
# Plan Institucional de Seguridad de la Información (PISI)
# Versión 1.0

UNIVERSIDAD PÚBLICA DE EL ALTO (UPEA)

El Alto – La Paz - Bolivia
2022

# ÍNDICE

## 1. INTRODUCCIÓN

La información se considerada un activo imprescindible y muy valioso en todo ámbito de organización sea de carácter público o privado. Debido, al avance acelerado de las tecnologías de información, la seguridad de la información tiende a ser vulnerable y susceptible a recibir ciberataques que pueden ocasionar perjuicios al desenvolvimiento normal de la institución. Por lo que se hace muy necesario una adecuada gestión de seguridad de la información.

La protección de la seguridad de la información representa un reto para garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información.

La Universidad Pública de El Alto (UPEA), tomando en cuenta la importancia fundamental que representa la seguridad de la información, mediante el presente Plan Institucional de Seguridad de la Información (PISI), define las políticas, lineamientos y controles de gestión de riesgos de la seguridad de la información, en base a las normativas bolivianas vigentes.

## 2. MARCO NORMATIVO

La normativa vigente concerniente a la seguridad de la información, que otorga el respaldo a la elaboración del presente Plan Institucional de Seguridad de la Información de la UPEA, se compone de:

- El Parágrafo I del Artículo N° 72 de la Ley N° 164 de 28 de julio de 2011, Ley General de Telecomunicaciones, que establece que: "*El Estado en todos sus niveles, fomentará el acceso, uso y apropiación social de las tecnologías de información y comunicación, el despliegue y uso de infraestructura, el desarrollo de contenidos y aplicaciones, la protección de las usuarias y usuarios, la seguridad informática y de redes, como mecanismos de democratización de oportunidades para todos los sectores de la sociedad y especialmente para aquellos con menores ingresos y con necesidades especiales*".

- El inciso d) del parágrafo II del Artículo 4 (Principios), del Reglamento para el Desarrollo de Tecnologías de Información y Comunicación aprobado mediante el parágrafo I) del Artículo Único del Decreto Supremo N° 1793 de 13 de noviembre de 2013, que señala que: "*Seguridad: Se debe implementar los controles técnicos y administrativos que se requieran para preservar la confidencialidad, integridad, disponibilidad, autenticidad, no repudio y confiabilidad de la información, brindando seguridad a los registros, evitando su falsificación, extravío, utilización y acceso no autorizado o fraudulento;*". Asimismo, el Articulo 8 (Plan de contingencia) del Reglamento para el Desarrollo de Tecnologías de Información y Comunicación aprobado mediante el parágrafo I) del Artículo Único del Decreto Supremo N° 1793, de 13 de noviembre de 2013, que menciona: "*Las entidades públicas promoverán la seguridad informática para la protección de datos en sus sistemas*

*informáticos, a través de planes de contingencia desarrollados e implementados en cada entidad*".

- El Decreto Supremo N° 2514 de 9 de septiembre de 2015, el cual dispone en su Inciso f) del Artículo 7 que la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC) establecerá: "*los lineamientos técnicos en seguridad de información para las entidades del sector público*". Asimismo, el Inciso i) del Artículo 7, establece entre las funciones de la AGETIC "*Elaborar, proponer, promover, gestionar, articular y actualizar el Plan de Implementación de Gobierno Electrónico y el Plan de Implementación de Software Libre y Estándares Abiertos para las entidades del sector público; y otros planes relacionados con el ámbito de gobierno electrónico y seguridad informática*". Por otra parte, el Parágrafo I del Artículo 8, determina la creación del "*Centro de Gestión de Incidentes informáticos — CGII como parte de la estructura técnico operativa de la AGETIC*"; que según, el Inciso c) del Parágrafo II del Artículo 8 una de sus funciones es "*Establecer los lineamientos para la elaboración de Planes de Seguridad de Información de las entidades del sector público*".

- El Decreto Supremo N° 3251 del 12 de Julio de 2017 que en su Artículo 1 inciso a) aprueba el Plan de implementación de Gobierno Electrónico, que establece coma una de las líneas estratégicas del mismo, la seguridad informática y de la información, cuya programación debe estar incluida en dicho Plan.

- Resolución Administrativa AGETIC/RA/0051/2017 de fecha 19 de septiembre de 2017, a través de la cual el Consejo para las Tecnologías de la Información y Comunicación del Estado Plurinacional de Bolivia (CTlC-EPB) aprueba el documento "Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la información de las entidades del sector público".

En base al marco normativo y en cumplimiento a lo establecido en la Política de Seguridad de la información emanado por la AGETIC se presenta este Plan Institucional de Seguridad de la Información de la UPEA, afín de proteger los activos de información con que cuenta la universidad, para lo cual se hace la identificación de los activos de información y sus riesgos, y los controles de seguridad a ser aplicados para la mitigación de riesgos.

## 3. TÉRMINOS, DEFINICIONES Y SIGLAS

### 3.1. TÉRMINOS Y DEFINICIONES

A continuación, se presentan las definiciones de los términos utilizados en el contenido de este documento.

**Activo de Información.** Conocimientos o datos que tienen valor para la organización; corresponde a aquellos datos físicos, digitales, sistemas y elementos tanto de

hardware coma de software que se encuentran relacionados con el flujo de almacenamiento de información, conocimientos a datos.

Los activos de la información, se clasifican en:

**Datos/Información:** En esta clasificación ingresan procesos relevantes para la institución e información en cualquier medio de soporte físico o digital. Los tipos de información que ingresarían son: información estratégica, información relacionada con el archivo personal, información relacionada a la documentación administrativa, legal, procesos de adjudicación y otros que tengan un coste económico y de cumplimiento con la normativa legal. También, en esta categoría está la información de archivos tales como respaldos, documentos, credenciales de acceso, entre otros.

**Claves criptográficas:** Las claves criptográficas, combinando secretos e información pública, son esenciales para garantizar el funcionamiento de los mecanismos criptográficos. Algunos de los ejemplos de activos en esta categoría son: claves para cifrar, firmar, certificados x509, entre otros.

**Servicios:** En esta categoría ingresan: servicios de acceso remoto, transferencia de archivos, correo electrónico, servicios web, servicio de directorio, entre otros.

**Software — aplicaciones informáticas:** En esta categoría se encuentran: sistemas desarrollados y/o adquiridos, software de aplicación, sistemas operativos, software de virtualización, entre otros.

**Equipamiento informático (hardware):** En esta categoría están los medios físicos que soportan los procesos como ser: servidores, equipamiento de escritorio, periféricos, dispositivos de red perimetral, dispositivos de red, corta fuegos, entre otros.

**Redes de comunicaciones:** Están los servicios de comunicaciones como ser: la red telefónica, redes de datos, internet, entre otros.

**Soportes de información:** En esta categoría están: discos virtuales y físicos, memorias usb, discos y cintas, material impreso, entre otros.

**Equipamiento auxiliar:** En esta categoría están: fuentes de alimentación, generadores eléctricos, equipos de climatización, cableado eléctrico, mobiliario, entre otros.

**Instalaciones:** Edificio, vehículos, instalaciones de refuerzo, entre otros.

**Personal:** Incluye personal fijo, eventual, terceros, entre otros. También, incluye a los responsables y custodios de los activos de información que son los mismos que pueden ser parte del personal administrativo, autoridades o representantes

docente o estudiantiles de la institución; quienes tienen a su cargo uno o varios activos de información de la institución.

**Amenaza:** Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización.

**Análisis de riesgos:** proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización. Determina impactos y riesgos.

**Ataque:** Intento de destruir, exponer, alterar o inhabilitar un sistema de información o la información que el sistema maneja, o violar alguna política de seguridad de alguna otra manera. [

**Clave:** Contraseña o password, que permite la autentificación y control del acceso hacia algún recurso.

**Código malicioso:** Software diseñado para ejecutar acciones maliciosas, como provocar daños al software de la computadora, robar información almacenada en un sistema informático, aprovechar recursos informáticos para efectuar otras acciones perjudiciales para el usuario, entre otros. Este tipo de software incluye programas coma virus, gusanos, troyanos y spyware; utiliza como vía de diseminación el correo electrónico, sitios de internet, redes, dispositivos móviles y/o, dispositivos removibles.

**Copias de Seguridad:** Denominada copia de seguridad, respaldo, copia de respaldo, copia de reserva a backup, es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.

**Dimensiones de valoración:** Son las características o atributos que hacen valioso un activo. Una dimensión es una faceta o aspecto de un activo, independiente de otras facetas.

Las dimensiones de valoración de activos de la información son:

**Disponibilidad:** Propiedad o característica de la información, que la hace accesible y utilizable a quienes deben acceder a ella, ya sean personas, procesos y/o aplicaciones cuando lo requieran.

**Integridad:** Propiedad o característica que salvaguarda la exactitud y completitud de la información.

**Confidencialidad:** Propiedad o característica que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

**Firewall:** Denominado también cortafuegos, es un sistema diseñado para prevenir el acceso no autorizado hacia o desde una red privada. Puede ser implementado como

hardware o software, o en una combinación de ambos. Los cortafuegos impiden que usuarios no autorizados accedan a redes privadas conectadas a Internet, especialmente a intranets.

**Gestión de riesgos:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

**Impacto:** Consecuencia que sobre un activo tiene la materialización de una amenaza.

**Política:** Intenciones y dirección de una organización, según lo expresado formalmente por su alta dirección.

**Política de Seguridad de la Información:** Acciones o directrices que establecen la postura institucional en relación a la seguridad de la información, incluidas dentro del Plan Institucional de Seguridad de la Información.

**Riesgo.** Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización. Indica lo que le podría pasar a los activos si no se protegieran adecuadamente.

**Salvaguarda:** Procedimiento o mecanismo tecnológico que reduce el riesgo.

**Seguridad de la información.** Es la preservación de la confidencialidad, integridad y disponibilidad de la información; además, también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no repudio y confiabilidad; mediante medidas principalmente preventivas.

**Sistema de información:** Es un conjunto de componentes físicos, lógicos, elementos de comunicación, datos y personal que interaccionan entre sí para lograr un objetivo común que permiten el almacenamiento, transmisión y proceso de la información.

**Tecnología de la información:** Hace referencia a las aplicaciones, información e infraestructura requerida por una entidad para apoyar el funcionamiento de los procesos y servicios.

**Tratamiento de riesgos**: Proceso destinado a modificar el riesgo.

**Usuario:** Es la persona que utiliza un dispositivo o un ordenador y realiza múltiples operaciones con distintos propósitos, ya sea generar contenido y documentos, utilizar software de diverso tipo, entre otras.

**Vulnerabilidad:** Defecto o debilidad que puede ser aprovechada por una amenaza, o más detalladamente a las debilidades de los activos o de sus medidas de protección que facilitan el éxito de una amenaza potencial. Se caracteriza por ausencia en controles de seguridad que permite ser explotada.

### 3.2. SIGLAS

**CUADRO N° 1**
**ABREVIACIONES UTILIZADAS**

| SIGLA | DESCRIPCIÓN |
|---|---|
| **AGETIC** | Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación |
| **CC** | Claves Criptográficas |
| **CGII** | Centro de Gestión de Incidentes Informáticos |
| **CPD** | Centro de Procesamiento de Datos o Centro de Datos (en inglés Data Center) |
| **CSI** | Comité de Seguridad de la Información |
| **CTIC-EPB** | Consejo para las Tecnologías de la Información y Comunicación del Estado Plurinacional de Bolivia |
| **DBA** | DataBase Administrator (en español: Administrador de Base de Datos) |
| **DICyT** | Dirección de Investigación, Ciencia y Tecnología |
| **DISBED** | Dirección de Interacción Social Bienestar Estudiantil y Deportes |
| **EA** | Equipamiento Auxiliar |
| **H** | Hardware |
| **HCU** | Honorable Consejo Universitario |
| **I** | Información (datos) |
| **ISO** | Internacional Organization for Standardization (en español: Organización Internacional de Normalización) |
| **L** | InstaLaciones |
| **MAE** | Máxima Autoridad Ejecutiva [rector(a)] |
| **MAGERIT** | Metodología de Análisis y Gestión de Riesgos |
| **P** | Personal |
| **PISI** | Plan Institucional de Seguridad de la Información |
| **RC** | Redes de Comunicaciones |
| **RCPD** | Responsable del Centro de Procesamiento de Datos (Data Center) |
| **RRAA** | Registros y Admisiones |
| **RRHH** | Recursos Humanos |
| **RSI** | Responsable de Seguridad de la Información |
| **S** | Servicios |
| **SA** | Software – Aplicaciones informáticas |
| **SI** | Soportes de Información |
| **SIE** | Sistemas de Información y Estadística |
| **UPEA** | Universidad Pública de El Alto. |
| **UPS** | Uninterruptable Power Supply (en español: Suministro o Sistema de alimentación ininterrumpida) |
| **VAI** | Valoración de Activo de Información |
| **VR** | Valoración de Riesgo |

**Fuente:** Elaboración Propia.

## 4. CONTEXTUALIZACIÓN Y DIAGNÓSTICO INSTITUCIONAL

### 4.1. CONTEXTO GENERAL DE LA UPEA

#### 4.1.1. VISIÓN

La UPEA es una institución que se proyecta al desarrollo de sus actividades académicos-productivas, científicas, tecnológicas de interacción social contemporáneo, para priorizar la investigación científica en todos los campos del conocimiento relacionado la teoría con la práctica para transformar la estructura económica, social, cultural y política vigente en favor de las naciones originarias y clases populares.

### 4.1.2. MISIÓN

Formar profesionales integrales altamente calificados en todas las disciplinas del conocimiento científico-tecnológico, con conciencia crítica y reflexiva; capaz de crear, adaptar y transformar la realidad en que vive; desarrollar la investigación productiva para fomentar el desarrollo local, regional y nacional para que responda al encargo social y las necesidades de las nacionalidades de manera eficiente y oportuna hacia la transformación revolucionaria de la sociedad.

### 4.1.3. UNIDADES ACADÉMICAS DE LA UPEA

La UPEA cuenta en la actualidad con las siguientes áreas y carreras:

**CUADRO N° 2**
**UNIDADES ACADÉMICAS DE LA UPEA**

| ÁREA | CARRERA |
|---|---|
| SIN AREA | INGENIERÍA DE SISTEMAS<br>DERECHO<br>CIENCIAS POLÍTICAS<br>CIENCIAS FÍSICAS Y ENERGÍAS ALTERNATIVAS |
| CIENCIAS ECONÓMICAS, FINANCIERAS Y ADMINISTRATIVAS | CONTADURÍA PÚBLICA<br>ECONOMÍA<br>ADMINISTRACIÓN DE EMPRESAS<br>COMERCIO INTERNACIONAL<br>GESTIÓN TURÍSTICA Y HOTELERA |
| INGENIERÍA DESARROLLO TECNOLÓGICO PRODUCTIVO | INGENIERÍA EN PRODUCCIÓN EMPRESARIAL<br>INGENIERÍA ELECTRÓNICA<br>INGENIERÍA TEXTIL<br>INGENIERÍA ELÉCTRICA<br>INGENIERÍA AUTOTRÓNICA<br>INGENIERÍA AMBIENTAL |
| CIENCIAS DE LA SALUD | ENFERMERÍA<br>MEDICINA<br>NUTRICIÓN Y DIETÉTICA |
| ESTOMATOLOGÍA | ODONTOLOGÍA<br>TECNOLOGÍA EN LABORATORIO DENTAL |
| CIENCIAS SOCIALES | CIENCIAS DEL DESARROLLO<br>CIENCIAS DE LA COMUNICACIÓN SOCIAL<br>HISTORIA<br>LINGÜÍSTICA E IDIOMAS<br>SOCIOLOGÍA<br>TRABAJO SOCIAL<br>PSICOLOGÍA |
| CIENCIAS Y ARTES DEL HÁBITAT | ARQUITECTURA<br>ARTES PLÁSTICAS |
| CIENCIAS DE LA EDUCACIÓN | CIENCIAS DE LA EDUCACIÓN<br>EDUCACIÓN PARVULARIA<br>PSICOMOTRICIDAD Y DEPORTES |

| | |
|---|---|
| CIENCIAS AGRÍCOLAS, PECUARIAS Y RECURSOS NATURALES | INGENIERÍA AGRONÓMICA<br>MEDICINA VETERINARIA Y ZOOTECNIA<br>INGENIERÍA EN ZOOTECNIA E INDUSTRIA PECUARIA |
| CIENCIA Y TECNOLOGÍA | INGENIERÍA CIVIL<br>INGENIERÍA DE GAS Y PETROQUÍMICA |

**Fuente:** Elaboración propia.

Cada carrera de la UPEA está bajo el régimen: anual, semestral o mixto.

## 4.2. DIAGNÓSTICO INSTITUCIONAL ENTORNO A LA SEGURIDAD DE LA INFORMACIÓN

La UPEA fue creada mediante Ley 2115 del 5 de septiembre del año 2000 y consigue su autonomía mediante la Ley 2556 del 13 de noviembre del año 2003. Inicialmente inicio sus actividades con 19 carreras, posteriormente se fueron creando más carreras y áreas académicas, así como sub sedes en diferentes lugares. Las finalidades principales de la UPEA son: formar profesionales con una concepción crítica, y desarrollar y difundir ciencia, tecnología y cultura.

En los primeros años de su funcionamiento, la UPEA no tenía sistemas de información propias desarrolladas por lo que el manejo de la información se hacía de forma manual; sin embargo, después de forma paulatina se fue digitalizando la información institucional y actualmente se han desarrollado aplicaciones informáticas y sistemas de información según las necesidades de la institución.

En el desarrollo de las aplicaciones y sistemas de información de información, considerando la seguridad, se han tomado en cuenta los métodos de encriptación para el acceso a la información así como la funcionalidad solicitada por el usuario; pero, esto no asegura la protección total de la información, ante ataques potenciales de hackers, espías corporativos u otros similares, por lo que se debe dar más atención y prioridad a la seguridad de la información que no se tiene, a fin de prevenir y evitar futuros daños que puedan afectar la información de las distintas unidades académicas y/o administrativas, y el normal desenvolvimiento de nuestra casa superior de estudios. Cabe mencionar, que la Unidad de Sistemas de Información y Estadística (SIE), es la unidad especializada que se encarga del desarrollo, implementación y mantenimiento de los sistemas y aplicaciones informáticas de la UPEA, así como también del mantenimiento de redes e intranet, y los equipos computacionales. La unidad SIE ha hecho esfuerzos para dar protección de ataques informáticos provenientes del internet a los servidores, donde se encuentran alojados los sistemas de información y plataformas virtuales, ya que la perdida de la información no solamente puede ocasionar pérdidas económicas; sino que también, la paralización de procesos relevantes y además causaría graves daños al prestigio logrado por la universidad; Sin embargo, la Unidad SIE requiere más personal administrativo especializado en las áreas que tiene para cumplir oportunamente con las solicitudes y atenciones que brinda. Cabe mencionar, que no se cuenta a la fecha con el responsable de seguridad de la información.

## 5. OBJETIVO DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN

Definir las políticas, lineamientos, procedimientos y controles de seguridad de la información, en la Universidad Pública de El Alto, en base a la normativa legal vigente del país para mitigar los niveles de riesgos, y preservar de manera aceptable la confidencialidad, integridad y disponibilidad de la información institucional.

## 6. ALCANCE DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN

El Plan Institucional de Seguridad de la Información de la Universidad Pública de El Alto, es aplicable al interior de sus direcciones, unidades, Áreas y sus Carreras, para poner en ejecución un marco de seguridad de la información adecuado a sus necesidades.

### 6.1. ÁREAS ORGANIZACIONALES DE LA UPEA

Las Áreas Organizacionales involucradas en el proceso de implementación del plan y que integran el conjunto de los procesos esenciales institucionales son:

*NIVELES DE DECISIÓN*:

- Congreso Interno Universitario
- Asamblea General Docente Estudiantil
- Honorable Consejo Universitario
- Honorable Consejo de Área
- Honorable Consejo de Carrera

*DIRECCIONES Y UNIDADES*:

- RECTORADO
  *Nivel de Asesoramiento:*
  - Dirección de Asesoría Jurídica
  - Dirección de Auditoría Interna

  *Nivel Operativo:*
  - Unidad de Transparencia y Lucha Contra la Corrupción
  - Secretaría General
    - Unidad de Títulos y Diplomas
    - Archivo Central
  - Dirección Administrativa Financiera
    - Unidad de Presupuestos
    - Unidad de Contabilidad
    - Unidad de Bienes y Servicios
      - Unidad de Activos Fijos
      - Unidad de Almacenes
    - Unidad de Tesoro Universitario
  - Dirección de Recursos Humanos

        - Unidad de Limpieza y Control Sanitario
        - Unidad de Seguridad y Monitoreo
        - Unidad de Transporte
    - Dirección de Infraestructura
        - Unidad de Telecomunicaciones y Electricidad
    - Unidad de Televisión Universitaria
    - Unidad de Relaciones Públicas
    - Unidad de Radio
    - Unidad de Desarrollo Estratégico y Planificación
    - Unidad de Sistemas de Información y Estadística
    - Unidad de Relaciones Internacionales
    - Unidad del Seguro Social Universitario

- VICERRECTORADO

*Nivel de Asesoramiento*:

- Secretaría Académica

*Nivel Operativo*:

- Dirección de Investigación, Ciencia y Tecnología
- Dirección de Interacción Social, Bienestar Estudiantil
- Dirección de Posgrado
- Unidad de Evaluación y Acreditación.
- Unidad de Registros y Admisiones
- Biblioteca Central
- Decanatos de Áreas, Carreras de la UPEA

## 6.2. UBICACIONES FÍSICAS

La UPEA cuenta con sedes, mismas que para la implementación del PISI se mencionan a continuación:

**CUADRO N° 3**
**SEDES DE LA UPEA**

| N° | SEDE | OBSERVACIÓN |
|---|---|---|
| 1 | VILLA ESPERANZA | SEDE PRINCIPAL |
| 2 | VILLA TEJADA | ---------- |
| 3 | ACHACACHI | ---------- |
| 4 | ANCORAIMES | ---------- |
| 5 | BATALLAS | ---------- |
| 6 | CARANAVI | ---------- |
| 7 | CHAGUAYA | ---------- |
| 8 | COROICO-CRUZ LOMA | ---------- |
| 9 | GUAQUI | ---------- |
| 10 | MAPIRI-CHAROPAMPA | ---------- |
| 11 | PALOS BLANCOS | ---------- |
| 12 | VIACHA | ---------- |

**Fuente:** Elaboración propia.

# 7. DIAGNÓSTICO, PRIORIZACIÓN Y GESTIÓN DE RIESGOS

Para el diagnóstico del PISI, la Unidad de Sistemas de Información y Estadística (SIE) de la Universidad Pública de El Alto - UPEA, tomó en cuenta las vulnerabilidades, amenazas que inciden en la confidencialidad, integridad y disponibilidad de la información para llegar a una evaluación de riesgos; tomando en cuenta las experiencias sobre vulnerabilidades o ataques ocurridos tanto en la unidad SIE como en las otras dependencias administrativas y/o académicas de la UPEA referente a la información. Asimismo, para cada uno de los procesos críticos se identificaron actividades para la valoración de la criticidad acorde a los pilares de seguridad de la información y el tratamiento priorizando los activos críticos y altos, para su debida revisión y elaboración de un plan de contingencia.

## 7.1. GESTIÓN DE RIESGOS

### 7.1.1. SELECCIÓN DEL MÉTODO DE EVALUACIÓN DE RIESGO

Para realizar la evaluación de riesgo de los activos de información de la UPEA, se empleó la Metodología de Análisis y Gestión de Riesgos (MAGERIT), versión 3.0; así como también el estándar la familia ISO 27000 de "Tecnología de la información - Técnicas de Seguridad - Gestión de la seguridad de la información".

## 7.2. INVENTARIO DE ACTIVOS DE INFORMACIÓN

Para la identificación y valoración de los activos de información, relacionados a la Universidad Pública de El Alto - UPEA, se utilizaron como base la propuesta del "Anexo B" del documento "Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del Sector Público" y la Metodología de Análisis y Gestión de Riesgos MAGERIT, versión 3.0.

La identificación de los activos de información se realiza según la siguiente clasificación:

- Datos/información
- Claves criptográficas
- Servicios
- Software – aplicaciones informáticas
- Equipamiento informático (hardware)
- Redes de comunicaciones
- Soportes de información
- Equipamiento auxiliar
- Instalaciones
- Personal

En la elaboración del inventario de los activos de información de la UPEA, se han considerado los siguientes aspectos:

- Activo de información identificado.
- Descripción del activo de información.
- Tipo de activo según clasificación anterior.
- Ubicación física del activo de información.
- Unidad Responsable de gestionar el activo de información.
- Custodio, que es el encargado del custodio y reguardo del activo de información.
- Valoración de los activos de información y nivel de afectación con respecto a las dimensiones de disponibilidad, integridad y confidencialidad.

El ANEXO II (Anexo dos), se muestra el inventario de activos de información de la UPEA, que se efectuó.

### 7.3. EVALUACIÓN DE RIESGOS

A tiempo de realizar el inventario se hicieron la valoración, afín de asegurar los niveles de seguridad de la información (producto de la planificación). Para definir el valor de los activos de información, la escala de valoración es la siguiente:

**CUADRO N° 4**
**ESCALA DE VALORACIÓN DE LA CRITICIDAD**

| Escala de Valoración | |
|---|---|
| **1** | **Muy Bajo** |
| **2** | **Bajo** |
| **3** | **Medio** |
| **4** | **Alto** |
| **5** | **Muy Alto** |

**Fuente:** Anexo B 6.2 del documento “Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del Sector Público” (p. 93).

Partiendo del análisis en base a las posibles consecuencias que puede ocurrir si el activo de información pierda su confidencialidad, integridad y/o disponibilidad, se han valorado estas dimensiones de seguridad, considerando los siguientes criterios empleados y descritos en el Anexo B punto 6.2 del documento “Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del Sector Público”, elaborado por la CTIC-EPB y CGII:

- **Disponibilidad:** ¿Qué importancia tendría que el activo no estuviera disponible?
- **Integridad:** ¿Qué importancia tendría que la información aso ciada al activo fuera modificada sin control?
- **Confidencialidad:** ¿Qué importancia tendría que la información asociada al activo fuera conocida por personas no autorizadas?

**CUADRO N° 5**
**CRITERIO DE VALORACIÓN DE LA DIMENSIÓN "DISPONIBILIDAD"**

| DISPONIBILIDAD | | | |
|---|---|---|---|
| **VALOR DE CRITICIDAD** | **NIVEL DE CRITICIDAD** | **CLASIFICACIÓN** | **DESCRIPCIÓN** |
| 1 | Muy Bajo | Disponibilidad Muy Baja | La falla del activo de información, no incide en la consecución de objetivos y/o pérdida de niveles de servicios de procesos críticos del negocio. |
| 2 | Bajo | Disponibilidad Baja | La falla del activo de información, no incide en la consecución de objetivos y/o pérdida de niveles de servicio de procesos críticos de la institución, es considerada marginal. |
| 3 | Medio | Disponibilidad Media | La falla del activo de información, afecta a la consecución de objetivos y/o tiene incidencia en la pérdida de niveles de servicios de un proceso crítico. |
| 4 | Alto | Disponibilidad Alta | La falla del activo de información, tiene el potencial de interrumpir el negocio. |
| 5 | Muy Alto | Disponibilidad Muy Alta | La falla del activo de información, tiene el potencial de interrumpir el negocio o afectar gravemente a los niveles de servicios prestados por procesos críticos del negocio. |

**Fuente:** Elaboración Propia considerando los criterios Magerit versión 3.0

**CUADRO N° 6**
**CRITERIO DE VALORACIÓN DE LA DIMENSIÓN "INTEGRIDAD"**

| INTEGRIDAD | | | |
|---|---|---|---|
| **VALOR DE CRITICIDAD** | **NIVEL DE CRITICIDAD** | **CLASIFICACIÓN** | **DESCRIPCIÓN** |
| 1 | Muy Bajo | Integridad Muy Baja | El daño o modificación no autorizada del activo de información no es crítico y su impacto es insignificante. |
| 2 | Bajo | Integridad Baja | El daño o modificación no autorizada del activo de información no es crítico para para las aplicaciones del negocio y su impacto es menor. |
| 3 | Medio | Integridad Media | El daño o modificación no autorizada del activo de información es crítico para las aplicaciones del negocio, y su impacto es moderado. |
| 4 | Alto | Integridad Alta | El daño o modificación no autorizada del activo de información, es crítico afectando a las principales operaciones del negocio, y su impacto es grave. |
| 5 | Muy Alto | Integridad Muy Alta | El daño o modificación no autorizada del activo de información, es crítico afectando a las principales operaciones del negocio, y su impacto es muy grave, afectando seriamente los procesos de la institución, lo que puede afectar la imagen de la entidad. |

**Fuente:** Elaboración Propia considerando los criterios Magerit versión 3.0

**CUADRO N° 7**
**CRITERIO DE VALORACIÓN DE LA DIMENSIÓN "CONFIDENCIALIDAD"**

| CONFIDENCIALIDAD | | | |
|---|---|---|---|
| **VALOR DE CRITICIDAD** | **NIVEL DE CRITICIDAD** | **CLASIFICACIÓN** | **DESCRIPCIÓN** |
| 1 | Muy Bajo | Confidencialidad Muy Baja | Información pública, aplicaciones o instalaciones a disposición del público, que no supone algún riesgo para la entidad. |
| 2 | Bajo | Confidencialidad Baja | Información pública, aplicaciones o instalaciones a disposición del público, cuyo riesgo es insignificante para la entidad. |
| 3 | Medio | Confidencialidad Media | Información, sistemas, aplicaciones o instalaciones se restringe exclusivamente para el uso interno. En caso contrario, el riesgo o daño seria crítico. |
| 4 | Alto | Confidencialidad Alta | Información restringida por razones de interés público. En caso contrario el riesgo es grave. |
| 5 | Muy Alto | Confidencialidad Muy Alta | La información es sensible y debe estar clasificada, misma que debe ser resguardada contra cualquier posible filtración. En caso contrario, el riesgo es muy grave. |

**Fuente:** Elaboración Propia considerando los criterios Magerit versión 3.0

En los cuadros anteriores de criterios de valoración de las dimensiones de seguridad de la información se menciona la palabra "negocio" bajo el significado informático como "proceso o flujo interno de trabajo de una entidad que permite la circulación de información".

Cabe mencionar, una vez realizado el inventario de activos de información se hizo la valoración de dichos activos; que se muestra en el ANEXO III (Anexo tres) de este documento.

### 7.3.1. CRITERIOS DE EVALUACIÓN DEL RIESGO

Las vulnerabilidades son debilidades que presenta el activo de información por sí mismas no pueden ocasionar daños en los mismos ya que necesitan de amenazas que las exploten; asimismo, las amenazas pueden ser internas (que por lo general son de más alto riesgo) o externas; además, es necesario que sean debidamente identificadas en caso de que suceda algún cambio que implique la aparición de una nueva amenaza. Identificadas las vulnerabilidades y amenazas, se han identificado los riesgos en base a: nivel de riesgo que cada amenaza conlleva, probabilidad de que ocurra el incidente (amenaza que explota la vulnerabilidad), magnitud del impacto producido por el evento al activo.

Para la identificación, análisis y evaluación de riesgos se tomó en cuenta el catálogo de amenazas según MAGERIT 3.0, que está en el ANEXO I (Anexo uno) del presente plan.

La escala de valoración del riesgo que se ha utilizado es la siguiente:

**CUADRO N° 8**
**VALORACIÓN CUALITATIVA**

| ESCALAS | |
|---|---|
| **Probabilidad** | **Impacto** |
| Cierta/Inminente | Crítico |
| Muy Probable | Severo |
| Probable | Moderado |
| Poco Probable | Menor |
| Improbable | Irrelevante |

**Fuente:** Anexo B del documento "Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del Sector Público" (p. 103).

Las amenazas y vulnerabilidades identificadas son:

**CUADRO N° 8**
**VALORACIÓN CUALITATIVA**

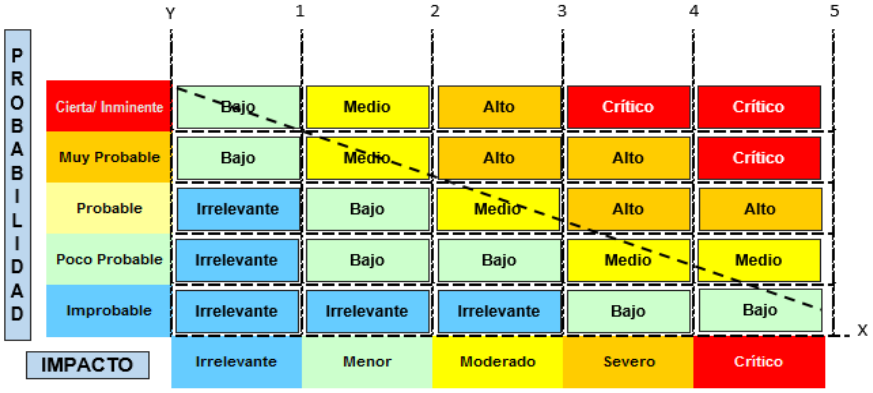
| N° | ORIGEN DE LA AMENAZA | AMENAZA | TIPOS DE ACTIVOS AFECTADOS | Degradación del activo | | |
|---|---|---|---|---|---|---|
| | | | | Disponibilidad | Integridad | Confidencialidad |
| 1 | De origen industrial | Avería de origen físico o lógico. | ➢ Servidores<br>➢ Equipamiento auxiliar del Data Center<br>➢ Equipo de Computación | x | | |
| 2 | De origen industrial | Corte de suministro eléctrico. | ➢ [RC1] Internet<br>➢ Equipo de Computación | x | | |
| 3 | De origen industrial | Condiciones inadecuadas de temperatura o humedad. | Equipo de Computación | x | | |
| 4 | De origen industrial | Degradación de los soportes de almacenamiento de la información. | Equipo de Computación | x | | |
| 5 | De origen industrial | Fallo de servicios de comunicaciones. | Red de Telecomunicaciones | x | | |
| 6 | Errores y fallos no intencionados | Errores de los usuarios. | ➢ [SA15] Sistema de información académica de departamento de idiomas (SI@DI)<br>➢ [SA17] Sistema de preuniversitario<br>➢ Sistemas de Información | x | x | x |

| | | | | | | |
|---|---|---|---|---|---|---|
| 7 | Errores y fallos no intencionados | Deficiencias en la organización, en algunos casos la atención de solicitudes de certificaciones, historiales, legalizaciones, entre otros similares no son atendidas por el orden secuencial de presentación. | Sistemas de Información | x | | |
| 8 | Errores y fallos no intencionados | Difusión de software dañino. | Equipo de Computación | x | x | x |
| 9 | Ataques intencionados | Modificación deliberada de la información; sin autorización escrita. | Sistemas de Información | | x | |
| 10 | Ataques intencionados | Destrucción de la información, de respaldo, que puede darse por criterio inapropiado o falta de conciencia de la seguridad de la información. | Sistemas de Información | x | | |

**Fuente:** Elaboración Propia tomando en cuenta el Catálogo de Amenazas de Magerit versión 3.0

De acuerdo a los niveles de riesgos identificados, en función de la probabilidad y el impacto, la matriz para valorar el riesgo se muestra a continuación.

**Figura 1: Matriz Para Valorar el Riesgo**




**Fuente:** Anexo B del documento "Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del Sector Público" (p. 104).

De la matriz para valorar el Riesgo, los niveles de riesgo establecidos son: Irrelevante, Bajo, Medio, Alto y Crítico. En la identificación, análisis y valoración de riesgos, los que presentan niveles de riesgo "Crítico" (color rojo) o "Alto" (color naranja), deberán ser tratados para minimizar su impacto; mientras que, los niveles de riesgo: "Medio", "Bajo" e "Irrelevante" no serán tratados.

En el ANEXO IV (Anexo cuatro), se muestra la matriz de identificación, análisis y valoración de riesgos; en la cual se han identificado las vulnerabilidades y amenazas críticas que en caso de materializarse causarían daños; asimismo, como resultado de la

valoración de riesgos se han identificado dos procesos con niveles de riesgos críticos y un proceso con nivel de riesgo Alto; que pueden llegar a tener interrupción y afectar los servicios que brinda la institución por lo que deberán ser tratados prioritariamente.

### 7.4. TRATAMIENTO DEL RIESGO

Una vez identificados y evaluados los riesgos, se debe realizar el tratamiento del riesgo que implica tomar decisiones respectivas, de acuerdo a las siguientes categorías de acción, que se mencionan a continuación.

**Aceptar el riesgo:** Significa estar conscientes de la afectación que se produzca en caso de materializarse la amenaza o vulnerabilidad; para esto se deberían disponer de recursos ante una eventualidad. En el marco de la aceptación del riesgo, los que no sean considerados relevantes podrán ser excluidos de la selección de controles, pero se deberá incluir una justificación para no tratarlos.

**Reducir el riesgo:** Implica realizar una selección de Controles de Seguridad de la Información o bien se pueden diseñar nuevos controles para cumplir con necesidades específicas que coadyuven a la reducción del riesgo.

**Retener el riesgo:** Implica establecer criterios para su aceptación, no es necesario implementar o seleccionar controles adicionales si el riesgo puede ser retenido.

**Evitar el riesgo:** El riesgo puede evitarse cuando este se considera muy alto, o Si los costos para implementar otras opciones de tratamiento del riesgo exceden los beneficios. Se puede tomar una decisión que logre evitar par completo el riesgo, mediante el retiro de una actividad, condiciones o conjunto de actividades ya sean planificadas o existentes. Esto deberá estar debidamente justificado y documentado.

**Transferir el riesgo:** Deben evaluarse las opciones y tomar las acciones pertinentes para ejecutar la escogida, en función del valor del activo y del coste de realizar esta transferencia (no sólo coste económico sino también los riesgos que conlleva esta transferencia en cuanto a la inclusión de un tercero).

### 7.5. CONTROLES IMPLEMENTADOS Y POR IMPLEMENTAR

Los controles implementados y por implementar producto del PISI, se mencionan en el Anexo A del documento “Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del Sector Público”. La matriz que se muestra en el “ANEXO IV: IDENTIFICACIÓN, ANÁLISIS Y VALORACIÓN DE RIESGOS”, permite que posteriormente se determinen los controles (salvaguardas) que se requieran implementar, para reducir el impacto o la probabilidad de los riesgos críticos y riesgo alto encontrados.

Las valoraciones finales de activos de información y riesgos, se obtienen de las fórmulas:

VAI = Valoración de Activo de Información = (Disponibilidad + Integridad + Confidencialidad)
VR = Valoración de Riesgo= (Disponibilidad + Integridad + Confidencialidad) / 3

Por tanto:

**CUADRO N° 9**
**VALORACIÓN DE CRITICIDAD**

| VALORACIÓN | | |
|---|---|---|
| **VAI** | **VR** | **NIVEL DE CRITICIDAD** |
| **[1-3]** | **1** | **Muy Bajo** |
| **[4-6]** | **2** | **Bajo** |
| **[7-9]** | **3** | **Medio** |
| **[10-12]** | **4** | **Alto** |
| **[13-15]** | **5** | **Muy Alto** |

**Fuente:** Elaboración Propia.

La valoración de la probabilidad y el impacto vienen dadas por la siguiente tabla:

**CUADRO N° 10**
**CRITERIOS DE VALORACIÓN DE RIESGO**

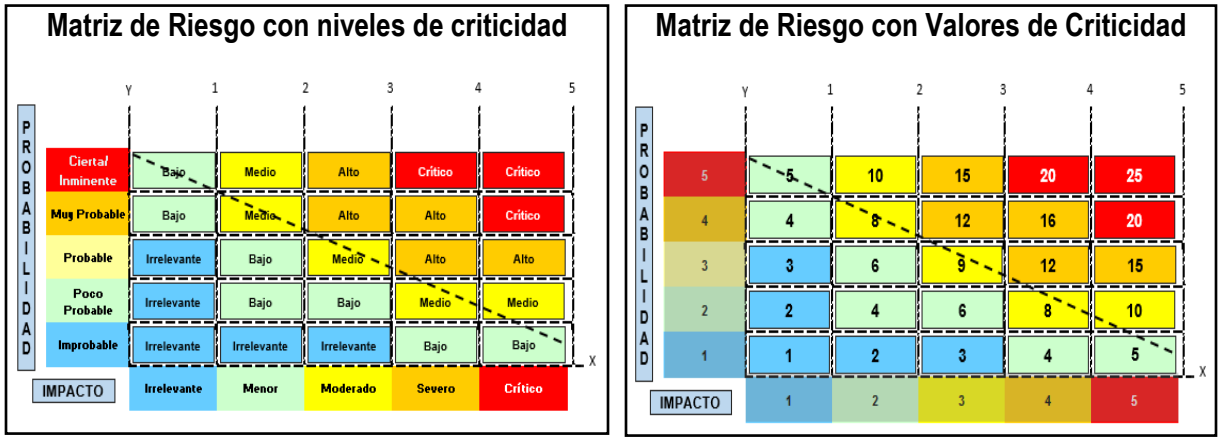
| PROBABILIDAD | IMPACTO | VALOR |
|---|---|---|
| Cierta/Inminente | Crítico | 5 |
| Muy Probable | Severo | 4 |
| Probable | Moderado | 3 |
| Poco Probable | Menor | 2 |
| Improbable | Irrelevante | 1 |

**Fuente:** Elaboración Propia.

Para calcular el riesgo, una vez identificados los valores de probabilidad e impacto, se utiliza la siguiente ecuación matemática: Riesgo = (Probabilidad) x (Impacto)

Cuyo valor se identifica de acuerdo a las siguientes matrices:

**Figura 2: Matrices para Valorar el Riesgo**




**Fuente:** Elaboración Propia considerando los criterios del documento "Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del Sector Público".

En el siguiente cuadro se resume los resultados de la valoración de riesgos.

**CUADRO N° 11**
**RESULTADOS DE VALORACIÓN DE RIESGO**

| NIVEL DE CRITICIDAD | VALOR DE CRITICIDAD | SIGNIFICADO |
|---|---|---|
| IRRELEVANTE | [1-3] | Riesgo Irrelevante |
| MENOR | [4-6] | Riesgo Menor |
| MODERADO | [8-10] | Riesgo Moderado |
| SEVERO | [12-16] | Riesgo Severo |
| CRÍTICO | [20-25] | Riesgo Crítico |

**Fuente:** Elaboración Propia.

Los valores de criticidad permitirán posteriormente hacer cálculos para el análisis de riesgo que se requiera.

## 8. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

En la actualidad la UPEA tiene el “Manual de Políticas y Procedimientos de Seguridad de la Información” aprobado mediante Resolución Nro. 148-A/2021 del HCU, en dónde si bien se mencionan las políticas de seguridad de la información y en qué consisten las mismas, no están determinadas las guías de procedimientos de cada política. Asimismo, a partir de la identificación, análisis y valoración de riesgos realizados; se deberán determinar las políticas de seguridad que se requieren implementar afín de proteger la información de la institución.

## 9. CRONOGRAMA DE IMPLEMENTACIÓN

**CUADRO N° 12**
**RESULTADOS DE VALORACIÓN DE RIESGO**

| N° | ACTIVIDAD | RESPONSABLE(S) DE LA ACTIVIDAD | FECHA ESTIMADA DE IMPLEMENTACIÓN |
|---|---|---|---|
| 1 | Designación del Responsable de Seguridad de la Información | MAE | 2023-2024 |
| 2 | Conformación del Comité de Seguridad de la Información | MAE | 2023-2024 |
| 3 | Revisiones, correcciones y/o modificaciones de la propuesta de PISI de la UPEA | RSI, CSI | 2025 |
| 4 | Aprobación del PISI de la UPEA | CSI | 2025 |

**Fuente:** Elaboración Propia.

# ANEXOS

## ANEXO I: CATÁLOGO DE AMENAZAS SEGÚN MAGERIT VERSIÓN 3.0

**Tabla Nº 3.** Catálogo de Amenazas (MAGERIT)

| Amenaza | Degradación del activo | | | DESCRIPCIÓN DE MAGERIT VERSIÓN 3.0 |
|---|---|---|---|---|
| | Disponibilidad | Integridad | Confidencialidad | |
| **Desastres Naturales** | | | | |
| Fuego (Incedios) | x | | | **[N.1] Fuego**<br>**Tipos de activos:**<br>• [HW] equipos informáticos (hardware)<br>• [Media] soportes de información<br>• [AUX] equipamiento auxiliar<br>• [L] instalaciones<br>**Dimensiones:**<br>1. [D] disponibilidad<br>**Descripción:**<br>incendios: posibilidad de que el fuego acabe con recursos del sistema.<br>**Ver:**<br>EBIOS: 01- INCENDIO |
| Daños por agua (Inundaciones) | x | | | **[N.2] Daños por agua**<br>**Tipos de activos:**<br>• [HW] equipos informáticos (hardware)<br>• [Media] soportes de información<br>• [AUX] equipamiento auxiliar<br>• [L] instalaciones<br>**Dimensiones:**<br>1. [D] disponibilidad<br>**Descripción:**<br>inundaciones: posibilidad de que el agua acabe con recursos del sistema.<br>**Ver:**<br>EBIOS: 02 - PERJUICIOS OCASIONADOS POR EL AGUA |
| Desastres Naturales | x | | | **[N.*] Desastres naturales**<br>**Tipos de activos:**<br>• [HW] equipos informáticos (hardware)<br>• [Media] soportes de información<br>• [AUX] equipamiento auxiliar<br>• [L] instalaciones<br>**Dimensiones:**<br>1. [D] disponibilidad<br>**Descripción:**<br>otros incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras, ...<br>Se excluyen desastres específicos tales como incendios (ver [N.1]) e inundaciones (ver [N.2]).<br>Se excluye al personal por cuanto se ha previsto una amenaza específica [E.31] para cubrir la indisponibilidad involuntaria del personal sin entrar en sus causas.<br>**Ver:**<br>EBIOS:<br>03 – CONTAMINACIÓN<br>04 - SINIESTRO MAYOR<br>06 - FENÓMENO CLIMÁTICO<br>07 - FENÓMENO SÍSMICO<br>08 - FENÓMENO DE ORIGEN VOLCÁNICO<br>09 - FENÓMENO METEOROLÓGICO<br>10 - INUNDACIÓN |

| De origen industrial | | | | |
|---|---|---|---|---|
| Fuego (Incendios) | x | | | **[I.1] Fuego**<br>**Tipos de activos:**<br>• [HW] equipos informáticos (hardware)<br>• [Media] soportes de información<br>• [AUX] equipamiento auxiliar<br>• [L] instalaciones<br>**Dimensiones:**<br>1. [D] disponibilidad<br>**Descripción:**<br>incendio: posibilidad de que el fuego acabe con los recursos del sistema.<br>**Origen:**<br>Entorno (accidental)<br>Humano (accidental o deliberado)<br>**Ver:**<br>EBIOS: 01- INCENDIO |
| Daños por agua (Inundaciones) | x | | | **[I.2] Daños por agua**<br>**Tipos de activos:**<br>• [HW] equipos informáticos (hardware)<br>• [Media] soportes de información<br>• [AUX] equipamiento auxiliar<br>• [L] instalaciones<br>**Dimensiones:**<br>1. [D] disponibilidad<br>**Descripción:**<br>escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.<br>**Origen:**<br>Entorno (accidental)<br>Humano (accidental o deliberado)<br>**Ver:**<br>EBIOS: 02 - PERJUICIOS OCASIONADOS POR EL AGUA |
| Desastres industriales | x | | | **[I.*] Desastres industriales**<br>**Tipos de activos:**<br>• [HW] equipos informáticos (hardware)<br>• [Media] soportes de información<br>• [AUX] equipamiento auxiliar<br>• [L] instalaciones<br>**Dimensiones:**<br>1. [D] disponibilidad<br>**Descripción:**<br>otros desastres debidos a la actividad humana: explosiones, derrumbes, ...<br>contaminación química, ...<br>sobrecarga eléctrica, fluctuaciones eléctricas, ...<br>accidentes de tráfico, ...<br>Se excluyen amenazas específicas como incendio (ver [I.1]) e inundación (ver [I.2]).<br>Se excluye al personal por cuanto se ha previsto una amenaza específica, [E.31], para cubrir la indisponibilidad involuntaria del personal sin entrar en sus causas.<br>**Origen:**<br>Entorno (accidental)<br>Humano (accidental o deliberado)<br>**Ver:**<br>EBIOS: 04 - SINIESTRO MAYOR |
| Contaminación mecánica | x | | | **[I.3] Contaminación mecánica**<br>**Tipos de activos:**<br>• [HW] equipos informáticos (hardware)<br>• [Media] soportes de información<br>• [AUX] equipamiento auxiliar<br>**Dimensiones:**<br>1. [D] disponibilidad<br>**Descripción:**<br>vibraciones, polvo, suciedad, ...<br>**Origen:**<br>Entorno (accidental)<br>Humano (accidental o deliberado)<br>**Ver:**<br>EBIOS: 03 – CONTAMINACIÓN |

| | | | | |
|---|---|---|---|---|
| Contaminación electromagnética | x | | | **[I.4] Contaminación electromagnética**<br>**Tipos de activos:**<br>• [HW] equipos informáticos (hardware)<br>• [Media] soportes de información (electrónicos)<br>• [AUX] equipamiento auxiliar<br>**Dimensiones:**<br>1. [D] disponibilidad<br>**Descripción:**<br>interferencias de radio, campos magnéticos, luz ultravioleta, ...<br>**Origen:**<br>Entorno (accidental)<br>Humano (accidental o deliberado)<br>**Ver:**<br>EBIOS:<br>14 - EMISIONES ELECTROMAGNÉTICAS<br>15- RADIACIONES TÉRMICAS<br>16 - IMPULSOS ELECTROMAGNÉTICOS |
| Avería de origen físico o lógico | x | | | **[I.5] Avería de origen físico o lógico**<br>**Tipos de activos:**<br>• [SW] aplicaciones (software)<br>• [HW] equipos informáticos (hardware)<br>• [Media] soportes de información<br>• [AUX] equipamiento auxiliar<br>**Dimensiones:**<br>1. [D] disponibilidad<br>**Descripción:**<br>fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.<br>En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.<br>**Origen:**<br>Entorno (accidental)<br>Humano (accidental o deliberado)<br>**Ver:**<br>EBIOS:<br>28 - AVERÍA DEL HARDWARE<br>29 - FALLA DE FUNCIONAMIENTO DEL HARDWARE |
| Corte del suministro eléctrico | x | | | **[I.6] Corte del suministro eléctrico**<br>**Tipos de activos:**<br>• [HW] equipos informáticos (hardware)<br>• [Media] soportes de información (electrónicos)<br>• [AUX] equipamiento auxiliar<br>**Dimensiones:**<br>1. [D] disponibilidad<br>**Descripción:**<br>cese de la alimentación de potencia<br>**Origen:**<br>Entorno (accidental)<br>Humano (accidental o deliberado)<br>**Ver:**<br>EBIOS: 12 - PÉRDIDA DE SUMINISTRO DE ENERGÍA |
| Condiciones inadecuadas de temperatura o humedad | x | | | **[I.7] Condiciones inadecuadas de temperatura y/o humedad**<br>**Tipos de activos:**<br>• [HW] equipos informáticos (hardware)<br>• [Media] soportes de información<br>• [AUX] equipamiento auxiliar<br>**Dimensiones:**<br>1. [D] disponibilidad<br>**Descripción:**<br>deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad, ...<br>**Origen:**<br>Entorno (accidental)<br>Humano (accidental o deliberado)<br>**Ver:**<br>EBIOS: 11- FALLAS EN LA CLIMATIZACIÓN |
| Fallo de servicios de comunicaciones | x | | | **[I.8] Fallo de servicios de comunicaciones**<br>**Tipos de activos:**<br>• [COM] redes de comunicaciones<br>**Dimensiones:**<br>1. [D] disponibilidad<br>**Descripción:**<br>cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente.<br>**Origen:**<br>Entorno (accidental)<br>Humano (accidental o deliberado)<br>**Ver:**<br>EBIOS: 13 - PÉRDIDA DE LOS MEDIOS DE TELECOMUNICACIÓN |

| | | | | |
|---|---|---|---|---|
| Interrupción de otros servicios y suministros esenciales | x | | | **[I.9] Interrupción de otros servicios y suministros esenciales**<br>**Tipos de activos:** • [AUX] equipamiento auxiliar<br>**Dimensiones:** 1. [D] disponibilidad<br>**Descripción:** otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, toner, refrigerante, ...<br>**Origen:** Entorno (accidental); Humano (accidental o deliberado)<br>**Ver:** EBIOS: no disponible |
| Degradación de los soportes de almacenamiento de la información | x | | | **[I.10] Degradación de los soportes de almacenamiento de la información**<br>**Tipos de activos:** • [Media] soportes de información<br>**Dimensiones:** 1. [D] disponibilidad<br>**Descripción:** como consecuencia del paso del tiempo<br>**Origen:** Entorno (accidental); Humano (accidental o deliberado)<br>**Ver:** EBIOS: 28 - AVERÍA DEL HARDWARE; 29 - FALLA DE FUNCIONAMIENTO DEL HARDWARE |
| Emanaciones electromagnéticas | | | x | **[I.11] Emanaciones electromagnéticas**<br>**Tipos de activos:** • [HW] equipos informáticos (hardware) • [Media] media • [AUX] equipamiento auxiliar • [L] instalaciones<br>**Dimensiones:** 1. [C] confidencialidad<br>**Descripción:** hecho de poner vía radio datos internos a disposición de terceros. Es una amenaza donde el emisor es víctima pasiva del ataque. Prácticamente todos los dispositivos electrónicos emiten radiaciones al exterior que pudieran ser interceptadas por otros equipos (receptores de radio) derivándose una fuga de información. Esta amenaza se denomina, incorrecta pero frecuentemente, ataque TEMPEST (del inglés *"Transient Electromagnetic Pulse Standard"*). Abusando del significado primigenio, es frecuente oír hablar de que un equipo disfruta de "*TEMPEST protection*", queriendo decir que se ha diseñado para que no emita, electromagnéticamente, nada de interés por si alguien lo captara. No se contempla en esta amenaza la emisión por necesidades del medio de comunicación: redes inalámbricas, enlaces de microondas, etc. que estarán amenazadas de interceptación.<br>**Origen:** Entorno (accidental); Humano (accidental o deliberado)<br>**Ver:** EBIOS: 17 - INTERCEPTACIÓN DE SEÑALES PARÁSITAS COMPROMETEDORAS |
| **Errores y fallos no intencionados** | | | | |
| Errores de los usuarios | x | x | x | **[E.1] Errores de los usuarios**<br>**Tipos de activos:** • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [Media] soportes de información<br>**Dimensiones:** 1. [I] integridad 2. [C] confidencialidad 3. [D] disponibilidad<br>**Descripción:** equivocaciones de las personas cuando usan los servicios, datos, etc.<br>**Ver:** EBIOS: 38 - ERROR DE USO |
| Errores del administrador | x | x | x | **[E.2] Errores del administrador**<br>**Tipos de activos:** • [D] datos / información • [keys] claves criptográficas • [S] servicios • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [Media] soportes de información<br>**Dimensiones:** 1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad<br>**Descripción:** equivocaciones de personas con responsabilidades de instalación y operación<br>**Ver:** EBIOS: 38 - ERROR DE USO |

| | | | | |
|---|---|---|---|---|
| Errores de monitorización (log) | | x | | **[E.3] Errores de monitorización *(log)***<br>**Tipos de activos:** • [D.log] registros de actividad<br>**Dimensiones:** 1. [I] integridad (trazabilidad)<br>**Descripción:** inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos, ...<br>**Ver:** EBIOS: no disponible |
| Errores de configuración | | x | | **[E.4] Errores de configuración**<br>**Tipos de activos:** • [D.conf] datos de configuración<br>**Dimensiones:** 1. [I] integridad<br>**Descripción:** introducción de datos de configuración erróneos.<br>Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.<br>**Ver:** EBIOS: no disponible |
| Deficiencias en la organización | x | | | **[E.7] Deficiencias en la organización**<br>**Tipos de activos:** • [P] personal<br>**Dimensiones:** 1. [D] disponibilidad<br>**Descripción:** cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión.<br>Acciones descoordinadas, errores por omisión, etc.<br>**Ver:** EBIOS: no disponible |
| Difusión de software dañino | x | x | x | **[E.8] Difusión de software dañino**<br>**Tipos de activos:** • [SW] aplicaciones (software)<br>**Dimensiones:** 1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad<br>**Descripción:** propagación inocente de virus, espías *(spyware)*, gusanos, troyanos, bombas lógicas, etc.<br>**Ver:** EBIOS: no disponible |
| Errores de [re-]encaminamiento | | | x | **[E.9] Errores de [re-]encaminamiento**<br>**Tipos de activos:** • [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones<br>**Dimensiones:** 1. [C] confidencialidad<br>**Descripción:** envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros.<br>Es particularmente destacable el caso de que el error de encaminamiento suponga un error de entrega, acabando la información en manos de quien no se espera.<br>**Ver:** EBIOS: no disponible |
| Errores de secuencia | | x | | **[E.10] Errores de secuencia**<br>**Tipos de activos:** • [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones<br>**Dimensiones:** 1. [I] integridad<br>**Descripción:** alteración accidental del orden de los mensajes transmitidos.<br>**Ver:** EBIOS: no disponible |
| Escapes de información | | | x | **[E.14] Escapes de información**<br>**Tipos de activos:** •<br>**Dimensiones:** 1. [C] confidencialidad<br>**Descripción:** la información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada. |

<table>
<tr><td>Alteración accidental de la información</td><td></td><td>x</td><td></td><td>
[E.15] Alteración accidental de la información<br>
Tipos de activos:<br>• [D] datos / información<br>• [keys] claves criptográficas<br>• [S] servicios<br>• [SW] aplicaciones (SW)<br>• [COM] comunicaciones (tránsito)<br>• [Media] soportes de información<br>• [L] instalaciones<br>
Dimensiones:<br>1. [I] integridad<br>
Descripción:<br>alteración accidental de la información.<br>Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.<br>
Ver:<br>EBIOS: no disponible
</td></tr>
<tr><td>Destrucción de información</td><td>x</td><td></td><td></td><td>
[E.18] Destrucción de información<br>
Tipos de activos:<br>• [D] datos / información<br>• [keys] claves criptográficas<br>• [S] servicios<br>• [SW] aplicaciones (SW)<br>• [COM] comunicaciones (tránsito)<br>• [Media] soportes de información<br>• [L] instalaciones<br>
Dimensiones:<br>1. [D] disponibilidad<br>
Descripción:<br>pérdida accidental de información.<br>Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.<br>
Ver:<br>EBIOS: no disponible
</td></tr>
<tr><td>Fugas de información</td><td></td><td></td><td>x</td><td>
[E.19] Fugas de información<br>
Tipos de activos:<br>• [D] datos / información<br>• [keys] claves criptográficas<br>• [S] servicios<br>• [SW] aplicaciones (SW)<br>• [COM] comunicaciones (tránsito)<br>• [Media] soportes de información<br>• [L] instalaciones<br>• [P] personal (revelación)<br>
Dimensiones:<br>1. [C] confidencialidad<br>
Descripción:<br>revelación por indiscreción.<br>Incontinencia verbal, medios electrónicos, soporte papel, etc.<br>
Ver:<br>EBIOS: no disponible
</td></tr>
<tr><td>Vulnerabilidades de los programas (software)</td><td>x</td><td>x</td><td>x</td><td>
[E.20] Vulnerabilidades de los programas (software)<br>
Tipos de activos:<br>• [SW] aplicaciones (software)<br>
Dimensiones:<br>1. [I] integridad<br>2. [D] disponibilidad<br>3. [C] confidencialidad<br>
Descripción:<br>defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.<br>
Ver:<br>EBIOS: no disponible
</td></tr>
<tr><td>Errores de mantenimiento / actualización de programas (software)</td><td>x</td><td>x</td><td></td><td>
[E.21] Errores de mantenimiento / actualización de programas (software)<br>
Tipos de activos:<br>• [SW] aplicaciones (software)<br>
Dimensiones:<br>1. [I] integridad<br>2. [D] disponibilidad<br>
Descripción:<br>defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.<br>
Ver:<br>EBIOS:<br>31 - FALLA DE FUNCIONAMIENTO DEL SOFTWARE<br>32 - PERJUICIO A LA MANTENIBILIDAD DEL SISTEMA DE INFORMACIÓN
</td></tr>
</table>

| | | | | |
|---|---|---|---|---|
| Errores de mantenimiento / actualización de equipos (hardware) | x | | | **[E.23] Errores de mantenimiento / actualización de equipos (hardware)**<br>**Tipos de activos:**<br>• [HW] equipos informáticos (hardware)<br>• [Media] soportes electrónicos<br>• [AUX] equipamiento auxiliar<br>**Dimensiones:**<br>1. [D] disponibilidad<br>**Descripción:**<br>defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.<br>**Ver:**<br>EBIOS: 32 - PERJUICIO A LA MANTENIBILIDAD DEL SISTEMA DE INFORMACIÓN |
| Caída del sistema por agotamiento de recursos | x | | | **[E.24] Caída del sistema por agotamiento de recursos**<br>**Tipos de activos:**<br>• [S] servicios<br>• [HW] equipos informáticos (hardware)<br>• [COM] redes de comunicaciones<br>**Dimensiones:**<br>1. [D] disponibilidad<br>**Descripción:**<br>la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.<br>**Ver:**<br>EBIOS: 30 - SATURACIÓN DEL SISTEMA INFORMÁTICO |
| Pérdida de equipos | x | | x | **[E.25] Robo**<br>**Tipos de activos:**<br>• [HW] equipos informáticos (hardware)<br>• [Media] soportes de información<br>• [AUX] equipamiento auxiliar<br>**Dimensiones:**<br>1. [D] disponibilidad<br>2. [C] confidencialidad<br>**Descripción:**<br>la pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad.<br>Se puede perder todo tipo de equipamiento, siendo la pérdida de equipos y soportes de información los más habituales.<br>En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.<br>**Ver:**<br>EBIOS: 22 - RECUPERACIÓN DE SOPORTES RECICLADOS O DESECHADOS |
| Indisponibilidad del personal | x | | | **[E.28] Indisponibilidad del personal**<br>**Tipos de activos:**<br>• [P] personal interno<br>**Dimensiones:**<br>1. [D] disponibilidad<br>**Descripción:**<br>ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica, ...<br>**Ver:**<br>EBIOS: 42 - DAÑO A LA DISPONIBILIDAD DEL PERSONAL |
| **Ataques intencionados** | | | | |
| Manipulación de los registros de actividad (log) | | x | | **[A.4] Manipulación de los registros de actividad (log)**<br>**Tipos de activos:**<br>• [D.log] registros de actividad<br>**Dimensiones:**<br>1. [I] integridad (trazabilidad)<br>**Descripción:**<br>**Ver:**<br>EBIOS: no disponible |
| Manipulación de la configuración | x | x | x | **[A.4] Manipulación de la configuración**<br>**Tipos de activos:**<br>• [D.log] registros de actividad<br>**Dimensiones:**<br>1. [I] integridad<br>2. [C] confidencialidad<br>3. [A] disponibilidad<br>**Descripción:**<br>prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.<br>**Ver:**<br>EBIOS: no disponible |

| | | | | |
|---|---|---|---|---|
| Suplantación de la identidad del usuario | x | x | x | **[A.5] Suplantación de la identidad del usuario**<br>**Tipos de activos:**<br>• [D] datos / información<br>• [keys] claves criptográficas<br>• [S] servicios<br>• [SW] aplicaciones (software)<br>• [COM] redes de comunicaciones<br>**Dimensiones:**<br>1. [C] confidencialidad<br>2. [A] autenticidad<br>3. [I] integridad<br>**Descripción:**<br>cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios.<br>Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente.<br>**Ver:**<br>EBIOS: 40 - USURPACIÓN DE DERECHO |
| Abuso de privilegios de acceso | x | x | x | **[A.6] Abuso de privilegios de acceso**<br>**Tipos de activos:**<br>• [D] datos / información<br>• [keys] claves criptográficas<br>• [S] servicios<br>• [SW] aplicaciones (software)<br>• [HW] equipos informáticos (hardware)<br>• [COM] redes de comunicaciones<br>**Dimensiones:**<br>1. [C] confidencialidad<br>2. [I] integridad<br>3. [D] disponibilidad<br>**Descripción:**<br>cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.<br>**Ver:**<br>EBIOS: 39 - ABUSO DE DERECHO |
| Uso no previsto | x | x | x | **[A.7] Uso no previsto**<br>**Tipos de activos:**<br>• [S] servicios<br>• [SW] aplicaciones (software)<br>• [HW] equipos informáticos (hardware)<br>• [COM] redes de comunicaciones<br>• [Media] soportes de información<br>• [AUX] equipamiento auxiliar<br>• [L] instalaciones<br>**Dimensiones:**<br>1. [D] disponibilidad<br>2. [C] confidencialidad<br>3. [I] integridad<br>**Descripción:**<br>utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.<br>**Ver:**<br>EBIOS: no disponible |
| Difusión de software dañino | x | x | x | **[A.8] Difusión de software dañino**<br>**Tipos de activos:**<br>• [SW] aplicaciones (software)<br>**Dimensiones:**<br>1. [D] disponibilidad<br>2. [I] integridad<br>3. [C] confidencialidad<br>**Descripción:**<br>propagación intencionada de virus, espías *(spyware)*, gusanos, troyanos, bombas lógicas, etc.<br>**Ver:**<br>EBIOS: no disponible |
| [Re-]encaminamiento de mensajes | | | x | **[A.9] [Re-]encaminamiento de mensajes**<br>**Tipos de activos:**<br>• [S] servicios<br>• [SW] aplicaciones (software)<br>• [COM] redes de comunicaciones<br>**Dimensiones:**<br>1. [C] confidencialidad<br>**Descripción:**<br>envío de información a un destino incorrecto a través de un sistema o una red, que llevan la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros.<br>Un atacante puede forzar un mensaje para circular a través de un nodo determinado de la red donde puede ser interceptado.<br>Es particularmente destacable el caso de que el ataque de encaminamiento lleve a una entrega fraudulenta, acabando la información en manos de quien no debe.<br>**Ver:**<br>EBIOS: no disponible |
| Alteración de secuencia | | x | | **[A.10] Alteración de secuencia**<br>**Tipos de activos:**<br>• [S] servicios<br>• [SW] aplicaciones (software)<br>• [COM] redes de comunicaciones<br>**Dimensiones:**<br>1. [I] integridad<br>**Descripción:**<br>alteración del orden de los mensajes transmitidos. Con ánimo de que el nuevo orden altere el significado del conjunto de mensajes, perjudicando a la integridad de los datos afectados.<br>**Ver:**<br>EBIOS: 36 - ALTERACIÓN DE DATOS |

| | | | | |
|---|---|---|---|---|
| Acceso no autorizado | | x | x | **[A.11] Acceso no autorizado**<br>**Tipos de activos:**<br>• [D] datos / información<br>• [keys] claves criptográficas<br>• [S] servicios<br>• [SW] aplicaciones (software)<br>• [HW] equipos informáticos (hardware)<br>• [COM] redes de comunicaciones<br>• [Media] soportes de información<br>• [AUX] equipamiento auxiliar<br>• [L] instalaciones<br>**Dim1nsiones:**<br>1. [C] confidencialidad<br>2. [I] integridad<br>**Descripción:**<br>el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.<br>**Ver:**<br>EBIOS: 33 - USO ILÍCITO DEL HARDWARE |
| Análisis de tráfico | | | x | **[A.12] Análisis de tráfico**<br>**Tipos de activos:**<br>• [COM] redes de comunicaciones<br>**Dimensiones:**<br>1. [C] confidencialidad<br>**Descripción:**<br>el atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios.<br>A veces se denomina "monitorización de tráfico".<br>**Ver:**<br>EBIOS: no disponible |
| Repudio | | x | | **[A.13] Repudio**<br>**Tipos de activos:**<br>• [S] servicios<br>• [D.log] registros de actividad<br>**Dimensiones:**<br>1. [I] integridad (trazabilidad)<br>**Descripción:**<br>negación a posteriori de actuaciones o compromisos adquiridos en el pasado.<br>Repudio de origen: negación de ser el remitente u origen de un mensaje o comunicación.<br>Repudio de recepción: negación de haber recibido un mensaje o comunicación.<br>Repudio de entrega: negación de haber recibido un mensaje para su entrega a otro.<br>**Ver:**<br>EBIOS: 41 - NEGACIÓN DE ACCIONES |
| Interceptación de información (escucha) | | | x | **[A.14] Interceptación de información (escucha)**<br>**Tipos de activos:**<br>• [COM] redes de comunicaciones<br>**Dimensiones:**<br>1. [C] confidencialidad<br>**Descripción:**<br>el atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada.<br>**Ver:**<br>EBIOS: 19 - ESCUCHA PASIVA |
| Modificación deliberada de la información | | x | | **[A.15] Modificación deliberada de la información**<br>**Tipos de activos:**<br>• [D] datos / información<br>• [keys] claves criptográficas<br>• [S] servicios (acceso)<br>• [SW] aplicaciones (SW)<br>• [COM] comunicaciones (tránsito)<br>• [Media] soportes de información<br>• [L] instalaciones<br>**Dimensiones:**<br>1. [I] integridad<br>**Descripción:**<br>alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.<br>**Ver:**<br>EBIOS: no disponible |
| Destrucción de información | x | | | **[A.18] Destrucción de información**<br>**Tipos de activos:**<br>• [D] datos / información<br>• [keys] claves criptográficas<br>• [S] servicios (acceso)<br>• [SW] aplicaciones (SW)<br>• [Media] soportes de información<br>• [L] instalaciones<br>**Dimensiones:**<br>1. [D] disponibilidad<br>**Descripción:**<br>eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.<br>**Ver:**<br>EBIOS: no disponible |

| | | | | |
|---|---|---|---|---|
| Divulgación de información | | | x | **[A.19] Revelación de información**<br>**Tipos de activos:**<br>• [D] datos / información<br>• [keys] claves criptográficas<br>• [S] servicios (acceso)<br>• [SW] aplicaciones (SW)<br>• [COM] comunicaciones (tránsito)<br>• [Media] soportes de información<br>• [L] instalaciones<br>**Dimensiones:**<br>1. [C] confidencialidad<br>**Descripción:**<br>revelación de información.<br>**Ver:**<br>EBIOS:<br>23 – DIVULGACIÓN<br>27 – GEOLOCALIZACIÓN<br>34 - COPIA ILEGAL DE SOFTWARE |
| Manipulación de programas | x | x | x | **[A.22] Manipulación de programas**<br>**Tipos de activos:**<br>• [SW] aplicaciones (software)<br>**Dimensiones:**<br>1. [C] confidencialidad<br>2. [I] integridad<br>3. [D] disponibilidad<br>**Descripción:**<br>alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.<br>**Ver:**<br>EBIOS: 26 - ALTERACIÓN DE PROGRAMAS |
| Manipulación de los equipos | x | | x | **[A.22] Manipulación de los equipos**<br>**Tipos de activos:**<br>• [HW] equipos<br>• [Media] soportes de información<br>• [AUX] equipamiento auxiliar<br>**Dimensiones:**<br>1. [C] confidencialidad<br>2. [D] disponibilidad<br>**Descripción:**<br>alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.<br>**Ver:**<br>EBIOS: 25 - SABOTAJE DEL HARDWARE |
| Denegación de servicio | x | | | **[A.24] Denegación de servicio**<br>**Tipos de activos:**<br>• [S] servicios<br>• [HW] equipos informáticos (hardware)<br>• [COM] redes de comunicaciones<br>**Dimensiones:**<br>1. [D] disponibilidad<br>**Descripción:**<br>la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.<br>**Ver:**<br>EBIOS: 30 - SATURACIÓN DEL SISTEMA INFORMÁTICO |
| Robo | x | | x | **[A.25] Robo**<br>**Tipos de activos:**<br>• [HW] equipos informáticos (hardware)<br>• [Media] soportes de información<br>• [AUX] equipamiento auxiliar<br>**Dimensiones:**<br>3. [D] disponibilidad<br>4. [C] confidencialidad<br>**Descripción:**<br>la sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad.<br>El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales.<br>El robo puede realizarlo personal interno, personas ajenas a la Organización o personas contratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias.<br>En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.<br>**Ver:**<br>EBIOS:<br>20 - ROBO DE SOPORTES O DOCUMENTOS<br>21 - ROBO DE HARDWARE |
| Ataque destructivo | x | | | **[A.26] Ataque destructivo**<br>**Tipos de activos:**<br>• [HW] equipos informáticos (hardware)<br>• [Media] soportes de información<br>• [AUX] equipamiento auxiliar<br>• [L] instalaciones<br>**Dimensiones:**<br>1. [D] disponibilidad<br>**Descripción:**<br>vandalismo, terrorismo, acción militar, ...<br>Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal.<br>**Ver:**<br>EBIOS: 05 - DESTRUCCIÓN DE HARDWARE O DE SOPORTES |

| | | | | |
|---|---|---|---|---|
| Ocupación enemiga | x | | x | **[A.27] Ocupación enemiga**<br>**Tipos de activos:** • [L] instalaciones<br>**Dimensiones:** 1. [D] disponibilidad 2. [C] confidencialidad<br>**Descripción:** cuando los locales han sido invadidos y se carece de control sobre los propios medios de trabajo.<br>**Ver:** EBIOS: no disponible |
| Indisponibilidad del personal | x | | | **[A.28] Indisponibilidad del personal**<br>**Tipos de activos:** • [P] personal interno<br>**Dimensiones:** 1. [D] disponibilidad<br>**Descripción:** ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos, ...<br>**Ver:** EBIOS: 42 - DAÑO A LA DISPONIBILIDAD DEL PERSONAL |
| Extorsión | x | x | x | **[A.29] Extorsión**<br>**Tipos de activos:** • [P] personal interno<br>**Dimensiones:** 1. [C] confidencialidad 2. [I] integridad 3. [D] disponibilidad<br>**Descripción:** presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.<br>**Ver:** EBIOS: no disponible |
| Ingeniería social (picaresca) | x | x | x | **[A.30] Ingeniería social (picaresca)**<br>**Tipos de activos:** • [P] personal interno<br>**Dimensiones:** 1. [C] confidencialidad 2. [I] integridad 3. [D] disponibilidad<br>**Descripción:** abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.<br>**Ver:** EBIOS: no disponible |

**Fuente:** Extraído del cuadro 3 del Anexo B del documento “Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del Sector Público” y MAGERIT versión 3.0.

## ANEXO II: INVENTARIO DE ACTIVOS DE INFORMACIÓN

| N° | CÓDIGO DEL ACTIVO | NOMBRE DEL ACTIVO | DESCRIPCIÓN | TIPO DE ACTIVO | UBICACIÓN | UNIDAD RESPONSABLE | CUSTODIO |
|---|---|---|---|---|---|---|---|
| 1 | S1 | Sistema de Repositorio Institucional | Sistema para publicación de trabajos de grado accesibles para el público en general, que fueron defendidos y aprobados, de la UPEA. | Servicios | [Servidor 3] / CPD (Data Center). | Unidad SIE | Administrador(es) del sistema |
| 2 | S2 | Sistema orientación vocacional | Sistema destinado a la población en general, el cual, mediante test, muestra las afinidades de las personas para postular a una carrera universitaria. | Servicios | [Servidor 15] / CPD (Data Center). | Unidad SIE | Administrador(es) del sistema |
| 3 | S3 | Zoom | Servicio de video conferencia adquirido. | Servicios | Nube. | Unidad SIE | Personal de Unidad SIE |
| 4 | S4 | Plataformas Virtuales Moodle | Plataforma en línea para el proceso de enseñanza-aprendizaje. | Servicios | [Servidor 13] / CPD (Data Center). | Unidad SIE | Personal de Unidad SIE |
| 5 | S5 | Zimbra y Zamba | Servicio de correo electrónico institucional. | Servicios | [Servidor 6] / CPD (Data Center). | Unidad SIE | Usuarios |
| 6 | S6 | Cloud | Servicio de almacenamiento remoto de archivos y procesamiento de datos. | Servicios | [Servidor 6] / CPD (Data Center). | Unidad SIE | Personal de Unidad SIE |
| 7 | S7 | Jitsi Meet | Servidor para videoconferencias sin límite de personas participantes. | Servicios | [Servidor 8] / CPD (Data Center). | Unidad SIE | Usuarios |
| 8 | S8 | Páginas Web Institucionales | Servidor para distribución y contenido de páginas web. | Servicios | 1) [Servidor 6] (páginas web de carreras) / CPD (Data Center).<br>2) [Servidor 1] (páginas web de las sedes académicas y otros) / CPD (Data Center).<br>3) [Servidor 2] (páginas web de la DICyT y de la Carrera Ciencias de la Comunicación Social y otros) / CPD (Data Center).<br>4) [Servidor 15] (páginas web de las áreas académicas, algunas carreras y unidades administrativas) / CPD (Data Center).<br>5) [Servidor 16] (páginas web de carreras Agronomía y Educación Parvularia y radioupea) / CPD (Data Center).<br>6) [Servidor 10] (página web de carrera Arquitectura) / CPD (Data Center). | Unidad SIE | Administradores de las páginas web institucionales |
| 9 | S9 | Servidor de Base de Datos | Servidor que tiene almacenado la base de datos principal y permite administrarlo. | Servicios | [Servidor 7] / CPD (Data Center). | Unidad SIE | DBA |
| 10 | S10 | Servidor de Backups | Servidor de Copia de Seguridad de Datos. | Servicios | [Servidor 8] / CPD (Data Center). | Unidad SIE | RCPD |
| 11 | S11 | Servidor DNS "upea.bo" | Servidor de Nombres de Dominio. | Servicios | [Servidor 6] / CPD (Data Center) | Unidad SIE | RCPD |
| 12 | S12 | Servidor DNS "upea.edu.bo" | Servidor de Nombres de Dominio. | Servicios | [Servidor 11] / CPD (Data Center). | Unidad SIE | RCPD |
| 13 | S13 | Servidor de Streaming de Radio UPEA | Servidor para la transmisión de audio en tiempo real de la radio UPEA. | Servicios | [Servidor 10] / CPD (Data Center). | Unidad SIE | Administrador del Streaming de Radio |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 14 | SA1 | Sistema de Control Docente (SICOD)" | Sistema de seguimiento y control para asignación y emisión de nombramientos de los docentes de las carreras, tanto para vicerrectorado y decanaturas. | Software – Aplicaciones informáticas | [Servidor 14] / CPD (Data Center). | Vicerrectorado UPEA | Responsable del Sistema |
| 15 | SA2 | Sistema de Control de Certificaciones (SICC) | Sistema para emisión de certificaciones para docentes de la universidad. | Software – Aplicaciones informáticas | [Servidor 14] / CPD (Data Center). | Tribunal de Proceso, Técnico de Tesorería, Responsable de Archivo Central y Responsable del Departamento de Idiomas. | Administradores del sistema |
| 16 | SA3 | Sistema de Logeo (SILOG) | Sistema de control y acceso de logeo genérico. | Software – Aplicaciones informáticas | [Servidor 14] / CPD (Data Center). | Unidad SIE | Administrador(es) del sistema |
| 17 | SA4 | Sistema de Autoevaluación, evaluación y acreditación "EVA" | Sistema de autoevaluación y posterior acreditación en la CEUB. | Software – Aplicaciones informáticas | [Servidor 14] / CPD (Data Center). | Vicerrectorado | Técnico de Acreditación de Vicerrectorado |
| 18 | SA5 | Sistema de convenios para la Dirección de Relaciones Nacionales e Internacionales | Sistema para publicar información relativo a los convenios interinstitucionales. | Software – Aplicaciones informáticas | [Servidor 15] / CPD (Data Center). | Unidad de Relaciones Internacionales | Administrador(es) del sistema |
| 19 | SA6 | Sistema de planillas y control de asistencias HCU "SAYP" | Sistema de seguimiento de control de planillas y control de consejeros de docentes y estudiantes e impresión de planillas de pago, reuniones, y sesiones de HCU. | Software – Aplicaciones informáticas | [Servidor 14] / CPD (Data Center). | HCU | Administrador del sistema |
| 20 | SA7 | CMS basado en codeigniter para publicaciones de páginas | Sistema de control de publicaciones y seguimiento de actividades para las unidades y carreras de la universidad. | Software – Aplicaciones informáticas | [Servidor 15] / CPD (Data Center). | Vicerrectorado | Administrador(es) del sistema |
| 21 | SA8 | Sistema de seguimiento y evaluación de pasantes “SIE-CEP” | Sistema para control de pasantes en cuanto a actividades, trabajos realizados, control de asistencia y finalmente la evaluación respectiva de la Unidad SIE. | Software – Aplicaciones informáticas | [Servidor 14] / CPD (Data Center). | Unidad SIE | Personal de SIE que administran el Sistema |
| 22 | SA9 | Sistema universitario de inscripciones académicas “SUYAY” | Sistema de inscripciones para las carreras en cuanto se refiere a la administración de Kardex, impresión de récord, historiales, llenado de notas, inscripciones web por el estudiante entre otros. | Software – Aplicaciones informáticas | 1) [Servidor 1] / CPD (Data Center).<br>2) [Servidor 2] / CPD (Data Center).<br>3) [Servidor 4] / CPD (Data Center).<br>4) [Servidor 5] / CPD (Data Center).<br>5) [Servidor 14] / CPD (Data Center). | Kardex Académico Estudiantil de las Carreras de la UPEA | Técnicos de Kardex Académico Estudiantil |
| 23 | SA10 | Rediseño de sistema para la Unidad de DISBED | Sistema reformulado para la Unidad de DISBEDC, para revisión, evaluación y calificación de las becas universitarias. | Software – Aplicaciones informáticas | [Servidor 14] / CPD (Data Center). | DISBED | Administrador(es) del Sistema |
| 24 | SA11 | Sistema de Matriculación Académica Estudiantil "MAE" | Sistema de matriculación anual de estudiantes universitarios. | Software – Aplicaciones informáticas | [Servidor 14] / CPD (Data Center). | Unidad de RRAA | Responsable del Sistema |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 25 | SA12 | Sistema de inscripciones "MAYA" | Sistema de inscripciones para las carreras en cuanto se refiere a la administración de Kardex, impresión de récord, historiales, llenado de notas, inscripciones web por el estudiante entre otros. | Software – Aplicaciones informáticas | 1) [Servidor 2] / CPD (Data Center).<br>2) [Servidor 14] / CPD (Data Center). | Kardex Académico Estudiantil de las Carreras de la UPEA | Técnicos de Kardex Académico Estudiantil |
| 26 | SA13 | Sistema de Vacaciones (SIVA) | Sistema que centraliza el uso de vacaciones del plantel administrativo de la institución. | Software – Aplicaciones informáticas | [Servidor 14] / CPD (Data Center). | Dirección de RRHH | Responsable del Sistema |
| 27 | SA14 | Sistema de administración y control de planillas (SI@COP) | Sistema de planillas de administrativos, docentes y estudiantes de la institución. | Software – Aplicaciones informáticas | [Servidor 14] / CPD (Data Center). | Dirección de RRHH | Responsable del Sistema |
| 28 | SA15 | Sistema de información académica de departamento de idiomas (SI@DI) | Sistema académico desarrollado para el Departamento de Idiomas dependiente de la Carrera de Lingüística e Idiomas el cual centraliza las inscripciones, Kardex y la emisión de certificados de los diferentes idiomas que se dicta en la universidad. | Software – Aplicaciones informáticas | [Servidor 9] / CPD (Data Center). | Departamento de Idiomas de la Carrera de Lingüística e Idiomas | Responsable de kardex del Departamento de Idiomas |
| 29 | SA16 | Sistema Administración y Control de Activos Fijos “SAF-ENOC” | Sistema desarrollado, para el control y seguimiento de los activos con que cuenta nuestra casa superior de estudios. | Software – Aplicaciones informáticas | [Servidor 4] / CPD (Data Center). | Unidad de Activos Fijos | Administrador(es) del Sistema |
| 30 | SA17 | Sistema de preuniversitario | Sistema de admisión estudiantil de postulantes a las diferentes carreras mediante las modalidades de admisión correspondientes. | Software – Aplicaciones informáticas | [Servidor 5] / CPD (Data Center). | Carreras de la UPEA | Coordinador del Curso Preuniversitario |
| 31 | SA18 | Sistema de Evaluación Docente (EVADOC) | Sistema para realizar la evaluación del personal docente de nuestra universidad. | Software – Aplicaciones informáticas | [Servidor 1] / CPD (Data Center). | Vicerrectorado | Responsable del Sistema |
| 32 | SA19 | Sistema de Biblioteca | Sistema de la Biblioteca Central de la institución, para el inventario y préstamo de libros, textos y otros a los estudiantes universitarios de nuestra casa superior de estudios. | Software – Aplicaciones informáticas | [Servidor 5] / CPD (Data Center). | Biblioteca Central, Bibliotecas de Carrera | Responsables de la Bibliotecas |
| 33 | SA20 | Sistema de Administración de la Dirección de Investigación Ciencia y Tecnología (SIAD-DICyT) | Sistema elaborado para la unidad de ciencias y tecnología dependiente de la UPEA, el cual centraliza los proyectos de los diferentes institutos de investigación con los que cuenta la UPEA. | Software – Aplicaciones informáticas | [Servidor 2] / CPD (Data Center). | DICyT | Administrador(es) del Sistema |
| 34 | SA21 | Sistema de Secretaria General | Sistema para el registro de resoluciones emanadas por el honorable consejo universitario (HCU), así como resoluciones administrativas (Rectorado y Dirección administrativa financiera). | Software – Aplicaciones informáticas | [Servidor 14] / CPD (Data Center). | Secretaría General | Administrador del sistema |
| 35 | SA22 | Sistema Operativo servidor | Gnu/Linux. | Software – Aplicaciones informáticas | Servidores del CPD (Data Center). | Unidad SIE | RCPD |
| 36 | SA23 | Sistema Operativo usuario administrativo o autoridad | Sistema operativo en computadoras de escritorio Windows 7 para adelante. | Software – Aplicaciones informáticas | Equipos computaciones de Oficinas de la UPEA. | Unidad SIE | Usuario |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 37 | SA24 | Ofimática | Aplicaciones Word, Excel, Power Point, etc. | Software – Aplicaciones informáticas | Equipos computaciones de Oficinas de la UPEA. | Unidad SIE | Usuario |
| 38 | H1 | Switch | Switch para IPs públicas, TRENDNET TL2-G244. | Equipamiento informático (hardware) | CPD (Data Center). | Unidad SIE | RCPD |
| 39 | H2 | Switches | 1) Switch de 24 puertos.<br>2) Switch de 24 puertos.<br>3) Switch de 24 puertos.<br>4) Switch de 24 puertos. | Equipamiento informático (hardware) | CPD (Data Center). | Unidad SIE | RCPD |
| 40 | H3 | Firewall | Firewall pfSense.. | Equipamiento informático (hardware) | CPD (Data Center). | Unidad SIE | RCPD |
| 41 | H4 | Router | Mikrotik Cloud Core Router CCR1036-86-2ST. | Equipamiento informático (hardware) | CPD (Data Center). | Unidad SIE | RCPD |
| 42 | H5 | Servidor 1 | Servidor de marca DELL R940. | Equipamiento informático (hardware) | CPD (Data Center). | Unidad SIE | RCPD |
| 43 | H6 | Servidor 2 | Servidor de marca DELL R740xd. | Equipamiento informático (hardware) | CPD (Data Center). | Unidad SIE | RCPD |
| 44 | H7 | Servidor 3 | Servidor de marca DELL R740. | Equipamiento informático (hardware) | CPD (Data Center). | Carrera de Derecho | RCPD |
| 45 | H8 | Servidor 4 | Servidor de marca DELL R730. | Equipamiento informático (hardware) | CPD (Data Center). | Carrera Ingeniería de Sistemas | RCPD |
| 46 | H9 | Servidor 5 | Servidor de marca DELL R630. | Equipamiento informático (hardware) | CPD (Data Center). | Carrera Ingeniería de Sistemas | RCPD |
| 47 | H10 | Servidor 6 | Servidor de marca DELL R740xd. | Equipamiento informático (hardware) | CPD (Data Center). | Unidad SIE | RCPD |
| 48 | H11 | Servidor 7 | Servidor de marca DELL R940. | Equipamiento informático (hardware) | CPD (Data Center). | Unidad SIE | RCPD |
| 49 | H12 | Servidor 8 | Servidor de marca DELL R940. | Equipamiento informático (hardware) | CPD (Data Center). | Unidad SIE | RCPD |
| 50 | H13 | Servidor 9 | Servidor de marca HP ML110 Gen9. | Equipamiento informático (hardware) | CPD (Data Center). | Departamento de Idiomas | RCPD |
| 51 | H14 | Servidor 10 | Servidor de marca DELL R440. | Equipamiento informático (hardware) | CPD (Data Center). | Carrera Arquitectura | RCPD |
| 52 | H15 | Servidor 11 | Servidor de marca DELL R710. | Equipamiento informático (hardware) | CPD (Data Center). | Unidad SIE | RCPD |
| 53 | H16 | Servidor 12 | Servidor de marca DELL R740xd. | Equipamiento informático (hardware) | CPD (Data Center). | Unidad SIE | RCPD |
| 54 | H17 | Servidor 13 | Servidor de marca DELL R740xd. | Equipamiento informático (hardware) | CPD (Data Center). | Unidad SIE | RCPD |
| 55 | H18 | Servidor 14 | Servidor de marca DELL R740xd. | Equipamiento informático (hardware) | CPD (Data Center). | Unidad SIE | RCPD |
| 56 | H19 | Servidor 15 | Servidor de marca HP ML150 Gen9. | Equipamiento informático (hardware) | CPD (Data Center). | Carrera Agronomía | RCPD |
| 57 | H20 | Servidor 16 | Servidor de marca HP ML150 Gen9. | Equipamiento informático (hardware) | CPD (Data Center). | Carrera Agronomía | RCPD |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 58 | H21 | Equipos Computacionales | Computadoras Personales de todas las dependencias administrativas de la UPEA. | Equipamiento informático (hardware) | Sedes de la UPEA. | Direcciones y Unidades Administrativas y/o Académicas | Administrativo(a) o autoridad universitaria al que le ha sido asignado el(los) equipo(s) computacional(es) |
| 59 | H22 | Impresoras | Impresoras de todas las dependencias administrativas de la UPEA. | Equipamiento informático (hardware) | Sedes de la UPEA. | Direcciones y Unidades Administrativas y/o Académicas | Administrativo(a) o autoridad universitaria al que le ha sido asignado la(s) impresora(s) |
| 60 | H23 | Fotocopiadoras | Fotocopiadoras de todas las dependencias administrativas de la UPEA. | Equipamiento informático (hardware) | Sedes de la UPEA. | Direcciones y Unidades Administrativas y/o Académicas | Administrativo(a) o autoridad universitaria al que le ha sido asignado la(s) fotocopiadora(s) |
| 61 | RC1 | Internet | Fibra AXS. | Redes de comunicaciones | CPD (Data Center). | Unidad SIE | RCPD, Técnico de redes |
| 62 | SI1 | Sistema Operativo Virtual para Posgrado de la UPEA | Sistema Operativo Gnu/Linux, que administra la Dirección de Posgrado de la UPEA. | Soportes de información | [Servidor 4] / CPD (Data Center). | Dirección de Posgrado-UPEA | Administrador del Sistema |
| 63 | SI2 | Sistema Operativo Virtual para los servicios: Cloud y Correo Institucional | Sistema Operativo Virtual Gnu/Linux para el soporte de Servicios Cloud y el Sistema de Correo Institucional. | Soportes de información | [Servidor 6] / CPD (Data Center). | Unidad SIE | RCPD |
| 64 | SI3 | Sistema Operativo Virtual para Instituto de Investigación de la Carrera de Ingeniería de Sistemas | Sistema Operativo Virtual Gnu/Linux, para el sitio web del Instituto de Investigación de la Carrera de Ingeniería de Sistemas. | Soportes de información | [Servidor 12] / CPD (Data Center). | Unidad SIE | RCPD |
| 65 | EA1 | UPS | Para la gestión de energía regulada. | Equipamiento auxiliar | TRIPP-LITE SU20KX / CPD (Data Center). | Unidad SIE | RCPD |
| 66 | EA2 | Climatizador | Sistema de aire acondicionado. | Equipamiento auxiliar | CLIMAVENE+A / CPD (Data Center). | Unidad SIE | RCPD |
| 67 | EA3 | Fuente de Alimentación de Cerradura Magnética | Para el acceso al Data Center. | Equipamiento auxiliar | CPD (Data Center). | Unidad SIE | RCPD |
| 68 | EA4 | Controlable Monofásico | 1) PDUMH20HVATNET, PDU Controlable de 200/240V.<br>2) PDUMH20HVATNET, PDU Controlable de 200/240V.<br>3) PDUMH20HVATNET, PDU Controlable de 200/240V.<br>4) PDUMH20HVATNET, PDU Controlable de 200/240V. | Equipamiento auxiliar | CPD (Data Center). | Unidad SIE | RCPD |
| 69 | P1 | Autoridades | Rector, Vicerrector, Decanos de Áreas, Directores de Carrera. | Personal | Oficinas de la UPEA | Dirección de RRHH | ---------- |
| 70 | P2 | Representantes | Docentes y estudiantes elegidos en sus estamentos. | Personal | Oficinas de la UPEA | Dirección de RRHH | ---------- |
| 71 | P3 | Administrativos | Plantel Administrativo de la UPEA. | Personal | Oficinas de la UPEA | Dirección de RRHH | ---------- |
| 72 | P4 | Docentes | Plantel Docente de la UPEA. | Personal | Aulas físicas o virtuales | Direcciones de Carreras | ---------- |
| 73 | P5 | Estudiantes | Estudiantes universitarios matriculados en la UPEA. | Personal | Aulas físicas o virtuales | Direcciones de Carrera | ---------- |

## ANEXO III: VALORACIÓN DE ACTIVOS DE INFORMACIÓN

| N° | CÓDIGO DEL ACTIVO | NOMBRE DEL ACTIVO | DESCRIPCIÓN | TIPO DE ACTIVO | Disponibilidad | Integridad | Confidencialidad | Valoración del Activo de Información | | Fecha de Inicio |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | S1 | Sistema de Repositorio Institucional | Sistema para publicación de trabajos de grado accesibles para el público en general, que fueron defendidos y aprobados, de la UPEA. | Servicios | 2 | 2 | 2 | 6 | Bajo | |
| 2 | S2 | Sistema orientación vocacional | Sistema destinado a la población en general, el cual, mediante test, muestra las afinidades de las personas para postular a una carrera universitaria. | Servicios | 1 | 1 | 1 | 3 | Muy Bajo | |
| 3 | S3 | Zoom | Servicio de video conferencia adquirido. | Servicios | 4 | 2 | 2 | 8 | Medio | |
| 4 | S4 | Plataformas Virtuales Moodle | Plataforma en línea para el proceso de enseñanza-aprendizaje. | Servicios | 3 | 3 | 3 | 9 | Medio | |
| 5 | S5 | Zimbra y Zamba | Servicio de correo electrónico institucional. | Servicios | 2 | 2 | 2 | 6 | Bajo | |
| 6 | S6 | Cloud | Servicio de almacenamiento remoto de archivos y procesamiento de datos. | Servicios | 1 | 2 | 2 | 5 | Bajo | |
| 7 | S7 | Jitsi Meet | Servidor para videoconferencias sin límite de personas participantes. | Servicios | 1 | 1 | 1 | 3 | Muy Bajo | |
| 8 | S8 | Páginas Web Institucionales | Servidor para distribución y contenido de páginas web. | Servicios | 2 | 2 | 1 | 5 | Bajo | |
| 9 | S9 | Servidor de Base de Datos | Servidor que tiene almacenado la base de datos principal y permite administrarlo. | Servicios | 5 | 5 | 5 | 15 | Muy Alto | |
| 10 | S10 | Servidor de Backups | Servidor de Copia de Seguridad de Datos. | Servicios | 4 | 4 | 4 | 12 | Alto | |
| 11 | S11 | Servidor DNS "upea.bo" | Servidor de Nombres de Dominio. | Servicios | 5 | 4 | 5 | 14 | Muy Alto | |
| 12 | S12 | Servidor DNS "upea.edu.bo" | Servidor de Nombres de Dominio. | Servicios | 5 | 4 | 5 | 14 | Muy Alto | |
| 13 | S13 | Servidor de Streaming de Radio UPEA | Servidor para la transmisión de audio en tiempo real de la radio UPEA. | Servicios | 3 | 2 | 1 | 6 | Bajo | |
| 14 | SA1 | Sistema de Control Docente (SICOD)" | Sistema de seguimiento y control para asignación y emisión de nombramientos de los docentes de las carreras, tanto para vicerrectorado y decanaturas. | Software – Aplicaciones informáticas | 5 | 4 | 3 | 12 | Alto | |
| 15 | SA2 | Sistema de Control de Certificaciones (SICC) | Sistema para emisión de certificaciones para docentes de la universidad. | Software – Aplicaciones informáticas | 5 | 4 | 3 | 12 | Alto | |
| 16 | SA3 | Sistema de Logeo (SILOG) | Sistema de control y acceso de logeo genérico. | Software – Aplicaciones informáticas | 3 | 3 | 3 | 9 | Medio | |
| 17 | SA4 | Sistema de Autoevaluación, evaluación y acreditación "EVA" | Sistema de autoevaluación y posterior acreditación en la CEUB. | Software – Aplicaciones informáticas | 2 | 2 | 2 | 6 | Bajo | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 18 | SA5 | Sistema de convenios para la Dirección de Relaciones Nacionales e Internacionales | Sistema para publicar información relativo a los convenios interinstitucionales. | Software – Aplicaciones informáticas | 2 | 2 | 2 | 6 | Bajo | |
| 19 | SA6 | Sistema de planillas y control de asistencias HCU "SAYP" | Sistema de seguimiento de control de planillas y control de consejeros de docentes y estudiantes e impresión de planillas de pago, reuniones, y sesiones de HCU. | Software – Aplicaciones informáticas | 5 | 4 | 3 | 12 | Alto | |
| 20 | SA7 | CMS basado en codeigniter para publicaciones de páginas | Sistema de control de publicaciones y seguimiento de actividades para las unidades y carreras de la universidad. | Software – Aplicaciones informáticas | 2 | 2 | 2 | 6 | Bajo | |
| 21 | SA8 | Sistema de seguimiento y evaluación de pasantes "SIE-CEP" | Sistema para control de pasantes en cuanto a actividades, trabajos realizados, control de asistencia y finalmente la evaluación respectiva de la Unidad SIE. | Software – Aplicaciones informáticas | 2 | 2 | 1 | 5 | Bajo | |
| 22 | SA9 | Sistema universitario de inscripciones académicas "SUYAY" | Sistema de inscripciones para las carreras en cuanto se refiere a la administración de Kardex, impresión de récord, historiales, llenado de notas, inscripciones web por el estudiante entre otros. | Software – Aplicaciones informáticas | 5 | 4 | 3 | 12 | Alto | |
| 23 | SA10 | Rediseño de sistema para la Unidad de DISBED | Sistema reformulado para la Unidad de DISBEDC, para revisión, evaluación y calificación de las becas universitarias. | Software – Aplicaciones informáticas | 5 | 4 | 3 | 12 | Alto | |
| 24 | SA11 | Sistema de Matriculación Académica Estudiantil "MAE" | Sistema de matriculación anual de estudiantes universitarios. | Software – Aplicaciones informáticas | 5 | 4 | 3 | 12 | Alto | |
| 25 | SA12 | Sistema de inscripciones "MAYA" | Sistema de inscripciones para las carreras en cuanto se refiere a la administración de Kardex, impresión de récord, historiales, llenado de notas, inscripciones web por el estudiante entre otros. | Software – Aplicaciones informáticas | 5 | 4 | 3 | 12 | Alto | |
| 26 | SA13 | Sistema de Vacaciones (SIVA) | Sistema que centraliza el uso de vacaciones del plantel administrativo de la institución. | Software – Aplicaciones informáticas | 2 | 2 | 2 | 6 | Bajo | |
| 27 | SA14 | Sistema de administración y control de planillas (SI@COP) | Sistema de planillas de administrativos, docentes y estudiantes de la institución. | Software – Aplicaciones informáticas | 5 | 4 | 3 | 12 | Alto | |
| 28 | SA15 | Sistema de información académica de departamento de idiomas (SI@DI) | Sistema académico desarrollado para el Departamento de Idiomas dependiente de la Carrera de Lingüística e Idiomas el cual centraliza las inscripciones, Kardex y la emisión de certificados de los diferentes idiomas que se dicta en la universidad. | Software – Aplicaciones informáticas | 5 | 4 | 3 | 12 | Alto | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 29 | SA16 | Sistema Administración y Control de Activos Fijos “SAF-ENOC” | Sistema desarrollado, para el control y seguimiento de los activos con que cuenta nuestra casa superior de estudios. | Software – Aplicaciones informáticas | 2 | 3 | 3 | 8 | Medio | |
| 30 | SA17 | Sistema de preuniversitario | Sistema de admisión estudiantil de postulantes a las diferentes carreras mediante las modalidades de admisión correspondientes. | Software – Aplicaciones informáticas | 5 | 4 | 3 | 12 | Alto | |
| 31 | SA18 | Sistema de Evaluación Docente (EVADOC) | Sistema para realizar la evaluación del personal docente de nuestra universidad. | Software – Aplicaciones informáticas | 5 | 4 | 3 | 12 | Alto | |
| 32 | SA19 | Sistema de Biblioteca | Sistema de la Biblioteca Central de la institución, para el inventario y préstamo de libros, textos y otros a los estudiantes universitarios de nuestra casa superior de estudios. | Software – Aplicaciones informáticas | 2 | 2 | 2 | 6 | Bajo | |
| 33 | SA20 | Sistema de Administración de la Dirección de Investigación Ciencia y Tecnología (SIAD-DICyT) | Sistema elaborado para la unidad de ciencias y tecnología dependiente de la UPEA, el cual centraliza los proyectos de los diferentes institutos de investigación con los que cuenta la UPEA. | Software – Aplicaciones informáticas | 2 | 2 | 2 | 6 | Bajo | |
| 34 | SA21 | Sistema de Secretaria General | Sistema para el registro de resoluciones emanadas por el honorable consejo universitario (HCU), así como resoluciones administrativas (Rectorado y Dirección administrativa financiera). | Software – Aplicaciones informáticas | 2 | 2 | 1 | 5 | Bajo | |
| 35 | SA22 | Sistema Operativo servidor | Gnu/Linux. | Software – Aplicaciones informáticas | 5 | 5 | 5 | 15 | Muy Alto | |
| 36 | SA23 | Sistema Operativo usuario administrativo o autoridad | Sistema operativo en computadoras de escritorio Windows 7 para adelante. | Software – Aplicaciones informáticas | 3 | 3 | 3 | 9 | Medio | |
| 37 | SA24 | Ofimática | Aplicaciones Word, Excel, Power Point, etc. | Software – Aplicaciones informáticas | 4 | 3 | 2 | 9 | Medio | |
| 38 | H1 | Switch | Switch para IPs públicas, TRENDNET TL2-G244. | Equipamiento informático (hardware) | 4 | 4 | 4 | 12 | Alto | |
| 39 | H2 | Switches | 1) Switch de 24 puertos.<br>2) Switch de 24 puertos.<br>3) Switch de 24 puertos.<br>4) Switch de 24 puertos. | Equipamiento informático (hardware) | 3 | 3 | 2 | 8 | Medio | |
| 40 | H3 | Firewall | Firewall pfSense.. | Equipamiento informático (hardware) | 4 | 4 | 4 | 12 | Alto | |
| 41 | H4 | Router | Mikrotik Cloud Core Router CCR1036-86-2ST. | Equipamiento informático (hardware) | 4 | 4 | 4 | 12 | Alto | |
| 42 | H5 | Servidor 1 | Servidor de marca DELL R940. | Equipamiento informático (hardware) | 5 | 4 | 5 | 14 | Muy Alto | |
| 43 | H6 | Servidor 2 | Servidor de marca DELL R740xd. | Equipamiento informático (hardware) | 4 | 4 | 4 | 12 | Alto | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 44 | H7 | Servidor 3 | Servidor de marca DELL R740. | Equipamiento informático (hardware) | 4 | 4 | 4 | 12 | Alto | |
| 45 | H8 | Servidor 4 | Servidor de marca DELL R730. | Equipamiento informático (hardware) | 4 | 4 | 4 | 12 | Alto | |
| 46 | H9 | Servidor 5 | Servidor de marca DELL R630. | Equipamiento informático (hardware) | 4 | 4 | 4 | 12 | Alto | |
| 47 | H10 | Servidor 6 | Servidor de marca DELL R740xd. | Equipamiento informático (hardware) | 5 | 5 | 5 | 15 | Muy Alto | |
| 48 | H11 | Servidor 7 | Servidor de marca DELL R940. | Equipamiento informático (hardware) | 5 | 5 | 5 | 15 | Muy Alto | |
| 49 | H12 | Servidor 8 | Servidor de marca DELL R940. | Equipamiento informático (hardware) | 5 | 4 | 5 | 14 | Muy Alto | |
| 50 | H13 | Servidor 9 | Servidor de marca HP ML110 Gen9. | Equipamiento informático (hardware) | 4 | 4 | 4 | 12 | Alto | |
| 51 | H14 | Servidor 10 | Servidor de marca DELL R440. | Equipamiento informático (hardware) | 4 | 4 | 4 | 12 | Alto | |
| 52 | H15 | Servidor 11 | Servidor de marca DELL R710. | Equipamiento informático (hardware) | 5 | 5 | 5 | 15 | Muy Alto | |
| 53 | H16 | Servidor 12 | Servidor de marca DELL R740xd. | Equipamiento informático (hardware) | 4 | 4 | 4 | 12 | Alto | |
| 54 | H17 | Servidor 13 | Servidor de marca DELL R740xd. | Equipamiento informático (hardware) | 4 | 4 | 4 | 12 | Alto | |
| 55 | H18 | Servidor 14 | Servidor de marca DELL R740xd. | Equipamiento informático (hardware) | 4 | 4 | 4 | 12 | Alto | |
| 56 | H19 | Servidor 15 | Servidor de marca HP ML150 Gen9. | Equipamiento informático (hardware) | 4 | 4 | 4 | 12 | Alto | |
| 57 | H20 | Servidor 16 | Servidor de marca HP ML150 Gen9. | Equipamiento informático (hardware) | 4 | 4 | 4 | 12 | Alto | |
| 58 | H21 | Equipos Computacionales | Computadoras Personales de todas las dependencias administrativas de la UPEA. | Equipamiento informático (hardware) | 4 | 4 | 4 | 12 | Alto | |
| 59 | H22 | Impresoras | Impresoras de todas las dependencias administrativas de la UPEA. | Equipamiento informático (hardware) | 3 | 2 | 1 | 6 | Bajo | |
| 60 | H23 | Fotocopiadoras | Fotocopiadoras de todas las dependencias administrativas de la UPEA. | Equipamiento informático (hardware) | 3 | 1 | 1 | 5 | Bajo | |
| 61 | RC1 | Internet | Fibra AXS. | Redes de comunicaciones | 5 | 3 | 3 | 11 | Alto | |
| 62 | SI1 | Sistema Operativo Virtual para Posgrado de la UPEA | Sistema Operativo Gnu/Linux, que administra la Dirección de Posgrado de la UPEA. | Soportes de información | 5 | 4 | 3 | 12 | Alto | |
| 63 | SI2 | Sistema Operativo Virtual para los servicios: Cloud y Correo Institucional | Sistema Operativo Virtual Gnu/Linux para el soporte de Servicios Cloud y el Sistema de Correo Institucional. | Soportes de información | 3 | 2 | 2 | 7 | Medio | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 64 | SI3 | Sistema Operativo Virtual para Instituto de Investigación de la Carrera de Ingeniería de Sistemas | Sistema Operativo Virtual Gnu/Linux, para el sitio web del Instituto de Investigación de la Carrera de Ingeniería de Sistemas. | Soportes de información | 5 | 4 | 3 | 12 | Alto | |
| 65 | EA1 | UPS | Para la gestión de energía regulada. | Equipamiento auxiliar | 5 | 3 | 3 | 11 | Alto | |
| 66 | EA2 | Climatizador | Sistema de aire acondicionado. | Equipamiento auxiliar | 5 | 3 | 3 | 11 | Alto | |
| 67 | EA3 | Fuente de Alimentación de Cerradura Magnética | Para el acceso al Data Center. | Equipamiento auxiliar | 5 | 3 | 3 | 11 | Alto | |
| 68 | EA4 | Controlable Monofásico | 1) PDUMH20HVATNET, PDU Controlable de 200/240V.<br>2) PDUMH20HVATNET, PDU Controlable de 200/240V.<br>3) PDUMH20HVATNET, PDU Controlable de 200/240V.<br>4) PDUMH20HVATNET, PDU Controlable de 200/240V. | Equipamiento auxiliar | 5 | 4 | 2 | 11 | Alto | |
| 69 | P1 | Autoridades | Rector, Vicerrector, Decanos de Áreas, Directores de Carrera. | Personal | 5 | 4 | 3 | 12 | Alto | |
| 70 | P2 | Representantes | Docentes y estudiantes elegidos en sus estamentos. | Personal | 3 | 3 | 3 | 9 | Medio | |
| 71 | P3 | Administrativos | Plantel Administrativo de la UPEA. | Personal | 5 | 4 | 3 | 12 | Alto | |
| 72 | P4 | Docentes | Plantel Docente de la UPEA. | Personal | 2 | 2 | 2 | 6 | Bajo | |
| 73 | P5 | Estudiantes | Estudiantes universitarios matriculados en la UPEA. | Personal | 2 | 2 | 1 | 5 | Bajo | |

## ANEXO IV: IDENTIFICACIÓN, ANÁLISIS Y VALORACIÓN DE RIESGOS

| N° | ACTIVO/PROCESO | Amenaza(s) | Situación | Vulnerabilidad | VALORACIÓN DE ACTIVOS | | | VALORACIÓN DE RIESGO | | RIESGO | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Disponibilidad | Integridad | Confidencialidad | | | Probabilidad | | Impacto | | Nivel de riesgo | |
| 1 | [SA15] Sistema de información académica de departamento de idiomas (SI@DI) | Errores de los usuarios. | En algunos casos, el estudiante llena mal sus datos de inscripción. | Algún(os) dato(s) incorrecto(s) del estudiante por equivocación en el taypeo. | 3 | 4 | 3 | 3 | Medio | 2 | Poco Probable | 1 | Irrelevante | 2 | Irrelevante |
| 2 | [SA17] Sistema de preuniversitario | Errores de los usuarios. | En varios casos el estudiante hace llenar sus datos, en un café internet, para obtener el Formulario de inscripción al Curso Pre-Universitario y no revisa que todos los datos estén correctos. | Algún(os) dato(s) incorrecto(s) del estudiante por equivocación en el taypeo. | 3 | 4 | 3 | 3 | Medio | 5 | Cierta / Inminente | 1 | Irrelevante | 5 | Bajo |
| 3 | [RC1] Internet | Corte de suministro eléctrico. | Corte de energía eléctrica prolongada puede producir la interrupción de la conexión en línea. | Interrupción de los procesos u operaciones en línea de la institución por corte prolongado de energía eléctrica. | 4 | 2 | 2 | 3 | Medio | 3 | Probable | 3 | Moderado | 9 | Medio |
| 4 | Servidores | Avería de origen físico o lógico. | Servidores sin reemplazo cuando cumplan su ciclo de vida. Ataque mediante internet. | Fallas de hardware. Código malicioso, virus o similar. | 4 | 5 | 4 | 4 | Alto | 4 | Probable | 5 | Crítico | 20 | Crítico |
| 5 | Equipamiento auxiliar del Data Center | Avería de origen físico o lógico | Equipamiento auxiliar sin reemplazo y cuya interrupción de funcionamiento puede ocasionar daños físicos y/o lógicos en los servidores. | Falla(s) de hardware. | 5 | 4 | 2 | 4 | Alto | 4 | Muy Probable | 5 | Crítico | 20 | Crítico |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 6 | Equipo de Computación | ➢ Avería de origen físico o lógico.<br>➢ Corte de suministro eléctrico.<br>➢ Condiciones inadecuadas de temperatura o humedad.<br>➢ Degradación de los soportes de almacenamiento de la información.<br>➢ Difusión de software dañino. | ➢ Equipos computacionales en mal estado, que ocasionan la interrupción temporal de operatividad, mientras son reemplazados.<br>➢ Interrupción de operaciones que afecta en la atención a los usuarios o clientes.<br>➢ Equipos de computación sin mantenimiento.<br>➢ Pérdida de la información por fallas del disco duro y falta de copias de seguridad.<br>➢ Algunos equipos de computación no cuentan con Antivirus. | ➢ Falta de funcionamiento de hardware.<br>➢ Falta de funcionamiento de software.<br>➢ Susceptibilidad a la humedad, el polvo y la suciedad.<br>➢ Desgaste o falla en los soportes de almacenamiento, que pueden ocasionar daños o pérdida de la información.<br>➢ Alteración del normal funcionamiento por código malicioso. | 3 | 3 | 2 | 3 | Medio | 3 | Probable | 3 | Moderado | 9 | Medio |
| 7 | Red de Telecomunicaciones | Fallo de servicios de comunicaciones | ➢ Fallos por deterioro de dispositivos de red o por agotamiento de recursos.<br>➢ Cables de red con mala conexión. | ➢ Fallo en hardware o software.<br>➢ Fallo en la conexión de cables de red. | 4 | 3 | 2 | 3 | Medio | 2 | Poco Probable | 3 | Moderado | 6 | Bajo |
| 8 | Sistemas de Información | ➢ Deficiencias en la organización, en algunos casos la atención de solicitudes de certificaciones, historiales, legalizaciones, entre otros similares no son atendidas por el orden secuencial de presentación.<br>➢ Modificación deliberada de la información; sin autorización escrita.<br>➢ Errores de los usuarios.<br>➢ Destrucción de la información de respaldo, que puede darse por criterio inapropiado o falta de conciencia de la seguridad de la información. | ➢ Solicitudes de certificaciones, historiales, legalizaciones, entre otros similares presentadas después son atendidas en primer lugar sin seguirse el orden secuencial de presentación, en algunos casos.<br>➢ Datos personales de los usuarios obtenidos por orden verbal y no escrita, en algunos casos.<br>➢ Modificaciones de datos sensibles por autorización verbal y no escrita y justificada, en algunos casos.<br>➢ En algunos casos datos introducidos o modificados sin documento(s) o documentación física de respaldo.<br>➢ La información física de respaldo puede ser destruida por ser considerada de fecha pasada y no importante ante un criterio personal inapropiado o desconocimiento acerca de la seguridad de la información. | ➢ Atención a solicitudes de certificaciones, historiales, legalizaciones, entre otros similares sin seguir el orden secuencial de presentación, en algunos casos.<br>➢ Obtención de datos personales de los usuarios por orden verbal y no escrita, en algunos casos.<br>➢ Ausencia de autorización escrita y justificada en modificaciones de datos sensibles, en algunos casos.<br>➢ Ausencia de documentos físicos de respaldo en la introducción o modificación de datos, en algunos casos.<br>➢ Información física de respaldo que puede ser eliminada por criterio personal o falta de conciencia acerca de la seguridad de la información. | 4 | 4 | 3 | 4 | Alto | 3 | Probable | 5 | Crítico | 15 | Alto |