada sistema involucrado. • Aplicar el procedimiento de ajuste y monitoreo del sistema para garantizar y mejorar la disponibilidad y la eficiencia de los sistemas. • Considerar las proyecciones sobre los requisitos futuros, tendencias actuales y proyectadas en las capacidades de procesamiento de información de la organización.
A.12.1.4	Separación de ambientes de desarrollo, prueba y de operaciones	Se deben separar los ambientes de desarrollo, prueba y operación para reducir los riesgos de acceso o cambios no autorizados dentro del ambiente de operación.	• Definir y documentar las reglas de transferencia de software desde un estado de desarrollo al operacional • Ejecutar en distintos sistemas o procesadores de computador y en distintos dominios y directorio, el software de desarrollo • Probar los cambios a los sistemas operativos y aplicaciones en un entorno de pruebas • Utilizar distintos perfiles de usuario para los sistemas operacionales y de prueba
A.12.2 Protección contra el malware (programa malicioso)			
Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.			
Cód.	**Nombre**	**Control**	**Actividades necesarias**

A.12.2.1	Controles contra el malware	Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para protegerse contra códigos maliciosos.	• Establecer una política formal que prohíbe el uso de software no autorizado • Implementar controles que evitan o detectan el uso de software no autorizado • Implementar controles que eviten o detecten el uso de sitios web desconocidos o que se sospecha son maliciosos • Realizar revisiones periódicas del software y del contenido de los datos de los sistemas que apoyan los procesos críticos del negocio • Investigar formalmente la presencia de cualquier tipo de archivos o modificaciones no autorizados • Instalar y actualizar periódicamente un software que permita realizar la detección de malware
A.12.3 Backup			
Objetivo: Proteger la información contra la pérdida			
Cód.	**Nombre**	**Control**	**Actividades necesarias**
A.12.3.1	Backup de la información	Se deben hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptadas.	• Disponer de procedimientos para realizar copias de seguridad: • Procedimientos de copia • Procedimientos de restauración • Procedimientos de retención de copias de seguridad • Procedimientos de destrucción de copias de seguridad

			• Realizar copias de las aplicaciones críticas para el negocio • Realizar copias de los sistemas operativos en explotación • Verificar que las copias pueden ser restauradas correctamente • Almacenar las copias de seguridad se almacenan en lugares alternativos
A.12.4 Logueo y monitoreo			
Objetivo: Registrar eventos y generar evidencias			
Cód.	**Nombre**	**Control**	**Actividades necesarias**
A.12.4.1	Eventos de logueo	Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	• Registrar regularmente los registros de logueo, así como excepciones, faltas y eventos de seguridad de la información
A.12.4.2	Protección de la información del logueo	Se debe proteger contra la falsificación y el acceso no autorizado a los medios de logueo y a la información de logueo.	• Proteger las instalaciones de registro y la información de registro, para evitar alteraciones y accesos no autorizados
A.12.4.3	Logueo del administrador y operador	Debe loguearse las actividades del sistema del administrador y del operador, y los logs deben ser protegidos y revisados de manera regular.	• Revisar regularmente el registro de las actividades del operador y del administrador del sistema
A.12.4.4	Sincronización de los relojes	Se debe sincronizar a una sola fuente de tiempo de referencia, los relojes de todos los sistemas de procesamiento de la información correspondientes dentro de la organización o del dominio de seguridad.	• Utilizar una sola fuente horaria para sincronizar los relojes de todos los sistemas de procesamiento de información relevantes dentro de la organización o dominio de seguridad

A.12.5 Control del software operacional			
Objetivo: Asegurar la integridad de los sistemas operacionales.			
Cód.	**Nombre**	**Control**	**Actividades necesarias**
A.12.5.1	Instalación del software en los sistemas operacionales	Se deben implementar procedimientos para controlar la instalación del software en los sistemas operacionales.	• Estimar las necesidades de software. • Usar productos de software certificados o acreditados. • Realizar pruebas cuando se actualiza el software de base. • Se controla la instalación de software autorizado y productos con licencia. • Retener copias de las versiones anteriores de software como medida de precaución para contingencias.
A.12.6 Gestión de las vulnerabilidades técnicas			
Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.			
Cód.	**Nombre**	**Control**	**Actividades necesarias**
A.12.6.1	Gestión de las vulnerabilidades técnicas	Se debe obtener, de manera oportuna, información sobre las vulnerabilidades técnicas de los sistemas de información a ser utilizados; evaluar la exposición de la organización a dichas vulnerabilidades y tomar las medidas adecuadas para manejar los riesgos asociados.	• Disponer de personas dedicadas a la gestión de vulnerabilidades. • Prever mecanismos para informar de vulnerabilidades técnicas. • Utilizar Herramienta de análisis de vulnerabilidades. • Identificar las potenciales vulnerabilidades a partir del análisis previo. • Realizar pruebas para determinar la explotabilidad de vulnerabilidades identificadas. • Reparar urgentemente las vulnerabilidades que implican un alto riesgo.

			• Reparar con diligencia las vulnerabilidades que implican un cierto riesgo. • Identificar las vulnerabilidades en el uso del equipamiento de oficina (fotocopiadoras, FAX, etc.). • Identificar las vulnerabilidades del sistema.
A.12.6.2	Restricciones en la instalación de software	Se debe establecer e implementar las reglas que gobiernen la instalación del software.	• Instalar software no autorizado y/o productos sin licencia. • Software no transferido desde o hacia el ordenador central. • Instalar versiones no actualizadas o estables del software. • Instalar de software potencialmente dañino o de fuentes desconocidas.
A.12.7 Control del software operacional			
Objetivo: Minimizar el impacto de las actividades de las auditorias en los sistemas operacionales.			
Cód.	**Nombre**	**Control**	**Actividades necesarias**
A.12.7.1	Controles de la auditoria sobre los sistemas de información	Se debe planificar cuidadosamente los requisitos y actividades de la auditoria que involucren la verificación de los sistemas operacionales; y acordar minimizar las alteraciones a los procesos del negocio.	• Periódicamente, se debe realizar una auditoría. • Recoger pistas de auditoría, atendiendo a su validez, calidad y completitud. • La revisión debe ser ejecutada por un equipo de auditoría interna. • La revisión debe estar dada por un auditor / empresa especializado e independiente. • Tener en cuenta los requisitos de auditoría
A.13 Seguridad de las comunicaciones			
A.13.1 Gestión de la seguridad de las redes			
Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.			
Cód.	**Nombre**	**Control**	**Actividades necesarias**

A.13.1.1	Controles en las redes	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	• Identificar las redes y los servicios a los que se puede acceder. • Disponer de normativas relativas a las autorizaciones de acceso a las redes y servicios. • Disponer de normativas relativas a la protección de los accesos a las redes y servicios. • Se requiere autorización para que medios y dispositivos tengan acceso a redes y servicios.
A.13.1.2	Seguridad de los servicios de las redes	Se debe identificar los mecanismos de seguridad, los niveles del servicio y los requisitos de todos los servicios de redes e incluirlos en los acuerdos de servicios de redes, ya sea que los servicios sean proporcionados por la misma organización o por un tercero.	• Realizar pruebas cuando se conecta el sistema a nuevas redes. • Forzar el uso por usuarios de redes externas de ciertos sistemas de información específicos y / o pasarelas (gateways) de seguridad. • Aplicar restricciones al protocolo SNMP en redes wireless. • Establecer un control de conexión a las redes.
A.13.1.3	Segregación en las redes	Se deben segregar grupos de servicios de información, usuarios y sistemas de información.	• Restringir el acceso a la red estableciendo dominios lógicos separados, como redes privadas virtuales para ciertos grupos de usuarios dentro de la Organización. • Controlar el acceso de los usuarios al segmento. • Controlar la salida de información del segmento.
A.13.2 Gestión de la seguridad de las redes			

Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.			
Cód.	**Nombre**	**Control**	**Actividades necesarias**
A.13.2.1	Políticas y procedimientos de transferencia de la información	Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de equipos de comunicación.	• Designar personal específico para la realización de transferencias de la información. • Disponer de normativa para la transferencia de SW a otros (organizaciones externas). • Disponer de procedimientos para las tareas de identificación y autenticación
A.13.2.2	Acuerdos sobre transferencia de la información	Los acuerdos deberán señalar la transferencia segura de la información del negocio entre la organización y terceros.	• Proveer las garantías de integridad, y confidencialidad durante la transferencia. • Realizar transferencias de información encriptadas. • Utilizar herramientas de desencriptamiento de la información. • Monitorizar los datos transferidos al exterior (otras redes)
A.13.2.3	Mensajes electrónicos	Se debe proteger adecuadamente la información enviada mediante mensajes electrónicos.	• Se requiere de una cuenta personal para acceder a los mensajes electrónicos. • Los emisores de los mensajes electrónicos deben poseer una clave privada. • Lo receptores debe poseer una clave pública para acceder al mensaje electrónico.
A.13.2.4	Confidencialidad o acuerdos no divulgados	Se debe identificar, revisar regularmente y documentar los requisitos para la confidencialidad o acuerdos no divulgados que reflejan las necesidades de la organización sobre la protección de la información.	• Establecer los acuerdos de confidencialidad. • Mantener actualizados los acuerdos de confidencialidad.

			• Revisar las cláusulas de confidencialidad al modificar / expirar los contratos
A.14 Adquisición, desarrollo y mantenimientos de sistemas			
A.14.1 Requisitos de seguridad de los sistemas de información			
Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos del sistema de la información que proveen servicios mediante las redes públicas.			
Cód.	**Nombre**	**Control**	**Actividades necesarias**
A.14.1.1	Análisis y especificaciones de los requisitos de la seguridad de la información	Se debe incluir la seguridad de la información relacionada a los requisitos en los requerimientos de nuevos sistemas de información o en el mejoramiento de los sistemas de información existentes.	• Identificar y analizar los requisitos de seguridad de acuerdo a los condicionantes del negocio. • Identificar y analizar los requisitos técnicos de seguridad de la información.
A.14.1.2	Seguridad de los servicios de aplicación en las redes públicas	Se debe proteger la información que pasa a través de las redes públicas de las actividades fraudulentas, controversias contractuales y divulgación y modificaciones no autorizadas.	• Revisar las características de la solución propuesta sobre la red pública de datos, de voz y datos, etc. • Se tienen en cuenta las obligaciones legales, contractuales, y los estándares. • Identificar los riesgos de la solución propuesta, y las salvaguardas necesarias.
A.14.1.3	Protección de las transacciones de los servicios de aplicación	Se debe proteger la información que provenga de las transacciones de los servicios de aplicación, para evitar las transmisiones incompletas, desvíos, duplicado o reproducción no autorizada de mensajes.	• Establecer controles de sesión o de lotes, para conciliación de cuadres de ficheros tras las actualizaciones de transacciones. • Impedir que los operadores puedan realizar transacciones.
A.15 Relación con los proveedores			
A.15.1 Seguridad de la información en las relaciones con los proveedores			
Objetivo: Garantizar la protección de los activos de la información a los que los proveedores tienen acceso.			
Cód.	**Nombre**	**Control**	**Actividades necesarias**

A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	Se debe acordar y documentar los requisitos de seguridad de la información para mitigar los riesgos asociados al acceso de los proveedores a los activos de la organización	• Establecer un contrato de prestación de servicio con el proveedor del sistema, de acuerdo a los requisitos del negocio. • Seguir las recomendaciones del fabricante o proveedor.
A.15.1.2	Consideración de la seguridad en los acuerdos con los proveedores	Se debe establecer y acordar todos los requisitos relacionados a la seguridad de la información con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proveer con elementos de infraestructura tecnológica, información de la organización.	• Realizar pruebas de los recursos y servicios de los proveedores. • Actualizar regularmente el conjunto de vulnerabilidades utilizado por el proveedor. • Participar en foros de seguridad propuestos por los proveedores.
A.15.1.3	Cadena de suministro de tecnología de la información y comunicación	Los acuerdos con proveedores deberían incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	• Mantener contactos con los proveedores de servicios de información. • Mantener contactos con los operadores de telecomunicaciones. • Establecer los requisitos de los suministros de tecnología de la información y comunicación.

A.16 Gestión de los incidentes de seguridad de la información

A.16.1 Gestión de los incidentes de la seguridad de la información y la mejora

Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.

Cód.	Nombre	Control	Actividades necesarias
A.16.1.1	Responsabilidades y procedimientos	Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	• Identificar los roles y responsabilidades requeridas • Nombrar al responsable de cada activo o proceso de seguridad

			• Documentar los detalles de cada responsabilidad. • Separar las responsabilidades de administración y operación
A.16.1.2	Reporte de eventos de seguridad de la información	Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados, tan pronto como sea posible.	• Designar responsables de reportar eventos de la información. • Identificar eventos posibles y su potencialidad de producir una interrupción. • Establecer los canales de gestión de eventos. • Registrar los eventos una vez suscitados
A.16.1.3	Reporte de debilidades de seguridad de la información	Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	• Designar responsables de reportar debilidades de la información. • Identificar posibles debilidades y su potencialidad de afectar la seguridad de la información. • Se adoptan medidas preventivas. • Registrar las debilidades encontradas de la seguridad de la seguridad.
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Se debe evaluar los eventos de seguridad de la información; y tomar una decisión sobre si deben ser clasificados como incidentes de la seguridad de la información.	• Identificar los impactos en términos de tiempo de interrupción, daños y tiempo de recuperación.
A.16.1.5	Respuesta a incidentes de seguridad de la información	Se debe responder a los incidentes de seguridad de la información de acuerdo a los procedimientos documentados.	• Activar los seguros contra interrupciones en el negocio • Identificar las copias de seguridad (backups) y su almacenamiento.

			• Identificar las necesidades de equipamiento alternativo. • Activar el plan de gestión de crisis del negocio. • Activar un plan de recuperación.
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Se debe usar el conocimiento obtenido del análisis y resolución de los incidentes de la seguridad de la información, con la finalidad de reducir la probabilidad o impacto de futuros incidentes.	• Documentar todos los incidentes de seguridad suscitados. • Los planes se mantienen al día dentro de un proceso de mejora continua. • Realizar las copias de seguridad (backups) con la frecuencia acordada.
A.16.1.7	Recolección de evidencia	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y conservación de la información que puede servir como evidencia.	• Las evidencias recogidas deben ser almacenadas de forma segura. • Las evidencias en documentos deben constar de: autor del documento, testigos del incidente reportado, acciones del proceso de copia y testigos del proceso de copia. • Las evidencias en medios electrónicos debe constar de: origen de la evidencia, copias en medios de alta fiabilidad, testigos del proceso de copia.
A.17 Gestión de los aspectos de la seguridad de la información para la continuidad del negocio			
A.17.1 Continuidad de la seguridad de la información			
Objetivo: La continuidad de la seguridad de la información debe ser incrustada en los sistemas de gestión de la continuidad del negocio de la organización			
Cód.	**Nombre**	**Control**	**Actividades necesarias**

A.17.1.1	Planificación de la continuidad de la seguridad de la información.	La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	• Disponer de normativas relativas a la continuidad de la seguridad de la información. • Disponer de un plan de gestión de crisis y desastres. • Disponer de normativas para la vuelta a la normalidad.
A.17.1.2	Implementación de la continuidad de la seguridad de la información	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	• La documentación se aprueba y se garantiza que llegue a los afectados
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	La organización debe verificar los controles de continuidad de la seguridad de la información establecidos e implementados, a intervalos regulares con la finalidad de asegurar su validez y efectividad durante situaciones adversas.	• Simular situaciones de crisis • Realizar pruebas de recuperación técnica. • Realizar pruebas de recuperación en un centro alternativo. • Registrar las lecciones aprendidas para aplicar dentro del proceso de mejora continua
A.17.2 Redundancias			
Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.			
Cód.	**Nombre**	**Control**	**Actividades necesarias**
A.17.2.1	Disponibilidad de las instalaciones de procesamiento de la información	Se debe implementar las instalaciones de procesamiento de la información con una capacidad adicional suficiente para cumplir con los requisitos de disponibilidad.	• Disponer un inventario de instalaciones de procesamiento de la información. • Disponer de un registro de instalaciones propias.

			• Identificar al responsable de cada instalación de procesamiento de la información. • Revisar regularmente las instalaciones por los bomberos o personal especializado. • Disponer de instalaciones alternativas.
A.18 Cumplimiento			
A.18.1 Cumplimiento de los requisitos legales y contractuales			
Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad			
Cód.	**Nombre**	**Control**	**Actividades necesarias**
A.18.1.1	Identificación de la legislación aplicable y requisitos contractuales	Se debe identificar de manera explícita, documentar y mantener actualizados todos los requisitos legislativos, regulatorios y contractuales así como el enfoque de la organización para cumplir con estos requisitos, con respecto a cada sistema de información de la organización.	• Identificar los lineamientos de la legislación • Identificar todos los requisitos contractuales.
A.18.1.2	Derechos de propiedad intelectual	Se deberían implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.	• Establecer acuerdos sobre los derechos de propiedad intelectual del producto. • Establecer acuerdos sobre licencia, propiedad y derechos de propiedad intelectual. • Proteger los derechos de propiedad intelectual de las aplicaciones (SW).
A.18.1.3	Protección de registros	Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	• Revisar regularmente los registros en busca de acciones inapropiadas. • Garantizar la integridad de los registros. • Verificar el funcionamiento de los registros.

A.18.1.4	Privacidad y protección de datos personales	Cuando sea aplicable, se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes.	• La información, o los datos se deben registrar en un sistema de datos personales. • No podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información. • El titular de los datos es el único que tiene derecho a decidir quién, cómo cuándo y para qué se tratan sus datos.
A.18.1.5	Reglamentación de controles criptográficos	Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	• Disponer de normativa relativa a los controles criptográficos. • Se tienen en cuenta los requisitos de protección para los mecanismos criptográficos. • Se tienen en cuenta los requisitos de control de los mecanismos criptográficos (registro, contabilidad, auditoría, etc.).
A.18.2 Revisiones de la seguridad de la información			
Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.			
Cód.	**Nombre**	**Control**	**Actividades necesarias**
A.18.2.1	Revisión independiente de la seguridad de la información	El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) independientemente a intervalos planificados o cuando ocurran cambios significativos.	• Establecer un comité de seguridad de la información • Designar un responsable de la seguridad de la información. • Revisar, evaluar y aprobar la normativa de seguridad de la información • Asegurar la coordinación en materia de seguridad de la información dentro de la organización

A.18.2.2	Cumplimiento con las políticas y normas de seguridad	Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	• Revisar periódicamente el cumplimiento de las políticas y normas de seguridad por parte del personal. • Las normas de seguridad deben ser revisadas regularmente
A.18.2.3	Revisión del cumplimiento técnico	Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	• Disponer de normativas de obligado cumplimiento en el desempeño del puesto de trabajo. • Generar compromiso escrito de cumplimiento de la política y la normativa correspondiente. • Revisar periódicamente el cumplimiento por parte del personal.

Fuente: (Guía: Controles de Seguridad y Privacidad de la Información MIN)

Elaborado por: Ing. Ing. Viviana Tixilima

4 Conclusiones y Recomendaciones

Conclusiones:

- *Los activos de una empresa son los componentes más importantes para el desarrollo de sus funciones, por lo que es transcendental identificar adecuadamente cada activo para poder proporcionarle las políticas de seguridad que minimicen su riesgo.*
- *Los criterios de valoración de activos permiten establecer los umbrales sobre los cuales se puede medir los riesgos de cada activo, estos valores permiten identificar los activos con más alto riesgo.*
- *Para determinar las Políticas de Seguridad que se pueden aplicar en una empresa, se debe identificar cual es el servicio más importante, el cual se constituye en la base de la orientación del negocio.*
- *En la actualidad el servicio más importante de una empresa se lo puede gestionar a través de herramientas de tecnologías de la Información y Comunicación TIC's, las cuales permiten enlazar entre el usuario final y la información.*

Recomendaciones:

- *Es recomendable que para poder establecer las políticas de seguridad de una empresa, se utilice la herramienta PILAR, ya que posee una enorme cantidad de librerías que consideran todos los riesgos y vulnerabilidades de la empresa.*
- *Se recomienda que para poder aplicar las políticas de seguridad en el Campus Sur de la Universidad Politécnica, se establezcan todos los formatos para la consecución de cada política.*
- *Para determinar las Políticas de Seguridad se debe sustentarse de una norma internacional como la ISO 27001, la cual guie y delimite todas las acciones en la aplicación de las Políticas.*

- *Es recomendable utilizar la metodología Magerit ya que se esfuerza por enfatizarse en dividir los activos de la organización en variados grupos, para identificar más riesgos y poder tomar contramedidas para evitar así cualquier inconveniente.*

Bibliografía:

[1] UNIVERSIDAD POLITECNICA SALESIANA. (2012). *ESTATUTO DE LA UNIVERSIDAD POLITECNICA SALESIANA.* Obtenido de http://cinaj.ups.edu.ec/c/document_library/get_file?uuid=dd1f9bc0-3c9f-4022-9827-0cdbb418be25&groupId=10156

ALEJANDRO, M., & LUIS, T. (04 de 2015). Diseño de una red de alta disponibilidad para la Universidad Politécnica Salesiana Sede Quito Campus Sur. Quito, Pichincha, Ecuador.

AREITIO, J. (2008). *Seguridad de la Información.* Madrid-España: Cengage.

CESAR MEJIA, N. R. (2012). Vulnerabilidad, tipos de ataques y formas de mitigarlos en las capas del modelo OSI en las redes de datos en las organizaciones. Perreira, Peru.

El portal de ISO 27001 en Español. (2005). Obtenido de http://www.iso27000.es/sgsi.html

EL PORTAL DE ISO 27001 EN ESPAÑOL. (2012). Obtenido de http://www.iso27000.es/sgsi.html

GALINDO, E. F., & MORALES, J. G. (23 de 3 de 2008). APLICACIÓN DE LA METODOLOGÍA MAGERIT EN EL ANÁLISIS DE RIESGO DEL FLUJO DE INFORMACIÓN EN EL ÁREA DE GESTIÓN DE UNA EMPRESA DEDICADA A LA APLICACIÓN DE EXÁMENES DE CONTROL DE CONFIANZA . México D.F, México .

Gaona Vásquez, K. D. (2013). Aplicación de la metodología Magerit para el análisis y gestión de riesgos de la seguridad de la información aplicado a la empresa Pesquera e Industrial Bravito SA en la ciudad de Machala. Machala, Ecuador. Obtenido de http://dspace.ups.edu.ec/bitstream/123456789/5272/1/UPS-CT002759.pdf

ISO. (15 de 06 de 2005). *ISO/IEC 17799.* Recuperado el 01 de 02 de 2015, de https://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf

iso27000. (2012). Obtenido de http://www.iso27000.es/sgsi_implantar.html

Mancha, C. d.-l. (20 de 07 de 2011). RECOMENDACIONES PARA EL DESARROLLO DE UNA PLAN DE SEGURIDAD DE LA INFORMACIÓN. Castilla-La Mancha, España. Obtenido de http://docplayer.es/1624628-Recomendaciones-para-el-desarrollo-de-una-plan-de-seguridad-de-la-informacion.html

MATUTE MACIAS, Q. C. (02 de 2006). *Repositorio Digital EPN.* Recuperado el 01 de 02 de 2015, de Repositorio Digital EPN: http://bibdigital.epn.edu.ec/handle/15000/78

MELO, A. H. (Junio de 2008). *EL DERECHO INFORMÁTICO Y LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN UNA PERSPECTIVA CON BASE EN LA NORMA ISO 27 001*. Obtenido de Revista de Derecho: http://www.scielo.org.co/scielo.php?pid=S0121-86972008000100013&script=sci_arttext&tlng=pt

Miguel Ángel Mendoza López, P. A. (Marzo de 2013). *Normatividad en las organizaciones: Políticas de seguridad de la información - Parte I*. Obtenido de http://revista.seguridad.unam.mx/numero-16/normatividad-en-las-organizaciones-pol%C3%ADticas-de-seguridad-de-la-informaci%C3%B3n-parte-i

MOGUERZA, L. M. (2010). DISEÑO DE UN SISTEMA DE GESTTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) . España.

MÓNICA, G. (28 de 10 de 2014). *Herramientas de escaneo de vulnerabilidades para SO, BD y re*. Obtenido de PREZI: https://prezi.com/l9ogc4bwnoex/herramientas-de-escaneo-de-vulnerabilidades-para-so-bd-y-re/

PILAR / ayuda. (s.f.). Obtenido de https://www.ccn-cert.cni.es/publico/herramientas/Pilar-5.4.5/Pilar_5.4.5/bcm_es/index.html?n=76.html

PUBLICA, G. (07 de 2005). *Modelo de Política de Seguridad de la Información para Organismos de la Administración Pública Nacional.* Obtenido de http://www.sgp.gov.ar/sitio/PSI_Modelo-v1_200507.pdf

REYES, M. P. (s.f.). *Simulación de Esquemas de QoS en Redes Convergentes Ethernet.* Obtenido de http://docente.ucol.mx/xe1aom/public_html/doc/Simulaciones.pdf

Seguridad Informatica. (Diciembre de 2014). Obtenido de http://www.clubensayos.com/Acontecimientos-Sociales/Seguridad-Informatica/2245970.html

UNIVERSIDAD NACIONAL DE LUJAN. (s.f.). Riesgo vs. Seguridad de la Información. Argentina. Obtenido de http://www.seguridadinformatica.unlu.edu.ar/sites/www.seguridadinformatica.unlu.edu.ar/files/site/material_taller_gestion_de_riesgo.pdf

UPS. (2014). *Universidad Politécnica Salesiana*. Obtenido de http://www.ups.edu.ec/web/guest/organigrama

Anexos:

ANEXO A:

Modelo de valor

proyecto: [ProyTesis01] TesisPUCE

1. Datos del proyecto

ProyTesis01	TesisPUCE
desc	Proyecto de Tesis
resp	Ing. Viviana Tixilima
org	PUCE
ver	1
date	Abril 2016
biblioteca	[std] Biblioteca INFOSEC (8.11.2013)

Licencia

2. Dimensiones

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

3. Dominios de seguridad

- [base] Base

4. Activos

4.1. Capa - [B] Activos esenciales

[Servicio01UPS] Portal_Web

4.2. Capa - [IS] Servicios internos

4.3. Capa - [E] Equipamiento

[SW] Aplicaciones
- [SOFT01UPS_SNA] SNA
- [SOF02UPS_SQUAD] SQUAD
- [SOF03UPS_OFIMATICA] OFIMATICA
- [SOF04UPS_ANTIVIRUS] ANTIVIRUS
- [SOF05UPS_SIST_OPER] SIST_OPERATIVO
- [SOF06UPS_SIST_SOLICIT] SIST_SOLICITUDES
- [SOF07UPS_CORREO_ELEC] CORREO_ELECTRONICO
- [SOF08UPS_BIBLIO] SIST_BIBLIOTECA

[HW] Equipos
- [HW01UPS_SBDD] SER_BDD
- [HW02UPS_MED_IMPRES] MEDIOS_IMPRESION
- [HW03UPS_PC] PC_ESCRITORIO
- [HW04UPS_ROUTER] ROUTER

[HW05UPS_SWITCH] SWITCH
[HW06UPS_SCORREO] SER_CORREO
[COM] Comunicaciones
[COM01UPS_FONOIP] TELEFONIA_IP
[COM02UPS_WI-FI] WI_FI
[COM03UPS_LAN] RED_LAN
[COM04_WAN] RED_WAN
[COM04UPS_INTERNET] INTERNET
[COM05UPS_INTRANET] INTRANET
[AUX] Elementos auxiliares
[AUX01UPS_GELECTRICO] GEN_ELECTRICO
[AUX02UPS_CABLEADO] CABLEADO
[AUX03UPS_MOBILIARIO] MOBILIARIO
[AUX04UPS_SISTVIGILANCIA] SIST_VIGILANCIA
[AUX05UPS_ANTENAS] ANTENAS
[AUX06UPS_RADIOS] RADIOS
[AUX07UPS_SISTALIMENT] SIST_ALIMENTAC_INENTERRUMPIDA

4.4. Capa - [SS] Servicios subcontratados

4.5. Capa - [L] Instalaciones

[INST01_BLOQUEA] BLOQUE_A

4.6. Capa - [P] Personal

[PER01UPS_COORDINADOR] COORDINADOR_UNADEVI
[PER02UPS_PROGR] PROGRAMADORES

4.7. Resumen de valoración

[B] Activos esenciales

activo	[D]	[I]	[C]	[A]	[T]
[Servicio01UPS] Portal_Web	[7](1)			[6](2)	[6]

(1) [6.pi1] probablemente afecte gravemente a un grupo de individuos
[7.si] probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[1.olm] Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local)
[1.adm] pudiera impedir la operación efectiva de una parte de la Organización
[4.rto] 4 horas < RTO < 1 día

(2) [6.pi1] probablemente afecte gravemente a un grupo de individuos
[1.si] pudiera causar una merma en la seguridad o dificultar la investigación de un incidente
[3.da] Probablemente cause la interrupción de actividades propias de la Organización
[1.olm] Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local)
[1.adm] pudiera impedir la operación efectiva de una parte de la Organización
[1.lg] Pudiera causar una pérdida menor de la confianza dentro de la Organización

[E] Equipamiento

activo	[D]	[I]	[C]	[A]	[T]
[SW.SOFT01UPS_SNA] SNA	[7]	[7](1)	[7]	[7]	[7]
[SW.SOF02UPS_SQUAD] SQUAD	[7]	[7]	[7]	[7]	[7]
[SW.SOF03UPS_OFIMATICA] OFIMATICA					[5]
[SW.SOF04UPS_ANTIVIRUS] ANTIVIRUS					[6]
[SW.SOF05UPS_SIST_OPER] SIST_OPERATIVO				[6]	[6]
[SW.SOF06UPS_SIST_SOLICIT] SIST_SOLICITUDES				[6]	[6]
[SW.SOF07UPS_CORREO_ELEC] CORREO_ELECTRONICO				[6]	[6]
[SW.SOF08UPS_BIBLIO] SIST_BIBLIOTECA				[6]	[6]
[HW.HW01UPS_SBDD] SER_BDD	[8]	[8]	[8]	[8]	[8]
[HW.HW02UPS_MED_IMPRES] MEDIOS_IMPRESION					[5]
[HW.HW03UPS_PC] PC_ESCRITORIO				[6]	[6]
[HW.HW04UPS_ROUTER] ROUTER	[7]				[6]
[HW.HW05UPS_SWITCH] SWITCH	[7]				[7]
[HW.HW06UPS_SCORREO] SER_CORREO				[6]	[6]
[COM.COM02UPS_WI-FI] WI_FI	[6]			[6]	[6]
[COM.COM03UPS_LAN] RED_LAN	[7]			[7]	[6]
[COM.COM04_WAN] RED_WAN	[7]			[7]	[7]
[COM.COM04UPS_INTERNET] INTERNET	[8]			[8]	[7]
[COM.COM05UPS_INTRANET] INTRANET	[7]			[8]	
[AUX.AUX01UPS_GELECTRICO] GEN_ELECTRICO	[8]				
[AUX.AUX02UPS_CABLEADO] CABLEADO	[7]			[6]	[6]
[AUX.AUX05UPS_ANTENAS] ANTENAS	[6]				
[AUX.AUX07UPS_SISTALIMENT] SIST_ALIMENTAC_INENTERRUMPIDA	[8]				

(1) El sistema nacional de admisiones recopila información sobre horarios docentes estudiantes carreras

[L] Instalaciones

activo	[D]	[I]	[C]	[A]	[T]
[INST01_BLOQUEA] BLOQUE_A	[6]				

[P] Personal

activo	[D]	[I]	[C]	[A]	[T]
[PER01UPS_COORDINADOR] COORDINADOR_UNADEVI			[6]		
[PER02UPS_PROGR] PROGRAMADORES			[6]		

ANEXO B:

Informe de amenazas

proyecto: [ProyTesis01] TesisPUCE

5. Datos del proyecto

ProyTesis01	TesisPUCE
desc	Proyecto de Tesis
resp	Ing. Viviana Tixilima
org	PUCE
ver	1
date	Abril 2016
biblioteca	[std] Biblioteca INFOSEC (8.11.2013)

Licencia

PUCE
Pontificia Universidad Católica del Ecuador

6. Dimensiones

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

7. Dominios de seguridad

- [base] Base

8. amenazas / activo

[Servicio01UPS] Portal_Web

[SW.SOFT01UPS_SNA] SNA

Amenaza	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[I.5] Avería de origen físico o lógico	1	50%	-	-	-	-
[E.1] Errores de los usuarios	1	1%	10%	10%	-	-
[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%	20%	-	-
[E.8] Difusión de software dañino	1	10%	10%	10%	-	-
[E.15] Alteración de la información	1	-	1%	-	-	-
[E.18] Destrucción de la información	1	50%	-	-	-	-
[E.19] Fugas de información	1	-	-	10%	-	-
[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%	-	-
[E.21] Errores de mantenimiento / actualización de programas (software)	10	1%	1%	-	-	-
[A.5] Suplantación de la identidad	1	-	50%	50%	100%	-
[A.6] Abuso de privilegios de acceso	1	1%	10%	10%	-	-
[A.7] Uso no previsto	1	1%	10%	10%	-	-
[A.8] Difusión de software dañino	1	100%	100%	100%	-	-

[A.11] Acceso no autorizado	1	-	10%	50%	-	-
[A.15] Modificación de la información	1	-	50%	-	-	-
[A.18] Destrucción de la información	1	50%	-	-	-	-
[A.19] Revelación de información	1	-	-	50%	-	-
[A.22] Manipulación de programas	1	50%	100%	100%	-	-

[SW.SOF02UPS_SQUAD] SQUAD

amenaza	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[I.5] Avería de origen físico o lógico	1	50%	-	-	-	-
[E.1] Errores de los usuarios	1	1%	10%	10%	-	-
[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%	20%	-	-
[E.8] Difusión de software dañino	1	10%	10%	10%	-	-
[E.15] Alteración de la información	1	-	1%	-	-	-
[E.18] Destrucción de la información	1	50%	-	-	-	-
[E.19] Fugas de información	1	-	-	10%	-	-
[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%	-	-
[E.21] Errores de mantenimiento / actualización de programas (software)	10	1%	1%	-	-	-
[A.5] Suplantación de la identidad	1	-	50%	50%	100%	-
[A.6] Abuso de privilegios de acceso	1	1%	10%	10%	-	-
[A.7] Uso no previsto	1	1%	10%	10%	-	-
[A.8] Difusión de software dañino	1	100%	100%	100%	-	-
[A.11] Acceso no autorizado	1	-	10%	50%	-	-
[A.15] Modificación de la información	1	-	50%	-	-	-
[A.18] Destrucción de la información	1	50%	-	-	-	-
[A.19] Revelación de información	1	-	-	50%	-	-
[A.22] Manipulación de programas	1	50%	100%	100%	-	-

[SW.SOF03UPS_OFIMATICA] OFIMATICA

[SW.SOF04UPS_ANTIVIRUS] ANTIVIRUS

[SW.SOF05UPS_SIST_OPER] SIST_OPERATIVO

amenaza	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[I.5] Avería de origen físico o lógico	1	50%	-	-	-	-
[E.1] Errores de los usuarios	1	1%	10%	10%	-	-
[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%	20%	-	-
[E.8] Difusión de software dañino	1	10%	10%	10%	-	-
[E.15] Alteración de la información	1	-	1%	-	-	-
[E.18] Destrucción de la información	1	50%	-	-	-	-
[E.19] Fugas de información	1	-	-	10%	-	-
[E.20] Vulnerabilidades de los programas (software)	1	1%	20%	20%	-	-
[E.21] Errores de mantenimiento / actualización de programas (software)	10	1%	1%	-	-	-
[A.5] Suplantación de la identidad	1	-	50%	50%	100%	-
[A.6] Abuso de privilegios de acceso	1	1%	10%	10%	-	-
[A.7] Uso no previsto	1	1%	10%	10%	-	-
[A.8] Difusión de software dañino	1	100%	100%	100%	-	-

[A.11] Acceso no autorizado	1	-	10%	50%	-	-
[A.15] Modificación de la información	1	-	50%	-	-	-
[A.18] Destrucción de la información	1	50%	-	-	-	-
[A.19] Revelación de información	1	-	-	50%	-	-
[A.22] Manipulación de programas	1	50%	100%	100%	-	-

[SW.SOF06UPS_SIST_SOLICIT] SIST_SOLICITUDES

amenaza	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[I.5] Avería de origen físico o lógico	1	50%	-	-	-	-
[E.1] Errores de los usuarios	1	1%	-	-	-	-
[E.2] Errores del administrador del sistema / de la seguridad	1	20%	-	-	-	-
[E.8] Difusión de software dañino	1	10%	-	-	-	-
[E.18] Destrucción de la información	1	50%	-	-	-	-
[E.20] Vulnerabilidades de los programas (software)	1	1%	-	-	-	-
[E.21] Errores de mantenimiento / actualización de programas (software)	10	1%	-	-	-	-
[A.5] Suplantación de la identidad	1	-	-	-	100%	-
[A.6] Abuso de privilegios de acceso	1	1%	-	-	-	-
[A.7] Uso no previsto	1	1%	-	-	-	-
[A.8] Difusión de software dañino	1	100%	-	-	-	-
[A.18] Destrucción de la información	1	50%	-	-	-	-
[A.22] Manipulación de programas	1	50%	-	-	-	-

[SW.SOF07UPS_CORREO_ELEC] CORREO_ELECTRONICO

amenaza	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[I.5] Avería de origen físico o lógico	1	50%	-	-	-	-
[E.1] Errores de los usuarios	1	1%	-	-	-	-
[E.2] Errores del administrador del sistema / de la seguridad	1	20%	-	-	-	-
[E.8] Difusión de software dañino	1	10%	-	-	-	-
[E.18] Destrucción de la información	1	50%	-	-	-	-
[E.20] Vulnerabilidades de los programas (software)	1	1%	-	-	-	-
[E.21] Errores de mantenimiento / actualización de programas (software)	10	1%	-	-	-	-
[A.5] Suplantación de la identidad	1	-	-	-	100%	-
[A.6] Abuso de privilegios de acceso	1	1%	-	-	-	-
[A.7] Uso no previsto	1	1%	-	-	-	-
[A.8] Difusión de software dañino	1	100%	-	-	-	-
[A.18] Destrucción de la información	1	50%	-	-	-	-
[A.22] Manipulación de programas	1	50%	-	-	-	-

[SW.SOF08UPS_BIBLIO] SIST_BIBLIOTECA

amenaza	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[I.5] Avería de origen físico o lógico	1	50%	-	-	-	-
[E.1] Errores de los usuarios	1	1%	-	-	-	-
[E.2] Errores del administrador del sistema / de la seguridad	1	20%	-	-	-	-

[E.8] Difusión de software dañino	1	10%	-	-	-	-
[E.18] Destrucción de la información	1	50%	-	-	-	-
[E.20] Vulnerabilidades de los programas (software)	1	1%	-	-	-	-
[E.21] Errores de mantenimiento / actualización de programas (software)	10	1%	-	-	-	-
[A.5] Suplantación de la identidad	1	-	-	-	100%	-
[A.6] Abuso de privilegios de acceso	1	1%	-	-	-	-
[A.7] Uso no previsto	1	1%	-	-	-	-
[A.8] Difusión de software dañino	1	100%	-	-	-	-
[A.18] Destrucción de la información	1	50%	-	-	-	-
[A.22] Manipulación de programas	1	50%	-	-	-	-

[HW.HW01UPS_SBDD] SER_BDD

amenaza	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[N.1] Fuego	0,1	100%	-	-	-	-
[N.2] Daños por agua	0,1	50%	-	-	-	-
[N.*] Desastres naturales	0,1	100%	-	-	-	-
[I.1] Fuego	0,5	100%	-	-	-	-
[I.2] Daños por agua	0,5	50%	-	-	-	-
[I.*] Desastres industriales	0,5	100%	-	-	-	-
[I.3] Contaminación medioambiental	0,1	50%	-	-	-	-
[I.4] Contaminación electromagnética	1	10%	-	-	-	-
[I.5] Avería de origen físico o lógico	1	50%	-	-	-	-
[I.6] Corte del suministro eléctrico	1	100%	-	-	-	-
[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%	-	-	-	-
[I.11] Emanaciones electromagnéticas	1	-	-	1%	-	-
[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%	20%	-	-
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	10	50%	-	-	-	-
[E.25] Pérdida de equipos	1	100%	-	100%	-	-
[A.6] Abuso de privilegios de acceso	1	10%	100%	100%	-	-
[A.7] Uso no previsto	1	10%	10%	100%	-	-
[A.11] Acceso no autorizado	1	10%	100%	100%	-	-
[A.23] Manipulación del hardware	0	50%	-	50%	-	-
[A.24] Denegación de servicio	2	100%	-	-	-	-
[A.25] Robo de equipos	0,5	100%	-	100%	-	-
[A.26] Ataque destructivo	1	100%	-	-	-	-

[HW.HW02UPS_MED_IMPRES] MEDIOS_IMPRESION

[HW.HW03UPS_PC] PC_ESCRITORIO

[HW.HW04UPS_ROUTER] ROUTER

amenaza	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[N.1] Fuego	0,1	100%	-	-	-	-
[N.2] Daños por agua	0,1	50%	-	-	-	-
[N.*] Desastres naturales	0,1	100%	-	-	-	-

[I.1] Fuego	0,5	100%	-	-	-	-
[I.2] Daños por agua	0,5	50%	-	-	-	-
[I.*] Desastres industriales	0,5	100%	-	-	-	-
[I.3] Contaminación medioambiental	0,1	50%	-	-	-	-
[I.4] Contaminación electromagnética	1	10%	-	-	-	-
[I.5] Avería de origen físico o lógico	1	50%	-	-	-	-
[I.6] Corte del suministro eléctrico	1	100%	-	-	-	-
[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%	-	-	-	-
[I.11] Emanaciones electromagnéticas	1	-	-	1%	-	-
[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%	20%	-	-
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	10	50%	-	-	-	-
[E.25] Pérdida de equipos	1	20%	-	50%	-	-
[A.6] Abuso de privilegios de acceso	1	10%	10%	50%	-	-
[A.7] Uso no previsto	1	10%	1%	10%	-	-
[A.11] Acceso no autorizado	1	10%	10%	50%	-	-
[A.23] Manipulación del hardware	0,5	100%	-	50%	-	-
[A.24] Denegación de servicio	2	100%	-	-	-	-
[A.25] Robo de equipos	0,5	20%	-	50%	-	-
[A.26] Ataque destructivo	1	100%	-	-	-	-

[HW.HW05UPS_SWITCH] SWITCH

amenaza	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[N.1] Fuego	0,1	100%	-	-	-	-
[N.2] Daños por agua	0,1	50%	-	-	-	-
[N.*] Desastres naturales	0,1	100%	-	-	-	-
[I.1] Fuego	0,5	100%	-	-	-	-
[I.2] Daños por agua	0,5	50%	-	-	-	-
[I.*] Desastres industriales	0,5	100%	-	-	-	-
[I.3] Contaminación medioambiental	0,1	50%	-	-	-	-
[I.4] Contaminación electromagnética	1	10%	-	-	-	-
[I.5] Avería de origen físico o lógico	1	50%	-	-	-	-
[I.6] Corte del suministro eléctrico	1	100%	-	-	-	-
[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%	-	-	-	-
[I.11] Emanaciones electromagnéticas	1	-	-	1%	-	-
[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%	20%	-	-
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	10	50%	-	-	-	-
[E.25] Pérdida de equipos	1	20%	-	50%	-	-
[A.6] Abuso de privilegios de acceso	1	10%	10%	50%	-	-
[A.7] Uso no previsto	1	10%	1%	10%	-	-
[A.11] Acceso no autorizado	1	10%	10%	50%	-	-
[A.23] Manipulación del hardware	0,5	100%	-	50%	-	-
[A.24] Denegación de servicio	2	100%	-	-	-	-
[A.25] Robo de equipos	0,5	20%	-	50%	-	-

[A.26] Ataque destructivo	1	100%	-	-	-	-

[HW.HW06UPS_SCORREO] SER_CORREO

amenaza	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[N.1] Fuego	0,1	100%	-	-	-	-
[N.2] Daños por agua	0,1	50%	-	-	-	-
[N.*] Desastres naturales	0,1	100%	-	-	-	-
[I.1] Fuego	0,5	100%	-	-	-	-
[I.2] Daños por agua	0,5	50%	-	-	-	-
[I.*] Desastres industriales	0,5	100%	-	-	-	-
[I.3] Contaminación medioambiental	0,1	50%	-	-	-	-
[I.4] Contaminación electromagnética	1	10%	-	-	-	-
[I.5] Avería de origen físico o lógico	1	50%	-	-	-	-
[I.6] Corte del suministro eléctrico	1	100%	-	-	-	-
[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%	-	-	-	-
[E.2] Errores del administrador del sistema / de la seguridad	1	20%	-	-	-	-
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	10	50%	-	-	-	-
[E.25] Pérdida de equipos	1	100%	-	-	-	-
[A.6] Abuso de privilegios de acceso	1	10%	-	-	-	-
[A.7] Uso no previsto	1	10%	-	-	-	-
[A.11] Acceso no autorizado	1	10%	-	-	-	-
[A.23] Manipulación del hardware	0,5	50%	-	-	-	-
[A.24] Denegación de servicio	2	100%	-	-	-	-
[A.25] Robo de equipos	0,5	100%	-	-	-	-
[A.26] Ataque destructivo	1	100%	-	-	-	-

[COM.COM01UPS_FONOIP] TELEFONIA_IP

[COM.COM02UPS_WI-FI] WI_FI

amenaza	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[I.8] Fallo de servicios de comunicaciones	1	50%	-	-	-	-
[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%	20%	-	-
[E.9] Errores de [re-]encaminamiento	1	-	-	10%	-	-
[E.10] Errores de secuencia	1	-	10%	-	-	-
[E.15] Alteración de la información	1	-	1%	-	-	-
[E.19] Fugas de información	1	-	-	10%	-	-
[E.24] Caída del sistema por agotamiento de recursos	1	50%	-	-	-	-
[A.5] Suplantación de la identidad	1	-	10%	50%	100%	-
[A.6] Abuso de privilegios de acceso	1	-	10%	50%	100%	-
[A.7] Uso no previsto	1	10%	10%	10%	-	-
[A.9] [Re-]encaminamiento de mensajes	1	-	-	10%	-	-
[A.10] Alteración de secuencia	1	-	10%	-	-	-
[A.11] Acceso no autorizado	1	-	10%	50%	100%	-
[A.12] Análisis de tráfico	1	-	-	2%	-	-
[A.14] Interceptación de información	1	-	-	10%	-	-

(escucha)						
[A.15] Modificación de la información	1	-	10%	-	-	-
[A.18] Destrucción de la información	1	50%	-	-	-	-
[A.19] Revelación de información	1	-	-	50%	-	-
[A.24] Denegación de servicio	10	50%	-	-	-	-

[COM.COM03UPS_LAN] RED_LAN

amenaza	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[I.8] Fallo de servicios de comunicaciones	1	50%	-	-	-	-
[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%	20%	-	-
[E.9] Errores de [re-]encaminamiento	1	-	-	10%	-	-
[E.10] Errores de secuencia	1	-	10%	-	-	-
[E.15] Alteración de la información	1	-	1%	-	-	-
[E.19] Fugas de información	1	-	-	10%	-	-
[E.24] Caída del sistema por agotamiento de recursos	1	50%	-	-	-	-
[A.5] Suplantación de la identidad	1	-	10%	50%	100%	-
[A.6] Abuso de privilegios de acceso	1	-	10%	50%	100%	-
[A.7] Uso no previsto	1	10%	10%	10%	-	-
[A.9] [Re-]encaminamiento de mensajes	1	-	-	10%	-	-
[A.10] Alteración de secuencia	1	-	10%	-	-	-
[A.11] Acceso no autorizado	1	-	10%	50%	100%	-
[A.12] Análisis de tráfico	1	-	-	2%	-	-
[A.14] Interceptación de información (escucha)	1	-	-	1%	-	-
[A.15] Modificación de la información	1	-	10%	-	-	-
[A.18] Destrucción de la información	1	50%	-	-	-	-
[A.19] Revelación de información	1	-	-	50%	-	-
[A.24] Denegación de servicio	10	50%	-	-	-	-

[COM.COM04_WAN] RED_WAN

amenaza	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[I.8] Fallo de servicios de comunicaciones	1	50%	-	-	-	-
[E.2] Errores del administrador del sistema / de la seguridad	1	20%	20%	20%	-	-
[E.9] Errores de [re-]encaminamiento	1	-	-	10%	-	-
[E.10] Errores de secuencia	1	-	10%	-	-	-
[E.15] Alteración de la información	1	-	1%	-	-	-
[E.19] Fugas de información	1	-	-	10%	-	-
[E.24] Caída del sistema por agotamiento de recursos	1	50%	-	-	-	-
[A.5] Suplantación de la identidad	1	-	10%	50%	100%	-
[A.6] Abuso de privilegios de acceso	1	-	10%	50%	100%	-
[A.7] Uso no previsto	1	10%	10%	10%	-	-
[A.9] [Re-]encaminamiento de mensajes	1	-	-	10%	-	-
[A.10] Alteración de secuencia	1	-	10%	-	-	-
[A.11] Acceso no autorizado	1	-	10%	50%	100%	-
[A.12] Análisis de tráfico	1	-	-	2%	-	-
[A.14] Interceptación de información (escucha)	1	-	-	10%	-	-
[A.15] Modificación de la información	1	-	10%	-	-	-

[A.18] Destrucción de la información	1	50%	-	-	-	-
[A.19] Revelación de información	1	-	-	50%	-	-
[A.24] Denegación de servicio	10	50%	-	-	-	-

[COM.COM04UPS_INTERNET] INTERNET

amenaza	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[I.8] Fallo de servicios de comunicaciones	1	50%	-	-	-	-
[E.2] Errores del administrador del sistema / de la seguridad	1	20%	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	1	50%	-	-	-	-
[A.5] Suplantación de la identidad	1	-	-	-	100%	-
[A.6] Abuso de privilegios de acceso	1	-	-	-	100%	-
[A.7] Uso no previsto	1	10%	-	-	-	-
[A.11] Acceso no autorizado	1	-	-	-	100%	-
[A.18] Destrucción de la información	1	50%	-	-	-	-
[A.24] Denegación de servicio	10	50%	-	-	-	-

[COM.COM05UPS_INTRANET] INTRANET

amenaza	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[I.8] Fallo de servicios de comunicaciones	1	50%	-	-	-	-
[E.2] Errores del administrador del sistema / de la seguridad	1	20%	-	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	1	50%	-	-	-	-
[A.5] Suplantación de la identidad	1	-	-	-	100%	-
[A.6] Abuso de privilegios de acceso	1	-	-	-	100%	-
[A.7] Uso no previsto	1	10%	-	-	-	-
[A.11] Acceso no autorizado	1	-	-	-	100%	-
[A.18] Destrucción de la información	1	50%	-	-	-	-
[A.24] Denegación de servicio	10	50%	-	-	-	-

[AUX.AUX01UPS_GELECTRICO] GEN_ELECTRICO

amenaza	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[N.1] Fuego	0,1	1%	-	-	-	-
[N.2] Daños por agua	0,1	1%	-	-	-	-
[N.*] Desastres naturales	0,1	1%	-	-	-	-
[I.1] Fuego	0,5	1%	-	-	-	-
[I.2] Daños por agua	0,5	1%	-	-	-	-
[I.*] Desastres industriales	0,5	1%	-	-	-	-
[I.3] Contaminación medioambiental	0,1	1%	-	-	-	-
[I.9] Interrupción de otros servicios o suministros esenciales	1	1%	-	-	-	-
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	1%	-	-	-	-
[A.7] Uso no previsto	1	1%	-	-	-	-
[A.23] Manipulación del hardware	1	1%	-	-	-	-
[A.25] Robo de equipos	0,5	1%	-	-	-	-
[A.26] Ataque destructivo	1	1%	-	-	-	-

[AUX.AUX02UPS_CABLEADO] CABLEADO

amenaza	*frecuencia*	[D]	[I]	[C]	[A]	[T]
[N.1] Fuego	0,1	100%	-	-	-	-
[N.2] Daños por agua	0,1	50%	-	-	-	-
[N.*] Desastres naturales	0,1	100%	-	-	-	-
[I.1] Fuego	0,5	100%	-	-	-	-
[I.2] Daños por agua	0,5	50%	-	-	-	-
[I.*] Desastres industriales	0,5	100%	-	-	-	-
[I.3] Contaminación medioambiental	0,1	50%	-	-	-	-
[I.4] Contaminación electromagnética	0,5	10%	-	-	-	-
[I.11] Emanaciones electromagnéticas	1	-	-	1%	-	-
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%	-	-	-	-
[A.7] Uso no previsto	1	50%	1%	1%	-	-
[A.11] Acceso no autorizado	1	-	10%	50%	-	-
[A.23] Manipulación del hardware	1	50%	-	50%	-	-
[A.25] Robo de equipos	0,8	100%	-	-	-	-
[A.26] Ataque destructivo	1	100%	-	-	-	-

[AUX.AUX03UPS_MOBILIARIO] MOBILIARIO

[AUX.AUX04UPS_SISTVIGILANCIA] SIST_VIGILANCIA

[AUX.AUX05UPS_ANTENAS] ANTENAS

amenaza	*frecuencia*	[D]	[I]	[C]	[A]	[T]
[N.1] Fuego	0,1	100%	-	-	-	-
[N.2] Daños por agua	0,1	50%	-	-	-	-
[N.*] Desastres naturales	0,1	100%	-	-	-	-
[I.1] Fuego	0,5	100%	-	-	-	-
[I.2] Daños por agua	0,5	50%	-	-	-	-
[I.*] Desastres industriales	0,5	100%	-	-	-	-
[I.3] Contaminación medioambiental	0,1	50%	-	-	-	-
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	10%	-	-	-	-
[A.7] Uso no previsto	1	50%	1%	1%	-	-
[A.23] Manipulación del hardware	1	50%	-	50%	-	-
[A.25] Robo de equipos	0,5	10%	-	-	-	-
[A.26] Ataque destructivo	1	10%	-	-	-	-

[AUX.AUX06UPS_RADIOS] RADIOS

[AUX.AUX07UPS_SISTALIMENT] SIST_ALIMENTAC_INENTERRUMPIDA

amenaza	*frecuencia*	[D]	[I]	[C]	[A]	[T]
[N.1] Fuego	0,1	1%	-	-	-	-
[N.2] Daños por agua	0,1	1%	-	-	-	-
[N.*] Desastres naturales	0,1	1%	-	-	-	-
[I.1] Fuego	0,5	1%	-	-	-	-
[I.2] Daños por agua	0,5	1%	-	-	-	-
[I.*] Desastres industriales	0,5	1%	-	-	-	-
[I.3] Contaminación medioambiental	0,1	1%	-	-	-	-
[E.23] Errores de mantenimiento / actualización de	1	1%	-	-	-	-

equipos (hardware)						
[A.7] Uso no previsto	1	1%	-	-	-	-
[A.23] Manipulación del hardware	1	1%	-	-	-	-
[A.25] Robo de equipos	0,5	1%	-	-	-	-
[A.26] Ataque destructivo	1	1%	-	-	-	-

[INST01_BLOQUEA] BLOQUE_A

amenaza	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[N.1] Fuego	1	100%	-	-	-	-
[N.2] Daños por agua	1	100%	-	-	-	-
[N.*] Desastres naturales	0,5	100%	-	-	-	-
[I.1] Fuego	1	100%	-	-	-	-
[I.2] Daños por agua	1	100%	-	-	-	-
[I.*] Desastres industriales	1	100%	-	-	-	-
[I.3] Contaminación medioambiental	1	10%	-	-	-	-
[I.4] Contaminación electromagnética	0,1	10%	-	-	-	-
[I.11] Emanaciones electromagnéticas	0,1	-	-	1%	-	-
[A.5] Suplantación de la identidad	1	-	10%	50%	-	-
[A.6] Abuso de privilegios de acceso	1	10%	10%	50%	-	-
[A.7] Uso no previsto	1	10%	10%	50%	-	-
[A.11] Acceso no autorizado	5	-	10%	50%	-	-
[A.26] Ataque destructivo	0,1	100%	-	-	-	-
[A.27] Ocupación enemiga	1	100%	-	50%	-	-

[PER01UPS_COORDINADOR] COORDINADOR_UNADEVI

amenaza	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[E.19] Fugas de información	1	-	-	10%	-	-
[A.19] Revelación de información	10	-	-	50%	-	-
[A.29] Extorsión	0,9	-	-	100%	-	-
[A.30] Ingeniería social (picaresca)	0,5	-	-	100%	-	-

[PER02UPS_PROGR] PROGRAMADORES

amenaza	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[E.19] Fugas de información	1	-	-	10%	-	-
[A.19] Revelación de información	10	-	-	50%	-	-
[A.29] Extorsión	0,9	-	-	100%	-	-
[A.30] Ingeniería social (picaresca)	0,5	-	-	100%	-	-

9. activos / amenaza

[N.1] Fuego

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[HW.HW01UPS_SBDD] SER_BDD	0,1	100%	-	-	-	-
[HW.HW04UPS_ROUTER] ROUTER	0,1	100%	-	-	-	-
[HW.HW05UPS_SWITCH] SWITCH	0,1	100%	-	-	-	-
[HW.HW06UPS_SCORREO] SER_CORREO	0,1	100%	-	-	-	-
[AUX.AUX01UPS_GELECTRICO] GEN_ELECTRICO	0,1	1%	-	-	-	-
[AUX.AUX02UPS_CABLEADO] CABLEADO	0,1	100%	-	-	-	-
[AUX.AUX05UPS_ANTENAS] ANTENAS	0,1	100%	-	-	-	-
[AUX.AUX07UPS_SISTALIMENT]	0,1	1%	-	-	-	-

SIST_ALIMENTAC_INENTERRUMPIDA						
[INST01_BLOQUEA] BLOQUE_A	1	100%	-	-	-	-

[N.2] Daños por agua

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[HW.HW01UPS_SBDD] SER_BDD	0,1	50%	-	-	-	-
[HW.HW04UPS_ROUTER] ROUTER	0,1	50%	-	-	-	-
[HW.HW05UPS_SWITCH] SWITCH	0,1	50%	-	-	-	-
[HW.HW06UPS_SCORREO] SER_CORREO	0,1	50%	-	-	-	-
[AUX.AUX01UPS_GELECTRICO] GEN_ELECTRICO	0,1	1%	-	-	-	-
[AUX.AUX02UPS_CABLEADO] CABLEADO	0,1	50%	-	-	-	-
[AUX.AUX05UPS_ANTENAS] ANTENAS	0,1	50%	-	-	-	-
[AUX.AUX07UPS_SISTALIMENT] SIST_ALIMENTAC_INENTERRUMPIDA	0,1	1%	-	-	-	-
[INST01_BLOQUEA] BLOQUE_A	1	100%	-	-	-	-

[N.*] Desastres naturales

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[HW.HW01UPS_SBDD] SER_BDD	0,1	100%	-	-	-	-
[HW.HW04UPS_ROUTER] ROUTER	0,1	100%	-	-	-	-
[HW.HW05UPS_SWITCH] SWITCH	0,1	100%	-	-	-	-
[HW.HW06UPS_SCORREO] SER_CORREO	0,1	100%	-	-	-	-
[AUX.AUX01UPS_GELECTRICO] GEN_ELECTRICO	0,1	1%	-	-	-	-
[AUX.AUX02UPS_CABLEADO] CABLEADO	0,1	100%	-	-	-	-
[AUX.AUX05UPS_ANTENAS] ANTENAS	0,1	100%	-	-	-	-
[AUX.AUX07UPS_SISTALIMENT] SIST_ALIMENTAC_INENTERRUMPIDA	0,1	1%	-	-	-	-
[INST01_BLOQUEA] BLOQUE_A	0,5	100%	-	-	-	-

[I.1] Fuego

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[HW.HW01UPS_SBDD] SER_BDD	0,5	100%	-	-	-	-
[HW.HW04UPS_ROUTER] ROUTER	0,5	100%	-	-	-	-
[HW.HW05UPS_SWITCH] SWITCH	0,5	100%	-	-	-	-
[HW.HW06UPS_SCORREO] SER_CORREO	0,5	100%	-	-	-	-
[AUX.AUX01UPS_GELECTRICO] GEN_ELECTRICO	0,5	1%	-	-	-	-
[AUX.AUX02UPS_CABLEADO] CABLEADO	0,5	100%	-	-	-	-
[AUX.AUX05UPS_ANTENAS] ANTENAS	0,5	100%	-	-	-	-
[AUX.AUX07UPS_SISTALIMENT] SIST_ALIMENTAC_INENTERRUMPIDA	0,5	1%	-	-	-	-
[INST01_BLOQUEA] BLOQUE_A	1	100%	-	-	-	-

[I.2] Daños por agua

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[HW.HW01UPS_SBDD] SER_BDD	0,5	50%	-	-	-	-
[HW.HW04UPS_ROUTER] ROUTER	0,5	50%	-	-	-	-
[HW.HW05UPS_SWITCH] SWITCH	0,5	50%	-	-	-	-
[HW.HW06UPS_SCORREO] SER_CORREO	0,5	50%	-	-	-	-

[AUX.AUX01UPS_GELECTRICO] GEN_ELECTRICO	0,5	1%	-	-	-	-
[AUX.AUX02UPS_CABLEADO] CABLEADO	0,5	50%	-	-	-	-
[AUX.AUX05UPS_ANTENAS] ANTENAS	0,5	50%	-	-	-	-
[AUX.AUX07UPS_SISTALIMENT] SIST_ALIMENTAC_INENTERRUMPIDA	0,5	1%	-	-	-	-
[INST01_BLOQUEA] BLOQUE_A	1	100%	-	-	-	-

[I.*] Desastres industriales

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[HW.HW01UPS_SBDD] SER_BDD	0,5	100%	-	-	-	-
[HW.HW04UPS_ROUTER] ROUTER	0,5	100%	-	-	-	-
[HW.HW05UPS_SWITCH] SWITCH	0,5	100%	-	-	-	-
[HW.HW06UPS_SCORREO] SER_CORREO	0,5	100%	-	-	-	-
[AUX.AUX01UPS_GELECTRICO] GEN_ELECTRICO	0,5	1%	-	-	-	-
[AUX.AUX02UPS_CABLEADO] CABLEADO	0,5	100%	-	-	-	-
[AUX.AUX05UPS_ANTENAS] ANTENAS	0,5	100%	-	-	-	-
[AUX.AUX07UPS_SISTALIMENT] SIST_ALIMENTAC_INENTERRUMPIDA	0,5	1%	-	-	-	-
[INST01_BLOQUEA] BLOQUE_A	1	100%	-	-	-	-

[I.3] Contaminación medioambiental

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[HW.HW01UPS_SBDD] SER_BDD	0,1	50%	-	-	-	-
[HW.HW04UPS_ROUTER] ROUTER	0,1	50%	-	-	-	-
[HW.HW05UPS_SWITCH] SWITCH	0,1	50%	-	-	-	-
[HW.HW06UPS_SCORREO] SER_CORREO	0,1	50%	-	-	-	-
[AUX.AUX01UPS_GELECTRICO] GEN_ELECTRICO	0,1	1%	-	-	-	-
[AUX.AUX02UPS_CABLEADO] CABLEADO	0,1	50%	-	-	-	-
[AUX.AUX05UPS_ANTENAS] ANTENAS	0,1	50%	-	-	-	-
[AUX.AUX07UPS_SISTALIMENT] SIST_ALIMENTAC_INENTERRUMPIDA	0,1	1%	-	-	-	-
[INST01_BLOQUEA] BLOQUE_A	1	10%	-	-	-	-

[I.4] Contaminación electromagnética

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[HW.HW01UPS_SBDD] SER_BDD	1	10%	-	-	-	-
[HW.HW04UPS_ROUTER] ROUTER	1	10%	-	-	-	-
[HW.HW05UPS_SWITCH] SWITCH	1	10%	-	-	-	-
[HW.HW06UPS_SCORREO] SER_CORREO	1	10%	-	-	-	-
[AUX.AUX02UPS_CABLEADO] CABLEADO	0,5	10%	-	-	-	-
[INST01_BLOQUEA] BLOQUE_A	0,1	10%	-	-	-	-

[I.5] Avería de origen físico o lógico

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[SW.SOFT01UPS_SNA] SNA	1	50%	-	-	-	-
[SW.SOF02UPS_SQUAD] SQUAD	1	50%	-	-	-	-
[SW.SOF05UPS_SIST_OPER] SIST_OPERATIVO	1	50%	-	-	-	-

[SW.SOF06UPS_SIST_SOLICIT] SIST_SOLICITUDES	1	50%	-	-	-	-
[SW.SOF07UPS_CORREO_ELEC] CORREO_ELECTRONICO	1	50%	-	-	-	-
[SW.SOF08UPS_BIBLIO] SIST_BIBLIOTECA	1	50%	-	-	-	-
[HW.HW01UPS_SBDD] SER_BDD	1	50%	-	-	-	-
[HW.HW04UPS_ROUTER] ROUTER	1	50%	-	-	-	-
[HW.HW05UPS_SWITCH] SWITCH	1	50%	-	-	-	-
[HW.HW06UPS_SCORREO] SER_CORREO	1	50%	-	-	-	-

[I.6] Corte del suministro eléctrico

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[HW.HW01UPS_SBDD] SER_BDD	1	100%	-	-	-	-
[HW.HW04UPS_ROUTER] ROUTER	1	100%	-	-	-	-
[HW.HW05UPS_SWITCH] SWITCH	1	100%	-	-	-	-
[HW.HW06UPS_SCORREO] SER_CORREO	1	100%	-	-	-	-

[I.7] Condiciones inadecuadas de temperatura o humedad

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[HW.HW01UPS_SBDD] SER_BDD	1	100%	-	-	-	-
[HW.HW04UPS_ROUTER] ROUTER	1	100%	-	-	-	-
[HW.HW05UPS_SWITCH] SWITCH	1	100%	-	-	-	-
[HW.HW06UPS_SCORREO] SER_CORREO	1	100%	-	-	-	-

[I.8] Fallo de servicios de comunicaciones

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[COM.COM02UPS_WI-FI] WI_FI	1	50%	-	-	-	-
[COM.COM03UPS_LAN] RED_LAN	1	50%	-	-	-	-
[COM.COM04_WAN] RED_WAN	1	50%	-	-	-	-
[COM.COM04UPS_INTERNET] INTERNET	1	50%	-	-	-	-
[COM.COM05UPS_INTRANET] INTRANET	1	50%	-	-	-	-

[I.9] Interrupción de otros servicios o suministros esenciales

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[AUX.AUX01UPS_GELECTRICO] GEN_ELECTRICO	1	1%	-	-	-	-

[I.11] Emanaciones electromagnéticas

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[HW.HW01UPS_SBDD] SER_BDD	1	-	-	1%	-	-
[HW.HW04UPS_ROUTER] ROUTER	1	-	-	1%	-	-
[HW.HW05UPS_SWITCH] SWITCH	1	-	-	1%	-	-
[AUX.AUX02UPS_CABLEADO] CABLEADO	1	-	-	1%	-	-
[INST01_BLOQUEA] BLOQUE_A	0,1	-	-	1%	-	-

[E.1] Errores de los usuarios

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[SW.SOFT01UPS_SNA] SNA	1	1%	10%	10%	-	-
[SW.SOF02UPS_SQUAD] SQUAD	1	1%	10%	10%	-	-

[SW.SOF05UPS_SIST_OPER] SIST_OPERATIVO	1	1%	10%	10%	-	-
[SW.SOF06UPS_SIST_SOLICIT] SIST_SOLICITUDES	1	1%	-	-	-	-
[SW.SOF07UPS_CORREO_ELEC] CORREO_ELECTRONICO	1	1%	-	-	-	-
[SW.SOF08UPS_BIBLIO] SIST_BIBLIOTECA	1	1%	-	-	-	-

[E.2] Errores del administrador del sistema / de la seguridad

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[SW.SOFT01UPS_SNA] SNA	1	20%	20%	20%	-	-
[SW.SOF02UPS_SQUAD] SQUAD	1	20%	20%	20%	-	-
[SW.SOF05UPS_SIST_OPER] SIST_OPERATIVO	1	20%	20%	20%	-	-
[SW.SOF06UPS_SIST_SOLICIT] SIST_SOLICITUDES	1	20%	-	-	-	-
[SW.SOF07UPS_CORREO_ELEC] CORREO_ELECTRONICO	1	20%	-	-	-	-
[SW.SOF08UPS_BIBLIO] SIST_BIBLIOTECA	1	20%	-	-	-	-
[HW.HW01UPS_SBDD] SER_BDD	1	20%	20%	20%	-	-
[HW.HW04UPS_ROUTER] ROUTER	1	20%	20%	20%	-	-
[HW.HW05UPS_SWITCH] SWITCH	1	20%	20%	20%	-	-
[HW.HW06UPS_SCORREO] SER_CORREO	1	20%	-	-	-	-
[COM.COM02UPS_WI-FI] WI_FI	1	20%	20%	20%	-	-
[COM.COM03UPS_LAN] RED_LAN	1	20%	20%	20%	-	-
[COM.COM04_WAN] RED_WAN	1	20%	20%	20%	-	-
[COM.COM04UPS_INTERNET] INTERNET	1	20%	-	-	-	-
[COM.COM05UPS_INTRANET] INTRANET	1	20%	-	-	-	-

[E.8] Difusión de software dañino

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[SW.SOFT01UPS_SNA] SNA	1	10%	10%	10%	-	-
[SW.SOF02UPS_SQUAD] SQUAD	1	10%	10%	10%	-	-
[SW.SOF05UPS_SIST_OPER] SIST_OPERATIVO	1	10%	10%	10%	-	-
[SW.SOF06UPS_SIST_SOLICIT] SIST_SOLICITUDES	1	10%	-	-	-	-
[SW.SOF07UPS_CORREO_ELEC] CORREO_ELECTRONICO	1	10%	-	-	-	-
[SW.SOF08UPS_BIBLIO] SIST_BIBLIOTECA	1	10%	-	-	-	-

[E.9] Errores de [re-]encaminamiento

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[COM.COM02UPS_WI-FI] WI_FI	1	-	-	10%	-	-
[COM.COM03UPS_LAN] RED_LAN	1	-	-	10%	-	-
[COM.COM04_WAN] RED_WAN	1	-	-	10%	-	-

[E.10] Errores de secuencia

activo	*frecuencia*	[D]	[I]	[C]	[A]	[T]
[COM.COM02UPS_WI-FI] WI_FI	1	-	10%	-	-	-
[COM.COM03UPS_LAN] RED_LAN	1	-	10%	-	-	-
[COM.COM04_WAN] RED_WAN	1	-	10%	-	-	-

[E.15] Alteración de la información

activo	*frecuencia*	[D]	[I]	[C]	[A]	[T]
[SW.SOFT01UPS_SNA] SNA	1	-	1%	-	-	-
[SW.SOF02UPS_SQUAD] SQUAD	1	-	1%	-	-	-
[SW.SOF05UPS_SIST_OPER] SIST_OPERATIVO	1	-	1%	-	-	-
[COM.COM02UPS_WI-FI] WI_FI	1	-	1%	-	-	-
[COM.COM03UPS_LAN] RED_LAN	1	-	1%	-	-	-
[COM.COM04_WAN] RED_WAN	1	-	1%	-	-	-

[E.18] Destrucción de la información

activo	*frecuencia*	[D]	[I]	[C]	[A]	[T]
[SW.SOFT01UPS_SNA] SNA	1	50%	-	-	-	-
[SW.SOF02UPS_SQUAD] SQUAD	1	50%	-	-	-	-
[SW.SOF05UPS_SIST_OPER] SIST_OPERATIVO	1	50%	-	-	-	-
[SW.SOF06UPS_SIST_SOLICIT] SIST_SOLICITUDES	1	50%	-	-	-	-
[SW.SOF07UPS_CORREO_ELEC] CORREO_ELECTRONICO	1	50%	-	-	-	-
[SW.SOF08UPS_BIBLIO] SIST_BIBLIOTECA	1	50%	-	-	-	-

[E.19] Fugas de información

activo	*frecuencia*	[D]	[I]	[C]	[A]	[T]
[SW.SOFT01UPS_SNA] SNA	1	-	-	10%	-	-
[SW.SOF02UPS_SQUAD] SQUAD	1	-	-	10%	-	-
[SW.SOF05UPS_SIST_OPER] SIST_OPERATIVO	1	-	-	10%	-	-
[COM.COM02UPS_WI-FI] WI_FI	1	-	-	10%	-	-
[COM.COM03UPS_LAN] RED_LAN	1	-	-	10%	-	-
[COM.COM04_WAN] RED_WAN	1	-	-	10%	-	-
[PER01UPS_COORDINADOR] COORDINADOR_UNADEVI	1	-	-	10%	-	-
[PER02UPS_PROGR] PROGRAMADORES	1	-	-	10%	-	-

[E.20] Vulnerabilidades de los programas (software)

activo	*frecuencia*	[D]	[I]	[C]	[A]	[T]
[SW.SOFT01UPS_SNA] SNA	1	1%	20%	20%	-	-
[SW.SOF02UPS_SQUAD] SQUAD	1	1%	20%	20%	-	-
[SW.SOF05UPS_SIST_OPER] SIST_OPERATIVO	1	1%	20%	20%	-	-
[SW.SOF06UPS_SIST_SOLICIT] SIST_SOLICITUDES	1	1%	-	-	-	-
[SW.SOF07UPS_CORREO_ELEC] CORREO_ELECTRONICO	1	1%	-	-	-	-

[SW.SOF08UPS_BIBLIO] SIST_BIBLIOTECA	1	1%	-	-	-	-

[E.21] Errores de mantenimiento / actualización de programas (software)

activo	*frecuencia*	[D]	[I]	[C]	[A]	[T]
[SW.SOFT01UPS_SNA] SNA	10	1%	1%	-	-	-
[SW.SOF02UPS_SQUAD] SQUAD	10	1%	1%	-	-	-
[SW.SOF05UPS_SIST_OPER] SIST_OPERATIVO	10	1%	1%	-	-	-
[SW.SOF06UPS_SIST_SOLICIT] SIST_SOLICITUDES	10	1%	-	-	-	-
[SW.SOF07UPS_CORREO_ELEC] CORREO_ELECTRONICO	10	1%	-	-	-	-
[SW.SOF08UPS_BIBLIO] SIST_BIBLIOTECA	10	1%	-	-	-	-

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

activo	*frecuencia*	[D]	[I]	[C]	[A]	[T]
[HW.HW01UPS_SBDD] SER_BDD	1	10%	-	-	-	-
[HW.HW04UPS_ROUTER] ROUTER	1	10%	-	-	-	-
[HW.HW05UPS_SWITCH] SWITCH	1	10%	-	-	-	-
[HW.HW06UPS_SCORREO] SER_CORREO	1	10%	-	-	-	-
[AUX.AUX01UPS_GELECTRICO] GEN_ELECTRICO	1	1%	-	-	-	-
[AUX.AUX02UPS_CABLEADO] CABLEADO	1	10%	-	-	-	-
[AUX.AUX05UPS_ANTENAS] ANTENAS	1	10%	-	-	-	-
[AUX.AUX07UPS_SISTALIMENT] SIST_ALIMENTAC_INENTERRUMPIDA	1	1%	-	-	-	-

[E.24] Caída del sistema por agotamiento de recursos

activo	*frecuencia*	[D]	[I]	[C]	[A]	[T]
[HW.HW01UPS_SBDD] SER_BDD	10	50%	-	-	-	-
[HW.HW04UPS_ROUTER] ROUTER	10	50%	-	-	-	-
[HW.HW05UPS_SWITCH] SWITCH	10	50%	-	-	-	-
[HW.HW06UPS_SCORREO] SER_CORREO	10	50%	-	-	-	-
[COM.COM02UPS_WI-FI] WI_FI	1	50%	-	-	-	-
[COM.COM03UPS_LAN] RED_LAN	1	50%	-	-	-	-
[COM.COM04_WAN] RED_WAN	1	50%	-	-	-	-
[COM.COM04UPS_INTERNET] INTERNET	1	50%	-	-	-	-
[COM.COM05UPS_INTRANET] INTRANET	1	50%	-	-	-	-

[E.25] Pérdida de equipos

activo	*frecuencia*	[D]	[I]	[C]	[A]	[T]
[HW.HW01UPS_SBDD] SER_BDD	1	100%	-	100%	-	-
[HW.HW04UPS_ROUTER] ROUTER	1	20%	-	50%	-	-
[HW.HW05UPS_SWITCH] SWITCH	1	20%	-	50%	-	-
[HW.HW06UPS_SCORREO] SER_CORREO	1	100%	-	-	-	-

[A.5] Suplantación de la identidad

activo	*frecuencia*	[D]	[I]	[C]	[A]	[T]
[SW.SOFT01UPS_SNA] SNA	1	-	50%	50%	100%	-
[SW.SOF02UPS_SQUAD] SQUAD	1	-	50%	50%	100%	-
[SW.SOF05UPS_SIST_OPER] SIST_OPERATIVO	1	-	50%	50%	100%	-
[SW.SOF06UPS_SIST_SOLICIT] SIST_SOLICITUDES	1	-	-	-	100%	-
[SW.SOF07UPS_CORREO_ELEC] CORREO_ELECTRONICO	1	-	-	-	100%	-
[SW.SOF08UPS_BIBLIO] SIST_BIBLIOTECA	1	-	-	-	100%	-
[COM.COM02UPS_WI-FI] WI_FI	1	-	10%	50%	100%	-
[COM.COM03UPS_LAN] RED_LAN	1	-	10%	50%	100%	-
[COM.COM04_WAN] RED_WAN	1	-	10%	50%	100%	-
[COM.COM04UPS_INTERNET] INTERNET	1	-	-	-	100%	-
[COM.COM05UPS_INTRANET] INTRANET	1	-	-	-	100%	-
[INST01_BLOQUEA] BLOQUE_A	1	-	10%	50%	-	-

[A.6] Abuso de privilegios de acceso

activo	*frecuencia*	[D]	[I]	[C]	[A]	[T]
[SW.SOFT01UPS_SNA] SNA	1	1%	10%	10%	-	-
[SW.SOF02UPS_SQUAD] SQUAD	1	1%	10%	10%	-	-
[SW.SOF05UPS_SIST_OPER] SIST_OPERATIVO	1	1%	10%	10%	-	-
[SW.SOF06UPS_SIST_SOLICIT] SIST_SOLICITUDES	1	1%	-	-	-	-
[SW.SOF07UPS_CORREO_ELEC] CORREO_ELECTRONICO	1	1%	-	-	-	-
[SW.SOF08UPS_BIBLIO] SIST_BIBLIOTECA	1	1%	-	-	-	-
[HW.HW01UPS_SBDD] SER_BDD	1	10%	100%	100%	-	-
[HW.HW04UPS_ROUTER] ROUTER	1	10%	10%	50%	-	-
[HW.HW05UPS_SWITCH] SWITCH	1	10%	10%	50%	-	-
[HW.HW06UPS_SCORREO] SER_CORREO	1	10%	-	-	-	-
[COM.COM02UPS_WI-FI] WI_FI	1	-	10%	50%	100%	-
[COM.COM03UPS_LAN] RED_LAN	1	-	10%	50%	100%	-
[COM.COM04_WAN] RED_WAN	1	-	10%	50%	100%	-
[COM.COM04UPS_INTERNET] INTERNET	1	-	-	-	100%	-
[COM.COM05UPS_INTRANET] INTRANET	1	-	-	-	100%	-
[INST01_BLOQUEA] BLOQUE_A	1	10%	10%	50%	-	-

[A.7] Uso no previsto

activo	*frecuencia*	[D]	[I]	[C]	[A]	[T]
[SW.SOFT01UPS_SNA] SNA	1	1%	10%	10%	-	-
[SW.SOF02UPS_SQUAD] SQUAD	1	1%	10%	10%	-	-
[SW.SOF05UPS_SIST_OPER] SIST_OPERATIVO	1	1%	10%	10%	-	-

[SW.SOF06UPS_SIST_SOLICIT] SIST_SOLICITUDES	1	1%	-	-	-	-
[SW.SOF07UPS_CORREO_ELEC] CORREO_ELECTRONICO	1	1%	-	-	-	-
[SW.SOF08UPS_BIBLIO] SIST_BIBLIOTECA	1	1%	-	-	-	-
[HW.HW01UPS_SBDD] SER_BDD	1	10%	10%	100%	-	-
[HW.HW04UPS_ROUTER] ROUTER	1	10%	1%	10%	-	-
[HW.HW05UPS_SWITCH] SWITCH	1	10%	1%	10%	-	-
[HW.HW06UPS_SCORREO] SER_CORREO	1	10%	-	-	-	-
[COM.COM02UPS_WI-FI] WI_FI	1	10%	10%	10%	-	-
[COM.COM03UPS_LAN] RED_LAN	1	10%	10%	10%	-	-
[COM.COM04_WAN] RED_WAN	1	10%	10%	10%	-	-
[COM.COM04UPS_INTERNET] INTERNET	1	10%	-	-	-	-
[COM.COM05UPS_INTRANET] INTRANET	1	10%	-	-	-	-
[AUX.AUX01UPS_GELECTRICO] GEN_ELECTRICO	1	1%	-	-	-	-
[AUX.AUX02UPS_CABLEADO] CABLEADO	1	50%	1%	1%	-	-
[AUX.AUX05UPS_ANTENAS] ANTENAS	1	50%	1%	1%	-	-
[AUX.AUX07UPS_SISTALIMENT] SIST_ALIMENTAC_INENTERRUMPIDA	1	1%	-	-	-	-
[INST01_BLOQUEA] BLOQUE_A	1	10%	10%	50%	-	-

[A.8] Difusión de software dañino

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[SW.SOFT01UPS_SNA] SNA	1	100%	100%	100%	-	-
[SW.SOF02UPS_SQUAD] SQUAD	1	100%	100%	100%	-	-
[SW.SOF05UPS_SIST_OPER] SIST_OPERATIVO	1	100%	100%	100%	-	-
[SW.SOF06UPS_SIST_SOLICIT] SIST_SOLICITUDES	1	100%	-	-	-	-
[SW.SOF07UPS_CORREO_ELEC] CORREO_ELECTRONICO	1	100%	-	-	-	-
[SW.SOF08UPS_BIBLIO] SIST_BIBLIOTECA	1	100%	-	-	-	-

[A.9] [Re-]encaminamiento de mensajes

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[COM.COM02UPS_WI-FI] WI_FI	1	-	-	10%	-	-
[COM.COM03UPS_LAN] RED_LAN	1	-	-	10%	-	-
[COM.COM04_WAN] RED_WAN	1	-	-	10%	-	-

[A.10] Alteración de secuencia

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[COM.COM02UPS_WI-FI] WI_FI	1	-	10%	-	-	-
[COM.COM03UPS_LAN] RED_LAN	1	-	10%	-	-	-
[COM.COM04_WAN] RED_WAN	1	-	10%	-	-	-

[A.11] Acceso no autorizado

activo	*frecuencia*	[D]	[I]	[C]	[A]	[T]
[SW.SOFT01UPS_SNA] SNA	1	-	10%	50%	-	-
[SW.SOF02UPS_SQUAD] SQUAD	1	-	10%	50%	-	-
[SW.SOF05UPS_SIST_OPER] SIST_OPERATIVO	1	-	10%	50%	-	-
[HW.HW01UPS_SBDD] SER_BDD	1	10%	100%	100%	-	-
[HW.HW04UPS_ROUTER] ROUTER	1	10%	10%	50%	-	-
[HW.HW05UPS_SWITCH] SWITCH	1	10%	10%	50%	-	-
[HW.HW06UPS_SCORREO] SER_CORREO	1	10%	-	-	-	-
[COM.COM02UPS_WI-FI] WI_FI	1	-	10%	50%	100%	-
[COM.COM03UPS_LAN] RED_LAN	1	-	10%	50%	100%	-
[COM.COM04_WAN] RED_WAN	1	-	10%	50%	100%	-
[COM.COM04UPS_INTERNET] INTERNET	1	-	-	-	100%	-
[COM.COM05UPS_INTRANET] INTRANET	1	-	-	-	100%	-
[AUX.AUX02UPS_CABLEADO] CABLEADO	1	-	10%	50%	-	-
[INST01_BLOQUEA] BLOQUE_A	5	-	10%	50%	-	-

[A.12] Análisis de tráfico

activo	*frecuencia*	[D]	[I]	[C]	[A]	[T]
[COM.COM02UPS_WI-FI] WI_FI	1	-	-	2%	-	-
[COM.COM03UPS_LAN] RED_LAN	1	-	-	2%	-	-
[COM.COM04_WAN] RED_WAN	1	-	-	2%	-	-

[A.14] Interceptación de información (escucha)

activo	*frecuencia*	[D]	[I]	[C]	[A]	[T]
[COM.COM02UPS_WI-FI] WI_FI	1	-	-	10%	-	-
[COM.COM03UPS_LAN] RED_LAN	1	-	-	1%	-	-
[COM.COM04_WAN] RED_WAN	1	-	-	10%	-	-

[A.15] Modificación de la información

activo	*frecuencia*	[D]	[I]	[C]	[A]	[T]
[SW.SOFT01UPS_SNA] SNA	1	-	50%	-	-	-
[SW.SOF02UPS_SQUAD] SQUAD	1	-	50%	-	-	-
[SW.SOF05UPS_SIST_OPER] SIST_OPERATIVO	1	-	50%	-	-	-
[COM.COM02UPS_WI-FI] WI_FI	1	-	10%	-	-	-
[COM.COM03UPS_LAN] RED_LAN	1	-	10%	-	-	-
[COM.COM04_WAN] RED_WAN	1	-	10%	-	-	-

[A.18] Destrucción de la información

activo	*frecuencia*	[D]	[I]	[C]	[A]	[T]
[SW.SOFT01UPS_SNA] SNA	1	50%	-	-	-	-
[SW.SOF02UPS_SQUAD] SQUAD	1	50%	-	-	-	-
[SW.SOF05UPS_SIST_OPER] SIST_OPERATIVO	1	50%	-	-	-	-

[SW.SOF06UPS_SIST_SOLICIT] SIST_SOLICITUDES	1	50%	-	-	-	-
[SW.SOF07UPS_CORREO_ELEC] CORREO_ELECTRONICO	1	50%	-	-	-	-
[SW.SOF08UPS_BIBLIO] SIST_BIBLIOTECA	1	50%	-	-	-	-
[COM.COM02UPS_WI-FI] WI_FI	1	50%	-	-	-	-
[COM.COM03UPS_LAN] RED_LAN	1	50%	-	-	-	-
[COM.COM04_WAN] RED_WAN	1	50%	-	-	-	-
[COM.COM04UPS_INTERNET] INTERNET	1	50%	-	-	-	-
[COM.COM05UPS_INTRANET] INTRANET	1	50%	-	-	-	-

[A.19] Revelación de información

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[SW.SOFT01UPS_SNA] SNA	1	-	-	50%	-	-
[SW.SOF02UPS_SQUAD] SQUAD	1	-	-	50%	-	-
[SW.SOF05UPS_SIST_OPER] SIST_OPERATIVO	1	-	-	50%	-	-
[COM.COM02UPS_WI-FI] WI_FI	1	-	-	50%	-	-
[COM.COM03UPS_LAN] RED_LAN	1	-	-	50%	-	-
[COM.COM04_WAN] RED_WAN	1	-	-	50%	-	-
[PER01UPS_COORDINADOR] COORDINADOR_UNADEVI	10	-	-	50%	-	-
[PER02UPS_PROGR] PROGRAMADORES	10	-	-	50%	-	-

[A.22] Manipulación de programas

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[SW.SOFT01UPS_SNA] SNA	1	50%	100%	100%	-	-
[SW.SOF02UPS_SQUAD] SQUAD	1	50%	100%	100%	-	-
[SW.SOF05UPS_SIST_OPER] SIST_OPERATIVO	1	50%	100%	100%	-	-
[SW.SOF06UPS_SIST_SOLICIT] SIST_SOLICITUDES	1	50%	-	-	-	-
[SW.SOF07UPS_CORREO_ELEC] CORREO_ELECTRONICO	1	50%	-	-	-	-
[SW.SOF08UPS_BIBLIO] SIST_BIBLIOTECA	1	50%	-	-	-	-

[A.23] Manipulación del hardware

activo	***frecuencia***	[D]	[I]	[C]	[A]	[T]
[HW.HW01UPS_SBDD] SER_BDD	0	50%	-	50%	-	-
[HW.HW04UPS_ROUTER] ROUTER	0,5	100%	-	50%	-	-
[HW.HW05UPS_SWITCH] SWITCH	0,5	100%	-	50%	-	-
[HW.HW06UPS_SCORREO] SER_CORREO	0,5	50%	-	-	-	-
[AUX.AUX01UPS_GELECTRICO] GEN_ELECTRICO	1	1%	-	-	-	-
[AUX.AUX02UPS_CABLEADO] CABLEADO	1	50%	-	50%	-	-
[AUX.AUX05UPS_ANTENAS] ANTENAS	1	50%	-	50%	-	-
[AUX.AUX07UPS_SISTALIMENT] SIST_ALIMENTAC_INENTERRUMPIDA	1	1%	-	-	-	-

[A.24] Denegación de servicio

activo	*frecuencia*	[D]	[I]	[C]	[A]	[T]
[HW.HW01UPS_SBDD] SER_BDD	2	100%	-	-	-	-
[HW.HW04UPS_ROUTER] ROUTER	2	100%	-	-	-	-
[HW.HW05UPS_SWITCH] SWITCH	2	100%	-	-	-	-
[HW.HW06UPS_SCORREO] SER_CORREO	2	100%	-	-	-	-
[COM.COM02UPS_WI-FI] WI_FI	10	50%	-	-	-	-
[COM.COM03UPS_LAN] RED_LAN	10	50%	-	-	-	-
[COM.COM04_WAN] RED_WAN	10	50%	-	-	-	-
[COM.COM04UPS_INTERNET] INTERNET	10	50%	-	-	-	-
[COM.COM05UPS_INTRANET] INTRANET	10	50%	-	-	-	-

[A.25] Robo de equipos

activo	*frecuencia*	[D]	[I]	[C]	[A]	[T]
[HW.HW01UPS_SBDD] SER_BDD	0,5	100%	-	100%	-	-
[HW.HW04UPS_ROUTER] ROUTER	0,5	20%	-	50%	-	-
[HW.HW05UPS_SWITCH] SWITCH	0,5	20%	-	50%	-	-
[HW.HW06UPS_SCORREO] SER_CORREO	0,5	100%	-	-	-	-
[AUX.AUX01UPS_GELECTRICO] GEN_ELECTRICO	0,5	1%	-	-	-	-
[AUX.AUX02UPS_CABLEADO] CABLEADO	0,8	100%	-	-	-	-
[AUX.AUX05UPS_ANTENAS] ANTENAS	0,5	10%	-	-	-	-
[AUX.AUX07UPS_SISTALIMENT] SIST_ALIMENTAC_INENTERRUMPIDA	0,5	1%	-	-	-	-

[A.26] Ataque destructivo

activo	*frecuencia*	[D]	[I]	[C]	[A]	[T]
[HW.HW01UPS_SBDD] SER_BDD	1	100%	-	-	-	-
[HW.HW04UPS_ROUTER] ROUTER	1	100%	-	-	-	-
[HW.HW05UPS_SWITCH] SWITCH	1	100%	-	-	-	-
[HW.HW06UPS_SCORREO] SER_CORREO	1	100%	-	-	-	-
[AUX.AUX01UPS_GELECTRICO] GEN_ELECTRICO	1	1%	-	-	-	-
[AUX.AUX02UPS_CABLEADO] CABLEADO	1	100%	-	-	-	-
[AUX.AUX05UPS_ANTENAS] ANTENAS	1	10%	-	-	-	-
[AUX.AUX07UPS_SISTALIMENT] SIST_ALIMENTAC_INENTERRUMPIDA	1	1%	-	-	-	-
[INST01_BLOQUEA] BLOQUE_A	0,1	100%	-	-	-	-

[A.27] Ocupación enemiga

activo	*frecuencia*	[D]	[I]	[C]	[A]	[T]
[INST01_BLOQUEA] BLOQUE_A	1	100%	-	50%	-	-

[A.29] Extorsión

activo	*frecuencia*	[D]	[I]	[C]	[A]	[T]
[PER01UPS_COORDINADOR] COORDINADOR_UNADEVI	0,9	-	-	100%	-	-
[PER02UPS_PROGR] PROGRAMADORES	0,9	-	-	100%	-	-

[A.30] Ingeniería social (picaresca)

activo	*frecuencia*	[D]	[I]	[C]	[A]	[T]
[PER01UPS_COORDINADOR] COORDINADOR_UNADEVI	0,5	-	-	100%	-	-
[PER02UPS_PROGR] PROGRAMADORES	0,5	-	-	100%	-	-