*InFo-Cyber. Journal of Cybersecurity and Digital Forensics.*
Volumen 1, Número 1. Año 2025. ISSN: en trámite
https://revistas.ufasta.edu.ar/index.php/InFoCyber/index

INFO-CYBER CYBERSECURITY AND DIGITAL FORENSICS JOURNAL

# Matriz de Riesgos de la Seguridad Informática para Laboratorios de Informática Forense

*Computer Security Risk Matrix for Computer Forensic Laboratories*

**Herminia B. Parra de Gallo**
Universidad Católica de Salta (Argentina).
bgallo@ucasal.edu.ar
https://orcid.org/0000-0002-3230-3108

**Fernando Greco**
Universidad Fasta, Buenos Aires (Argentina).
fmartingreco@ufasta.edu.ar
https://orcid.org/0009-0007-5248-7745

**Mariela Ambrústolo**
Universidad Nacional de Mar del Plata (Argentina).
marielaambrustolo@ufasta.edu.ar
https://orcid.org/0009-0002-3072-2066

**Adolfo E. Onaine**
Universidad Nacional de Mar del Plata (Argentina).
adolfoeduardo.onaine@ufasta.edu.ar
https://orcid.org/0000-0001-9532-9631

**Marina Migueles**
Universidad Nacional de Mar del Plata (Argentina).
marinamigueles@ufasta.edu.ar
https://orcid.org/0009-0008-2652-0959

**Artículo de Investigación**
Recibido: 24-04-2025. Aceptado: 14-5-2025 Publicado: 03-03-2026



*Universidad FASTA. Facultad de ingeniería; Mar del*

## Resumen

El presente trabajo tiene por objetivo la descripción del proceso realizado para la identificación, análisis y gestión de los riesgos tecnológicos a los que estaría expuesto un Laboratorio de Informática Forense (LIF), tomando como referencia la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información). Basada en la norma ISO/IEC 31000, MAGERIT se presenta como una herramienta de gran utilidad para el estudio del riesgo en la infraestructura tecnológica de cualquier organización. Siguiendo los lineamientos generales de esta metodología y con la adaptación necesaria para el caso, se muestra como resultado la Matriz de Riesgo Tecnológico que debe considerarse para un LIF.

## Palabras clave

ciberataque, ciberseguridad, mitigación del riesgo, sitio web

## Abstract

*The objective of this work is to describe the process carried out for the identification, analysis and management of technological risks to which a Forensic Computing Laboratory (LIF) would be exposed, taking as reference the MAGERIT methodology (Methodology for Analysis and Risk Management of Information Systems). Based on the ISO/IEC 31000 standard, MAGERIT is presented as a very useful tool for studying risk in the technological infrastructure of any organization. The general guidelines of this methodology are followed and with the necessary adaptation for the case, the Technological Risk Matrix that must be considered for a LIF is shown as a result.*

## Keywords

*cyberattack, cybersecurity, risk mitigation, website.*

Herminia Beatriz Parra de Gallo. Especialista en Informática Forense, Dra. en Ingeniería Mención Sistemas de Información, Master en Administración de Negocios, Ingeniera en Computación. Con una extensa carrera académica como docente e investigadora en la Universidad Católica De Salta (Argentina) reviste la categoría de investigador independiente "b" (CI-UCASAL), y es Directora del Grupo de I+D+i de Forensia Digital y Ciberseguridad de esa institución, grupo abocado al desarrollo de proyectos de i+d interinstitucionales con universidades nacionales y latinoamericanas. Es además, Directora del Instituto de Estudios Interdisciplinarios de Ingeniería de la Facultad de Ingeniería de la UCASAL y Directora de la carrera de Especialización en Administración de Bases de Datos de UCASAL. Participa en la formación de recursos humanos impartiendo cursos de posgrado y como docente de carreras de grado y posgrado en UFASTA (Argentina), UTN-FRSF (Argentina), UTN-FRC (Argentina), UTN-FRCU (Argentina), UNIVA (México), UNISANGIL (Colombia), Universidad Católica de Colombia (Colombia), UniTECH (España). Perito Informático de Parte. Consultora en Proyectos Tecnológicos Críticos.

Fernando Greco. Es Ingeniero en Informática de la Universidad FASTA. Es Instructor Informático y Perito Oficial en el Ministerio Público de la Provincia de Buenos Aires. Es Investigador del InFo-Lab (Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense del Ministerio Público de la Provincia de Buenos Aires, Municipio de General Pueyrredon y Universidad FASTA). Es Profesor Titular de la cátedra de Informática Aplicada de la Licenciatura en Criminalidad, en la Facultad de Ciencias Jurídicas y Sociales, y Jefe de Trabajos Prácticos en la cátedra de Informática y Derecho, en la Facultad de Ingeniería de la Universidad FASTA. Participa como investigador en el Grupo de Investigación en Informática Forense de la Facultad de Ingeniería de la Universidad FASTA. Es coautor del Libro "El rastro digital del delito" - Universidad FASTA (2017).

Mariela Ambrústolo. Ingeniera Química egresada de la Universidad Nacional de Mar del Plata y Asesora en Tecnologías de Gestión por la Universidad Nacional General Sarmiento. Directora del grupo de investigación y extensión Gestión Integrada, Personas y Mejora Continua (GIPMeCo) en la Facultad de Ingeniería de UNMDP, y Profesora Asociada con dedicación exclusiva desde 1999 en materias vinculadas a sistemas de gestión y mejora continua, además de dictar clases en la Universidad Fasta. Ha sido evaluadora en múltiples ediciones del Premio Nacional a la Calidad y del Premio Iberoamericano de la Calidad. Co-dirige proyectos relacionados con sistemas integrados de gestión para laboratorios de informática forense y participa activamente en proyectos de extensión, capacitación y consultoría tecnológica. Integra el equipo directivo de SAMECO y coorganiza los Encuentros Regionales de Mejora Continua "Mar y Sierras", colaborando con diversas instituciones. Es autora de publicaciones académicas y científicas en su área de especialización.

Marina Migueles. Ingeniera Química (Universidad Nacional de Mar del Plata)/ Especialista en Higiene y Seguridad en el Trabajo. JTP Titular de las asignaturas de Gestión de Calidad y Sistemas de Gestión y Mejora Continua con dedicación exclusiva.Profesor Adjunta en la Asignatura Gestión Integrada de la Seguridad e Higiene en el Trabajo de la Licenciatura en Higiene y Seguridad en el trabajo, modalidad a distancia, en Universidad Fasta (2012-actual). Integrante del Grupo de Investigación y extensión en Gestión Integrada, Personas y Mejora Continua (GIPMeCo) del Departamento de Ingeniería Industrial de la Facultad de Ingeniería de la Universidad Nacional de Mar del Plata (UNMDP). Colabora en proyectos de implementación de Sistemas Integrados de Gestión para Laboratorios de Informática Forense en conjunto con UFASTA y UCASAL. Participa en proyectos de extensión y actividades de transferencias en temáticas de sistemas de gestión, calidad, y mejora continua. Forma parte de comités organizadores, académicos en eventos regionales y nacionales de mejora continua nacionales. Socio activo de SAMECO Sociedad Argentina Pro-Mejoramiento Continuo e integrante del equipo organizador de la Comisión de Intercambio de Experiencias de Enseñanza de la Mejora Continua en la Universidad - SAMECO. Autora en colaboración con el equipo de trabajo de material con finalidad docente y científica. Participación en diferentes congresos científicos con trabajos referidos a calidad, mejora continua e investigaciones sobre la enseñanza superior.

Adolfo Eduardo Onaine. Ingeniero Electricista (UNMdP), Master Internacional en Dirección de Empresas (UNSAL-DEUSTO) y Doctor en Ingeniería mención Industrial (UNLZ). Profesor Titular en la carrera de Ingeniería Industrial (UNMdP). Profesor y miembro de los Comités Académicos en las carreras Especialista Gestión de la Tecnología y la Innovación (UNMdP) y Maestría en Gestión Internacional de la Tecnología y la Innovación (UNMdP y UNLu). Integra Comisiones Asesoras de Concursos docentes en las Universidades Nacionales de Mar del Plata, del Sur, del Centro de la Provincia de Buenos Aires, de Córdoba, de Luján, del Litoral, del Nordeste, de Salta y la UTN. En Investigación y Extensión, es Director del Grupo de Investigación y Extensión *Investigación Operativa, Gestión Industrial y Desarrollo Regional* (GIOGIDeR) y Codirector del Programa de "Fortalecimiento de pequeños productores de la agricultura familiar como fuente de sustento y desarrollo regional" - UNMdP. Integra Proyectos de implementación de Sistemas Integrados de Gestión para Laboratorios de Informática Forense con UFASTA y UCASAL. Participa en eventos regionales, nacionales e internacionales como miembro de Comités Organizadores y Académicos, moderador, expositor de trabajos y disertante; en actividades de Extensión Universitaria; y en Asistencia Técnica a Instituciones y Empresas regionales. Posee publicaciones en revistas y trabajos presentados en congresos regionales, nacionales e internacionales.

## I. Introducción

El presente trabajo describe la matriz de riesgo tecnológico desarrollada para un Laboratorio de Informática Forense (LIF) a partir de la aplicación de la metodología MAGERIT [1].

Una matriz de riesgo tecnológico es un insumo importante para el desarrollo de un sistema de calidad y de seguridad informática para un LIF. Así, esta matriz se enmarca en la definición de un sistema de gestión integrado, que aborde los criterios generales de calidad de la ISO/IEC 9001:2015 y aquellos referidos a la seguridad de la información explicitados en la ISO/IEC 27001:2022. En [2] se explican las características generales del proyecto de integración de ambas normas. Por una parte, la norma ISO 9001:2015 permite la implementación de un sistema de gestión de la calidad basada en la mejora continua, mientras que la ISO/IEC 27001:2022 considera los procesos necesarios para preservar las características de confidencialidad, integridad y disponibilidad de la información, teniendo en cuenta la gestión de riesgos tecnológicos y no tecnológicos involucrados y que deben gestionarse adecuadamente.

Considerando las características propias de un laboratorio que brinda servicios de informática forense, se identifican los riesgos, las amenazas y el nivel de criticidad de cada componente, sea este de carácter tecnológico o no tecnológico. Se define además la degradación que podría sufrir cada componente ante el impacto del riesgo, así como las acciones de salvaguarda que permiten definir el riesgo residual. Por último, se toman de la norma ISO/IEC 27001:2015 los controles de seguridad que sirven de contención y control de las situaciones de riesgo identificadas.

Este trabajo tiene la siguiente estructura: en la Sección II se describe la metodología MAGERIT, en la Sección III se enuncian las características distintivas de un LIF, en la Sección IV se describe cómo se aplica la citada metodología para identificar y tratar los riesgos tecnológicos de un LIF, y por último, en la Sección V se enuncian las conclusiones de este trabajo.

## II. La metodología MAGERIT

A partir de la norma ISO/IEC 31000, MAGERIT define las actividades, estrategias, técnicas y herramientas adecuadas para la implementación de un proceso de gestión de riesgos en el contexto tecnológico de una empresa o institución.

En [1] se indican los objetivos de MAGERIT: a) Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos; b) Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC); c) Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control; y d) Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

Las características distintivas de MAGERIT incluyen:

- Enfoque Integral: la metodología permite cubrir todas las instancias del análisis y gestión del riesgo, desde la valoración de los activos hasta la aplicación de las medidas de seguridad.
- Adaptabilidad y flexibilidad: aunque inicialmente fue prevista para su uso en el contexto de la administración pública española, es reconocida por su capacidad para implementarse en cualquier organización, ajustándose a las necesidades específicas de cada caso.
- Proceso Estructurado y sistemático: MAGERIT incluye una serie de pasos perfectamente definidos que ordenan el proceso de identificación, análisis y gestión de riesgos tecnológicos.
- Valoración de las instancias de documentación y seguimiento: la metodología enfatiza la importancia de mantener procesos de documentación actualizados y continuos, a fin de alinear la gestión de la seguridad con la evolución de las amenazas y los cambios del entorno organizacional.

La metodología MAGERIT propone un espacio de trabajo claro y detallado para la gestión proactiva de los riesgos tecnológicos relativos a la seguridad informática en una organización, promoviendo además una cultura de la seguridad y la mejora continua. Ejemplos de aplicación de esta metodología se pueden ver en [3] y [4].

## III. El laboratorio de informática forense

De [5] se toman los conceptos de base para describir lo que es un Laboratorio de Informática Forense.

Un LIF es un espacio tecnológico destinado al tratamiento de la probable evidencia digital para dar respuesta a los requerimientos de quienes requieran los servicios de informática forense.

Es importante considerar la identidad del LIF basada en la misión, visión y valores, que marcan el ámbito de desarrollo de las actividades forenses. Ya sea que se trate de un LIF de carácter gubernamental (usualmente presente en áreas del Ministerio Público Fiscal o de las Fuerzas de Seguridad del Estado), o bien se conforma como un espacio privado que ofrece servicios

forenses especialmente relativos a la investigación de incidentes de seguridad informática.

Los servicios que ofrece un LIF abarcan 3 tareas generales: asesoramiento, investigación digital y actividades periciales. El desarrollo de estos servicios dependerá entonces de la identidad del LIF, en cuanto a si es un ámbito propio de la justicia o un espacio privado.

También se deben distinguir los servicios genéricos de los específicos. Los primeros se refieren a una prestación sin especificar una tecnología particular y concreta (adquisición de una copia forense, por ejemplo), mientras que los servicios específicos tratan aquellas prestaciones relativas a una tecnología precisa y limitada (adquisición de imágenes de una tarjeta SD, por ejemplo). En el caso de los servicios específicos, interesa identificar si el LIF cuenta con recursos humanos y técnicos relativos a la tecnología que se abordará.

Desde el punto de vista de la infraestructura general, un LIF debe radicarse en un espacio físico determinado, especialmente diseñado para los servicios que se ofrecerán. Respecto de la infraestructura tecnológica, el LIF contará con una arquitectura básica para el procesamiento de la evidencia digital, más el agregado de componentes y herramientas forenses específicas para los servicios específicos que se ofrecerán.

Más allá de los elementos que integren un LIF, se trata de una infraestructura tecnológica sobre la cual es importante considerar los riesgos que pueden impactar en los servicios ofrecidos.

## IV. APLICACIÓN DE MAGERIT AL CASO DE ESTUDIO

Teniendo presente los requerimientos particulares del caso, referidos a la identificación de riesgos para un LIF, se toma de la metodología citada aquellos elementos que resulten de utilidad para la elaboración de la MATRIZ DE RIESGOS TECNOLÓGICOS para este tipo de instalaciones.

El trabajo realizado incluyó las siguientes etapas:

- Análisis cualitativo de la infraestructura tecnológica para identificar los niveles de probabilidad e impacto del riesgo.
- Determinación de las amenazas internas y externas a las cuales está expuesta la infraestructura tecnológica.
- Determinación de las protecciones dispuestas y su control
- Elaboración de la Matriz de Riesgos Tecnológicos para un Laboratorio de Informática Forense

Cada una de estas etapas se describen a continuación.

### *A. Análisis cualitativo de la Infraestructura Tecnológica*

Se realizó el inventario de todos los componentes o activos de un LIF, considerando no solamente los principales elementos tecnológicos (*hardware*, *software*, datos), sino también otros componentes necesarios para la actividad forense (personal, instalaciones edilicias propias para un laboratorio de estas características, entre otras), resultando todo ello en una ESTRUCTURA BASE PARA EL INVENTARIO TECNOLÓGICO que se muestra en la Fig 1.

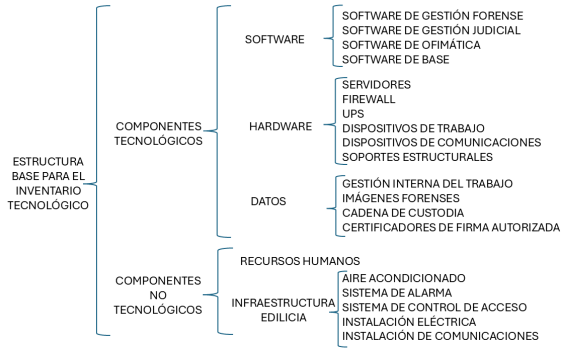


*Fig 1. Estructura Base para el Inventario Tecnológico.*

Esta clasificación permite ordenar los componentes a fin de estudiarlos y analizarlos mediante la aplicación de criterios de riesgos propios para cada elemento, teniendo presente las particularidades de estos.

### *B. Determinación de las Amenazas Internas y Externas*

En esta etapa se procedió a la identificación previa de un conjunto de factores que, una vez definidos para cada componente, permitieron determinar las amenazas a las que está expuesto un LIF. Los pasos seguidos en esta etapa son los siguientes:

#### *B.1. Valoración del Activo*

El estudio se inicia con un proceso de VALORACIÓN DEL ACTIVO, que permite cuantificar de manera numérica la importancia o aporte del componente en un Laboratorio de Informática Forense. Para cada elemento de la Estructura Base se realizaron las siguientes definiciones:

- Identificación del VALOR DEL ACTIVO TECNOLÓGICO, mediante la asignación de un puntaje de contribución a los criterios de integridad, confidencialidad y disponibilidad. Por las características propias de un LIF, a estos criterios se sumó el de trazabilidad.

- Identificación del VALOR DEL ACTIVO NO TECNOLÓGICO, mediante la asignación de un puntaje de contribución a los criterios de mayor impacto para el caso de estudio. Particularmente, los criterios para la valoración de estos componentes se definieron en función de las

características de cada tipo de componente:

- Para los recursos humanos, los criterios propuestos fueron: competencias requeridas, adaptabilidad a la tarea y costo de reemplazo.
- -Para los componentes de infraestructura edilicia, los criterios propuestos fueron: necesidad, costos de mantenimiento y costo de reemplazo.

Esta fase concluye con un único valor de cuantificación del activo que resulta del promedio de los valores considerados en los distintos criterios.

### *B.2.Nivel de Criticidad*

Realizada la valoración indicada, se identificó el NIVEL DE CRITICIDAD de cada componente, asociando este concepto a la relevancia que el activo presenta en el caso de un LIF. El nivel de criticidad de un componente es una medida de cuán esencial es este para el funcionamiento correcto del sistema y qué consecuencias tendría su fallo o mal funcionamiento. Se consideraron 4 opciones para el Nivel de Criticidad:

- Baja: cuando su degradación presenta un mínimo impacto para la operatividad segura del LIF.
- Alta: si existen peligros considerables que impactan de manera directa en la operatividad segura del LIF.
- Muy Alta: cuando los peligros significan una suspensión del servicio o funcionamiento del LIF.

De acuerdo con esta clasificación, se identifica el nivel de criticidad de los componentes y se resumen en la Tabla I para los componentes tecnológicos y en la Tabla II para los no tecnológicos.

TABLA I

NIVEL DE CRITICIDAD DE LOS COMPONENTES TECNOLÓGICOS

| | |
|---|---|
| | *Software* |
| Criticidad Baja | *Software* de Base |
| Criticidad Alta | Servidor File System<br>Otros Servidores |
| Criticidad Muy Alta | *Software* de Gestión Judicial<br>*Software* Básico de Gestión Forense |
| | *Hardware* |
| Criticidad Baja | Equipamiento de Repuesto<br>Impresoras<br>*Switch*<br>Dispositivo para conexión a internet<br>Soportes Estructurales |
| Criticidad Alta | UPS |
| Criticidad Muy Alta | Servidor de *Backcup*<br>Servidor de *Backcup* de Imágenes Forenses<br>*Firewalls*<br>Puestos de trabajo<br>Duplicadores Forenses<br>Dispositivos para resguardo de datos |
| | Datos |
| Criticidad Baja | -.- |
| Criticidad Alta | -.- |
| Criticidad Muy Alta | Datos para la Gestión Interna de las actividades forenses<br>Imágenes Forenses<br>Cadena de Custodia<br>Certificación de Firma de documentos |

TABLA II

NIVEL DE CRITICIDAD DE LOS COMPONENTES NO TECNOLÓGICOS

| | |
|---|---|
| | Recursos Humanos |
| Criticidad Baja | Formación, Conocimientos y Experiencia en Ciencias del Derecho<br>Formación, Conocimientos y Experiencia en investigación criminal |
| Criticidad Alta | Formación, Conocimientos y Experiencia en Informática Forense<br>Comportamiento Profesional y Ético |
| Criticidad Muy Alta | -.- |
| | Infraestructura Edilicia |
| Criticidad Baja | Alarma monitoreada<br>Seguridad Física de los efectos<br>Herramientas de taller |
| Criticidad Alta | Aire acondicionado<br>Infraestructura Eléctrica |
| Criticidad Muy Alta | -.- |

### *C. Identificación de Amenazas y Degradación del Activo*

Considerando tanto las amenazas internas como externas a la que puede estar expuesta la tecnología en general, se identificaron aquellas que particularmente representan una amenaza concreta para un LIF. De ese modo, se logra un listado de amenazas que impactan en uno o varios de los activos tecnológicos y no tecnológicos definidos, identificando en cada uno de ellos la degradación o impacto en el rendimiento del activo si es que la amenaza se concreta. Estos valores se pueden observar en la Tabla IV.

### *D. Evaluación del Riesgo*

La *probabilidad de ocurrencia* mide la frecuencia o posibilidad de que un riesgo ocurra, mientras que el *impacto* mide la gravedad de las consecuencias si el riesgo se materializa. Considerando la probabilidad de ocurrencia de la amenaza identificada, así como el impacto que produciría en cada caso, se identifica el riesgo según la matriz de evaluación que se indica en la Tabla III. Se puede evaluar en función de los efectos en las características de confidencialidad, integridad y disponibilidad que deben regir la operatividad de un LIF.

TABLA III:

MATRIZ DE EVALUACIÓN DE RIESGO

| | | IMPACTO | | |
|---|---|---|---|---|
| | | BAJO | MEDIO | ALTO |
| PROBABILIDAD DE OCURRENCIA | BAJA | TRIVIAL | TOLERABLE | MODERADO |
| | MEDIA | TOLERABLE | MODERADO | IMPORTANTE |
| | ALTA | MODERADO | IMPORTANTE | CRÍTICO |

### *E. Determinación de las Protecciones y Control*

En esta etapa se definieron las acciones pertinentes para la gestión de los riesgos identificados, que básicamente se agrupan en dos tareas:

- Salvaguarda y Riesgo Residual.
- Determinación de las protecciones dispuestas y su control.

Seguidamente se describen ambas actividades.

#### *E.1.Salvaguarda y Riesgo Residual*

Una vez identificado el riesgo para cada componente, sea este tecnológico o no tecnológico, se identificaron las acciones y estrategias que permiten mitigar o reducir ese riesgo, como una manera de responder preventivamente y con antelación a la materialización del riesgo.

Usualmente, una instalación tecnológica para el procesamiento de datos (o Data Center) mantiene una estructura básica para la cual ya son conocidos los riesgos, impactos que producen y, por ende, las salvaguardas que se aplica. En el caso de un LIF, se toma en consideración esta estructura básica de un Data Center y a partir de allí se identifican las salvaguardas en la Tabla IV, considerando las amenazas y degradaciones identificadas en el paso anterior.

TABLA IV:

AMENAZAS, DEGRADACIONES Y SALVAGUARDA PARA CADA COMPONENTE

| **Componente** | **Amenaza** | **Degradación del componente o impacto en las actividades forenses** | **Salvaguarda** |
|---|---|---|---|
| Tecnológico | Acceso no autorizado | Acceso no autorizado al resto de los dispositivos vinculados a éste | Monitoreo continuo del sistema de defensa del elemento. |
| | | | Resguardo seguro del elemento. |
| | | Acceso a información no autorizada o pérdida/destrucción de esta. | Monitoreo continuo del sistema de defensa del elemento. |
| | | | Resguardo seguro del elemento. |
| | Caída de la red o del puesto de trabajo | Impedimento de acceso a los datos o aplicaciones | Monitoreo continuo del funcionamiento de la red y de los puestos de trabajo |
| | Caída de las fuentes de energía | Impedimento para utilizar el dispositivo y los vinculados a éste | Puesta en funcionamiento inmediata y automática de la UPS. Monitoreo continuo de fase y tensión de la línea estabilizada. |
| | | Impedimento para utilizar el dispositivo | Puesta en funcionamiento inmediata y automática de la UPS. Monitoreo continuo de fase y tensión de la línea estabilizada. |
| | | | Contención Institucional de las instalaciones |
| | Errores o desactualización del *software* | Mal funcionamiento del software con impacto indirecto en las actividades forenses | Corrección y/o actualización del software. Utilización de un *software* alternativo |
| | | Mal funcionamiento del software con impacto directo en las actividades forenses | Corrección y/o actualización del software. Utilización de un *software* alternativo |
| | Fallas en la seguridad física de las instalaciones | Parada total o parcial de la operatividad del laboratorio | Actualización y refuerzo de la seguridad física de las instalaciones |
| | | Acceso a información no autorizada o pérdida/destrucción de esta. | Actualización y refuerzo de la seguridad física de las instalaciones |
| | Instalación inadecuada o fallas de los soportes estructurales | Parada total o parcial de la operatividad del laboratorio | Revisión y ajuste según normas de cableado estructurado |
| | Mal funcionamiento del equipo | Impedimento para utilizar el dispositivo | Cambio del dispositivo |
| | | | Realizar el mantenimiento preventivo del dispositivo |
| | Mantenimiento inadecuado | Impedimento para utilizar el dispositivo | Cambio del dispositivo |
| | Pérdida o robo | Acceso a información no autorizada o perdida/destrucción de esta. | Mantener inventario y resguardo de los elementos |
| | | Impedimento para utilizar el dispositivo | Mantener inventario y resguardo de los elementos |
| No Tecnológico | Conocimientos insuficientes o inadecuados | Impacta en la conformación de un equipo forense actualizado y experto | Capacitación continua |
| | Hace vulnerable el sistema y las actividades forenses | Se promueve la comisión de delitos relacionados con la actividad forense. | Verificación de antecedentes previo a la designación en el cargo |

| Componente | Amenaza | Degradación del componente o impacto en las actividades forenses | Salvaguarda |
|---|---|---|---|
| | Acceso no autorizado | Acceso a información no autorizada o pérdida/destrucción de esta. | Monitoreo continuo del sistema de defensa del elemento. |
| | | | Resguardo seguro del elemento. |
| | Caída de las fuentes de energía | Parada total o parcial de la operatividad del laboratorio | Puesta en funcionamiento inmediata y automática de la UPS. Monitoreo continuo de fase y tensión de la línea estabilizada. |
| | | Impedimento para utilizar el dispositivo y los vinculados a éste | Puesta en funcionamiento inmediata y automática de la UPS. Monitoreo continuo de fase y tensión de la línea estabilizada. |
| | Fallas en la seguridad física de las instalaciones | Acceso a información no autorizada o pérdida/destrucción de esta. | Actualización y refuerzo de la seguridad física de las instalaciones |
| | Mal funcionamiento del equipo | Impedimento para utilizar el dispositivo | Cambio del dispositivo |
| | | | Realizar el mantenimiento preventivo del dispositivo |
| | Mantenimiento inadecuado | Impedimento para utilizar el dispositivo | Cambio del dispositivo |
| | Pérdida o robo | Imposibilidad de realizar tareas manuales | Mantener inventario y resguardo de los elementos |

Por último, una vez identificadas las salvaguardas existentes, se vuelve a calcular el riesgo de cada componente y, de igual manera, un nuevo riesgo —riesgo residual— que sería el que se mantiene para el componente aun con la aplicación de la acción de salvaguarda.

### *E.2. Determinación de los Controles de Seguridad de la Información*

Por las características de un LIF, se consideraron las acciones de control basadas en la aplicación de lo dispuesto en la norma ISO 27001:2012, cuyo Anexo A.1 contiene una enumeración de los *controles de seguridad de la información*, asociando una o más instancias de control a cada componente tecnológico y no tecnológico que requiera un seguimiento continuo y formal a fin de gestionar debidamente los riesgos tecnológicos emergentes.

### *F. Elaboración de la Matriz de Riesgos*

La clasificación señalada en la sección anterior identifica 3 subtipos de componentes tecnológicos: *Software*, *Hardware* y Datos; más dos tipos de componentes no tecnológicos: Recursos Humanos e Infraestructura edilicia

Para cada uno de ellos se debe desarrollar la matriz de riesgos tecnológicos. Considerando las variables señaladas en los pasos anteriores, a continuación, en las Tablas V, VI y VII se muestra la Matriz de Riesgo Tecnológico para el componente de *SOFTWARE*, y sus distintos subcomponentes, en función del valor del activo, nivel de criticidad, amenaza, riesgo, salvaguarda y control seleccionado. La Matriz de Riesgo Tecnológico completa se muestra en el ANEXO 1.

TABLA V

COMPONENTE DE *SOFTWARE* - SUBCOMPONENTE: *SOFTWARE* DE GESTIÓN JUDICIAL (SISTEMAS INSTITUCIONALES EXTERNOS AL LIF)

**Valor del Activo:** 8.3 / 10 **Nivel de Criticidad:** Muy Alto

| Amenaza | Degradación del activo | Probabilidad de ocurrencia | Impacto | Riesgo | Salvaguarda | Probabilidad Residual | Impacto Residual | Riesgo Residual | Control seleccionado (Anexo 1 - ISO 27001) |
|---|---|---|---|---|---|---|---|---|---|
| Caída de la red o del puesto de trabajo | Impedimento de acceso a los datos o aplicaciones | Media | Alto | Importante | Monitoreo continuo del funcionamiento de la red y de los puestos de trabajo | Baja | Medio | Tolerable | Los asignados a la infraestructura de comunicaciones |
| Errores o desactualización del software | Mal funcionamiento del *software* con impacto directo en las actividades forenses | Baja | Alto | Moderado | Corrección y/o actualización del software. Utilización de un software alternativo | Baja | Medio | Tolerable | 8.5 Autenticación segura 8.8 Gestión de vulnerabilidades técnicas 8.9 Gestión de la configuración 8.12 Prevención de fuga de datos 8.16 Actividades de supervisión 8.26 Requisitos de seguridad de las aplicaciones |

TABLA VI

COMPONENTE DE *SOFTWARE* - SUBCOMPONENTE: *SOFTWARE* BÁSICO DE GESTIÓN FORENSE (EXTRACCIÓN DE DATOS, ANÁLISIS DE INFORMACIÓN, SANITIZACIÓN, ENCRIPTACIÓN, OTROS)

**Valor del Activo:** 9.3 / 10 **Nivel de Criticidad:** Muy Alto

| **Amenaza** | **Degradación del activo** | **Probabilidad de ocurrencia** | **Impacto** | **Riesgo** | **Salvaguarda** | **Probabilidad Residual** | **Impacto Residual** | **Riesgo Residual** | **Control seleccionado (Anexo 1 - ISO 27001)** |
|---|---|---|---|---|---|---|---|---|---|
| Caída de la red o del puesto de trabajo | Impedimento de acceso a los datos o aplicaciones | Media | Alto | Importante | Monitoreo continuo del funcionamiento de la red y de los puestos de trabajo | Baja | Medio | Tolerable | Los asignados a la infraestructura de comunicaciones |
| Errores o desactualización del software | Mal funcionamiento del *software* con impacto directo en las actividades forenses | Baja | Alto | Moderado | Corrección y/o actualización del *software*. Utilización de un *software* alternativo | Baja | Medio | Tolerable | 8.5 Autenticación segura<br>8.8 Gestión de vulnerabilidades técnicas<br>8.9 Gestión de la configuración<br>8.12 Prevención de fuga de datos<br>8.16 Actividades de supervisión<br>8.26 Requisitos de seguridad de las aplicaciones |

TABLA VII

COMPONENTE DE *SOFTWARE* - SUBCOMPONENTE: SOFTWARE DE BASE (SISTEMA OPERATIVO, OFIMÁTICA)

**Valor del Activo:** 5/ 10 **Nivel de Criticidad:** Alto

| **Amenaza** | **Degradación del activo** | **Probabilidad de ocurrencia** | **Impacto** | **Riesgo** | **Salvaguarda** | **Probabilidad Residual** | **Impacto Residual** | **Riesgo Residual** | **Control seleccionado (Anexo 1 - ISO 27001)** |
|---|---|---|---|---|---|---|---|---|---|
| Caída de la red o del puesto de trabajo | Impedimento de acceso a los datos o aplicaciones | Baja | Alto | Moderado | Monitoreo continuo del funcionamiento de la red y de los puestos de trabajo | Baja | Medio | Tolerable | Los asignados a la infraestructura de comunicaciones |
| Errores o desactualización del software | Mal funcionamiento del *software* con impacto indirecto en las actividades forenses | Baja | Alto | Moderado | Corrección y/o actualización del *software*. Utilización de un *software* alternativo | Baja | Medio | Tolerable | 8.5 Autenticación segura<br>8.8 Gestión de vulnerabilidades técnicas<br>8.9 Gestión de la configuración<br>8.12 Prevención de fuga de datos<br>8.16 Actividades de supervisión<br>8.18 Uso de programas de utilidad privilegiados<br>8.19 Instalación de software en sistemas operativos<br>8.26 Requisitos de seguridad de las aplicaciones |

## V. CONCLUSIONES

Definida la matriz de riesgos tecnológicos de un LIF, corresponde validar el modelo construido aplicándolo a casos ejemplos de un laboratorio gubernamental y de un laboratorio privado, a fin de confirmar que se han contemplado todas las variantes que impactan en el riesgo —principalmente las referidas a las amenazas—, de modo que sea posible nutrir el modelo con las propuestas de mejoras que pudieran surgir. Además de estas consideraciones, cabe tener presentes las acciones de salvaguarda que sean posibles de implementar, ya que estas usualmente dependen de cuestiones presupuestarias más que organizativas.

Se considera que la utilización de la metodología MAGERIT como guía para el estudio de los riesgos tecnológicos de un LIF es un aporte secundario, pero rico en cuanto a la experiencia lograda por parte de los integrantes del proyecto.

Como línea de continuidad para el análisis del riesgo tecnológico en un LIF, se puede estudiar la inclusión de tecnologías de *cloud computing* como base para la actividad diaria del LIF, así como el análisis del riesgo que implica la utilización de tecnologías emergentes como Big Data,

Inteligencia Artificial y Blockchain, entre otras, y analizar ese escenario desde la matriz de riesgos tecnológicos de la seguridad informática propuesta, con los ajustes que resultaran

necesarios.

## REFERENCIAS

[1] Ministerio de Administraciones Públicas, *MAGERIT v3: Libro 1, Método*, Madrid: Ministerio de Hacienda y Administraciones Públicas, 2012. [En línea]. Disponible: https://administracionelectronica.gob.es/pae_Home/dam/jcr:fb373672-f804-4d05-8567-2d44b3020387/2012_Magerit_v3_libro1_metodo_es_NIPO_630-12-171-8.pdf

[2] M. Ambrústolo, A. Onaine y M. Migueles, *Integración Sistemas de Gestión de la Calidad y Seguridad de la Información*. Mar del Plata: Universidad Nacional de Mar del Plata, 2023.

[3] M. Paez y D. Portilla, "La Metodología Magerit para la evaluación de riesgos de activos de información, caso Instituto Superior Tecnológico Nelson Torres: Evaluación de Riesgos," *Nexos Científicos*, vol. 8, no. 1, pp. 1-11, 2024.

[4] M. F. Molina-Miranda, "Análisis de riesgos de centro de datos basado en la herramienta pilar de Magerit," *Espirales Revista Multidisciplinaria de Investigación*, vol. 1, no. 11, 2017.

[5] A. H. Di Iorio *et al.*, *Guía técnica para el diseño, implementación y gestión de laboratorios de informática forense*, 1a ed. Mar del Plata: Universidad FASTA, 2019. [En línea]. Disponible: https://info-lab.org.ar/images/pdf/LibroGuiaTcnica.pdf

# ANEXO – MATRIZ DE RIESGO TECNOLÓGICO DEL LIF

**SOFTWARE:**

**Subcomponente:** Software de Gestión Judicial (sistemas institucionales externos al LIF)

**Valor del Activo:** 8.3 / 10 **Nivel de Criticidad:** Muy Alto

| Amenaza | Degradación del activo | Probabilidad de ocurrencia | Impacto | Riesgo | Salvaguarda | Probabilidad Residual | Impacto Residual | Riesgo Residual | Control seleccionado (Anexo 1 - ISO 27001) |
|---|---|---|---|---|---|---|---|---|---|
| Caída de la red o del puesto de trabajo | Impedimento de acceso a los datos o aplicaciones | Media | Alto | Importante | Monitoreo continuo del funcionamiento de la red y de los puestos de trabajo | Baja | Medio | Tolerable | Los asignados a la infraestructura de comunicaciones |
| Errores o desactualización del software | Mal funcionamiento del *software* con impacto directo en las actividades forenses | Baja | Alto | Moderado | Corrección y/o actualización del software. Utilización de un software alternativo | Baja | Medio | Tolerable | 8.5 Autenticación segura<br>8.8 Gestión de vulnerabilidades técnicas<br>8.9 Gestión de la configuración<br>8.12 Prevención de fuga de datos<br>8.16 Actividades de supervisión<br>8.26 Requisitos de seguridad de las aplicaciones |

**Subcomponente:** Software Básico de Gestión Forense (Extracción de Datos, Análisis de Información, Sanitización, Encriptación, otros)

**Valor del Activo:** 9.3 / 10 **Nivel de Criticidad:** Muy Alto

| Amenaza | Degradación del activo | Probabilidad de ocurrencia | Impacto | Riesgo | Salvaguarda | Probabilidad Residual | Impacto Residual | Riesgo Residual | Control seleccionado (Anexo 1 - ISO 27001) |
|---|---|---|---|---|---|---|---|---|---|
| Caída de la red o del puesto de trabajo | Impedimento de acceso a los datos o aplicaciones | Media | Alto | Importante | Monitoreo continuo del funcionamiento de la red y de los puestos de trabajo | Baja | Medio | Tolerable | Los asignados a la infraestructura de comunicaciones |
| Errores o desactualización del software | Mal funcionamiento del *software* con impacto directo en las actividades forenses | Baja | Alto | Moderado | Corrección y/o actualización del software. Utilización de un software alternativo | Baja | Medio | Tolerable | 8.5 Autenticación segura<br>8.8 Gestión de vulnerabilidades técnicas<br>8.9 Gestión de la configuración<br>8.12 Prevención de fuga de datos<br>8.16 Actividades de supervisión<br>8.26 Requisitos de seguridad de las aplicaciones |

**Subcomponente:** Software de Base (Sistema Operativo, Ofimática)

**Valor del Activo:** 5/ 10 **Nivel de Criticidad:** Alto

| Amenaza | Degradación del activo | Probabilidad de ocurrencia | Impacto | Riesgo | Salvaguarda | Probabilidad Residual | Impacto Residual | Riesgo Residual | Control seleccionado (Anexo 1 - ISO 27001) |
|---|---|---|---|---|---|---|---|---|---|
| Caída de la red o del puesto de trabajo | Impedimento de acceso a los datos o aplicaciones | Baja | Alto | Moderado | Monitoreo continuo del funcionamiento de la red y de los puestos de trabajo | Baja | Medio | Tolerable | Los asignados a la infraestructura de comunicaciones |
| Errores o desactualización del software | Mal funcionamiento del *software* con impacto indirecto en las actividades forenses | Baja | Alto | Moderado | Corrección y/o actualización del software. Utilización de un software alternativo | Baja | Medio | Tolerable | 8.5 Autenticación segura<br>8.8 Gestión de vulnerabilidades técnicas<br>8.9 Gestión de la configuración<br>8.12 Prevención de fuga de datos<br>8.16 Actividades de supervisión<br>8.18 Uso de programas de utilidad privilegiados<br>8.19 Instalación de *software* en sistemas operativos<br>8.26 Requisitos de seguridad de las aplicaciones |

***HARDWARE*:**

**Subcomponente:** Servidores – File System

**Valor del Activo:** 6.3 / 10 **Nivel de Criticidad:** Alto

| Amenaza | Degradación del activo | Probabilidad de ocurrencia | Impacto | Riesgo | Salvaguarda | Probabilidad Residual | Impacto Residual | Riesgo Residual | Control seleccionado (Anexo 1 - ISO 27001) |
|---|---|---|---|---|---|---|---|---|---|
| Mal funcionamiento del equipo | Impedimento para utilizar el dispositivo | Media | Alto | Importante | Realizar el mantenimiento preventivo del dispositivo. Cambio del dispositivo | Baja | Medio | Tolerable | 7.13 Mantenimiento de equipos |
| Acceso no autorizado | Acceso a información no autorizada o pérdida/-destrucción de esta | Media | Alto | Importante | Monitoreo continuo del sistema de defensa del elemento | Baja | Medio | Tolerable | 5.15 Control de acceso<br>5.17 Información de autenticación<br>5.18 Derechos de acceso<br>8.3 Restricción de acceso a la información<br>8.7 Protección contra *malware* |
| Caída de las fuentes de energía | Impedimento para utilizar el dispositivo y los vinculados a éste | Baja | Alto | Moderado | Puesta en funcionamiento inmediata y automática de la UPS. Monitoreo continuo de fase y tensión de la línea estabilizada. | Baja | Medio | Tolerable | 5.29 Seguridad de la información durante la interrupción |

**Subcomponente:** Servidores – Servidor de Backup

**Valor del Activo:** 8.3 / 10 **Nivel de Criticidad:** Muy Alto

| Amenaza | Degradación del activo | Probabilidad de ocurrencia | Impacto | Riesgo | Salvaguarda | Probabilidad Residual | Impacto Residual | Riesgo Residual | Control seleccionado (Anexo 1 - ISO 27001) |
|---|---|---|---|---|---|---|---|---|---|
| Mal funcionamiento del equipo | Impedimento para utilizar el dispositivo | Media | Alto | Importante | Realizar el mantenimiento preventivo del dispositivo. Cambio del dispositivo | Baja | Medio | Tolerable | 7.13 Mantenimiento de equipos |
| Acceso no autorizado | Acceso a información no autorizada o perdida/destrucción de esta | Media | Alto | Importante | Monitoreo continuo del sistema de defensa del elemento | Baja | Medio | Tolerable | 5.15 Control de acceso<br>5.17 Información de autenticación<br>5.18 Derechos de acceso<br>8.3 Restricción de acceso a la información<br>8.7 Protección contra *malware*<br>8.13 Copia de seguridad de la información |
| Caída de las fuentes de energía | Impedimento para utilizar el dispositivo y los vinculados a éste | Baja | Alto | Moderado | Puesta en funcionamiento inmediata y automática de la UPS. Monitoreo continuo de fase y tensión de la línea estabilizada. | Baja | Medio | Tolerable | 5.29 Seguridad de la información durante la interrupción |

**Subcomponente:** Servidores – Otros Servidores (Calendario, Correos, Mirror, etc)

**Valor del Activo:** 7.5 / 10 **Nivel de Criticidad:** Alto

| Amenaza | Degradación del activo | Probabilidad de ocurrencia | Impacto | Riesgo | Salvaguarda | Probabilidad Residual | Impacto Residual | Riesgo Residual | Control seleccionado (Anexo 1 - ISO 27001) |
|---|---|---|---|---|---|---|---|---|---|
| Caída de las fuentes de energía | Impedimento para utilizar el dispositivo y los vinculados a éste | Baja | Alto | Moderado | Puesta en funcionamiento inmediata y automática de la UPS. Monitoreo continuo de fase y tensión de la línea estabilizada. | Baja | Medio | Tolerable | 5.29 Seguridad de la información durante la interrupción |

**Subcomponente:** Servidores – Servidor de Backup de Imágenes Forenses
**Valor del Activo:** 10 / 10 **Nivel de Criticidad:** Muy Alto

| Amenaza | Degradación del activo | Probabilidad de ocurrencia | Impacto | Riesgo | Salvaguarda | Probabilidad Residual | Impacto Residual | Riesgo Residual | Control seleccionado (Anexo 1 - ISO 27001) |
|---|---|---|---|---|---|---|---|---|---|
| Mal funcionamiento del equipo | Impedimento para utilizar el dispositivo | Media | Alto | Importante | Realizar el mantenimiento preventivo del dispositivo. Cambio del dispositivo | Baja | Medio | Tolerable | 7.13 Mantenimiento de equipos |
| Acceso no autorizado | Acceso a información no autorizada o pérdida/ destrucción de esta | Media | Alto | Importante | Monitoreo continuo del sistema de defensa del elemento | Baja | Medio | Tolerable | 5.15 Control de acceso<br>5.17 Información de autenticación<br>5.18 Derechos de acceso<br>8.3 Restricción de acceso a la información<br>8.7 Protección contra *malware*<br>8.13 Copia de seguridad de la información |
| Caída de las fuentes de energía | Impedimento para utilizar el dispositivo y los vinculados a éste | Baja | Alto | Moderado | Puesta en funcionamiento inmediata y automática de la UPS. Monitoreo continuo de fase y tensión de la línea estabilizada. | Baja | Medio | Tolerable | 5.29 Seguridad de la información durante la interrupción |

**Subcomponente:** Firewalls
**Valor del Activo:** 8.5 / 10 **Nivel de Criticidad:** Muy Alto

| Amenaza | Degradación del activo | Probabilidad de ocurrencia | Impacto | Riesgo | Salvaguarda | Probabilidad Residual | Impacto Residual | Riesgo Residual | Control seleccionado (Anexo 1 - ISO 27001) |
|---|---|---|---|---|---|---|---|---|---|
| Mal funcionamiento del equipo | Impedimento para utilizar el dispositivo | Media | Alto | Importante | Realizar el mantenimiento preventivo del dispositivo. Cambio del dispositivo | Baja | Medio | Tolerable | 7.13 Mantenimiento de equipos |
| Acceso no autorizado | Acceso no autorizado al resto de los dispositivos vinculados a éste | Media | Alto | Importante | Monitoreo continuo del sistema de defensa del elemento | Baja | Medio | Tolerable | 5.15 Control de acceso<br>5.17 Información de autenticación<br>5.18 Derechos de acceso<br>8.3 Restricción de acceso a la información<br>8.7 Protección contra malware |
| Caída de las fuentes de energía | Impedimento para utilizar el dispositivo y los vinculados a éste | Baja | Alto | Moderado | Puesta en funcionamiento inmediata y automática de la UPS. Monitoreo continuo de fase y tensión de la línea estabilizada. | Baja | Medio | Tolerable | 5.29 Seguridad de la información durante la interrupción |

**Subcomponente:** Firewalls
**Valor del Activo:** 6.3 / 10 **Nivel de Criticidad:** Alto

| Amenaza | Degradación del activo | Probabilidad de ocurrencia | Impacto | Riesgo | Salvaguarda | Probabilidad Residual | Impacto Residual | Riesgo Residual | Control seleccionado (Anexo 1 - ISO 27001) |
|---|---|---|---|---|---|---|---|---|---|
| Mal funcionamiento del equipo | Impedimento para utilizar el dispositivo | Baja | Alto | Moderado | Realizar el mantenimiento preventivo del dispositivo. Cambio del dispositivo | Baja | Medio | Tolerable | 7.13 Mantenimiento de equipos |
| Mantenimiento inadecuado | Impedimento para utilizar el dispositivo | Baja | Alto | Moderado | Cambio del dispositivo | Baja | Medio | Tolerable | 7.13 Mantenimiento de equipos |
| Caída de las fuentes de energía | Impedimento para utilizar el dispositivo y los vinculados | Baja | Alto | Moderado | Contención Institucional de las instalaciones | Baja | Medio | Tolerable | 5.29 Seguridad de la información durante la interrupción |

| Amenaza | Degradación del activo | Probabilidad de ocurrencia | Impacto | Riesgo | Salvaguarda | Probabilidad Residual | Impacto Residual | Riesgo Residual | Control seleccionado (Anexo 1 - ISO 27001) |
|---|---|---|---|---|---|---|---|---|---|
| | a este | | | | | | | | |

**Subcomponente:** Dispositivos de Trabajo – Puestos de Trabajo
**Valor del Activo:** 9.5/ 10 **Nivel de Criticidad:** Muy Alto

| Amenaza | Degradación del activo | Probabilidad de ocurrencia | Impacto | Riesgo | Salvaguarda | Probabilidad Residual | Impacto Residual | Riesgo Residual | Control seleccionado (Anexo 1 - ISO 27001) |
|---|---|---|---|---|---|---|---|---|---|
| Mal funcionamiento del equipo | Impedimento para utilizar el dispositivo | Media | Alto | Importante | Realizar el mantenimiento preventivo del dispositivo. Cambio del dispositivo | Baja | Medio | Tolerable | 7.13 Mantenimiento de equipos |
| Acceso no autorizado | Acceso no autorizado al resto de los dispositivos vinculados a éste | Media | Alto | Importante | Monitoreo continuo del sistema de defensa del elemento | Baja | Medio | Tolerable | 5.15 Control de acceso 5.17 Información de autenticación 5.18 Derechos de acceso 8.3 Restricción de acceso a la información |
| Caída de las fuentes de energía | Impedimento para utilizar el dispositivo y los vinculados a este | Baja | Alto | Moderado | Puesta en funcionamiento inmediata y automática de la UPS. Monitoreo continuo de fase y tensión de la línea estabilizada. | Baja | Medio | Tolerable | 5.29 Seguridad de la información durante la interrupción |

**Subcomponente:** Dispositivos de Trabajo – Duplicadores Forenses
**Valor del Activo:** 9.5 / 10 **Nivel de Criticidad:** Muy Alto

| Amenaza | Degradación del activo | Probabilidad de ocurrencia | Impacto | Riesgo | Salvaguarda | Probabilidad Residual | Impacto Residual | Riesgo Residual | Control seleccionado (Anexo 1 - ISO 27001) |
|---|---|---|---|---|---|---|---|---|---|
| Mal funcionamiento del equipo | Impedimento para utilizar el dispositivo | Media | Alto | Importante | Realizar el mantenimiento preventivo del dispositivo. Cambio del dispositivo | Baja | Medio | Tolerable | 7.13 Mantenimiento de equipos |
| Acceso no autorizado | Acceso no autorizado al resto de los dispositivos vinculados a éste | Media | Alto | Importante | Monitoreo continuo del sistema de defensa del elemento. Resguardo seguro del elemento. | Baja | Medio | Tolerable | 5.15 Control de acceso 5.17 Información de autenticación 5.18 Derechos de acceso 8.3 Restricción de acceso a la información |
| Pérdida o robo | Acceso a información no autorizada o pérdida/destrucción de esta. Impedimento para utilizar el dispositivo | Baja | Alto | Moderado | Mantener inventario y resguardo de los elementos | Baja | Medio | Tolerable | 7.1 Perímetros de seguridad física 7.2 Entrada física 7.3 Asegurar oficinas, habitaciones e instalaciones 7.4 Monitoreo de seguridad física 7.7 Escritorio y pantalla claros |
| Caída de las fuentes de energía | Impedimento para utilizar el dispositivo | Baja | Alto | Moderado | Puesta en funcionamiento inmediata y automática de la UPS. Monitoreo continuo de fase y tensión de la línea estabilizada. | Baja | Medio | Tolerable | 5.15 Control de acceso 5.17 Información de autenticación 5.18 Derechos de acceso 8.3 Restricción de acceso a la información |

**Subcomponente:** Dispositivos de Trabajo – Dispositivos para resguardo de datos (Discos Externos, Pendrive, etc.)
**Valor del Activo:** 10 / 10 **Nivel de Criticidad:** Muy Alto

| Amenaza | Degradación del activo | Probabilidad de ocurrencia | Impacto | Riesgo | Salvaguarda | Probabilidad Residual | Impacto Residual | Riesgo Residual | Control seleccionado (Anexo 1 - ISO 27001) |
|---|---|---|---|---|---|---|---|---|---|
| Acceso no autorizado | Acceso a información no autorizada o pérdida/ destrucción de esta | Baja | Alto | Moderado | Monitoreo continuo del sistema de defensa del elemento. Resguardo seguro del elemento. | Baja | Medio | Tolerable | 5.15 Control de acceso 5.17 Información de autenticación 5.18 Derechos de acceso 8.3 Restricción de acceso a la información |
| Pérdida o robo | Acceso a información no autorizada o pérdida/ destrucción de esta. Impedimento para utilizar el dispositivo | Baja | Alto | Moderado | Mantener inventario y resguardo de los elementos | Baja | Medio | Tolerable | 7.1 Perímetros de seguridad física 7.2 Entrada física 7.3 Asegurar oficinas, habitaciones e instalaciones 7.4 Monitoreo de seguridad física 7.7 Escritorio y pantalla claros |
| Fallas en la seguridad física de las instalacio-nes | Acceso a información no autorizada o pérdida/ destrucción de esta | Baja | Alto | Moderado | Actualización y refuerzo de la seguridad física de las instalaciones | Baja | Medio | Tolerable | 7.1 Perímetros de seguridad física 7.2 Entrada física 7.3 Asegurar oficinas, habitaciones e instalaciones 7.4 Monitoreo de seguridad física |

**Subcomponente:** Dispositivos de Trabajo – Equipamiento de Repuesto
**Valor del Activo:** 5.8 / 10 **Nivel de Criticidad:** Muy Alto

| Amenaza | Degradación del activo | Probabilidad de ocurrencia | Impacto | Riesgo | Salvaguarda | Probabilidad Residual | Impacto Residual | Riesgo Residual | Control seleccionado (Anexo 1 - ISO 27001) |
|---|---|---|---|---|---|---|---|---|---|
| Mantenimiento inadecuado | Impedimento para utilizar el dispositivo | Baja | Bajo | Trivial | Cambio del dispositivo | Baja | Bajo | Trivial | 7.13 Mantenimiento de equipos |

**Subcomponente:** Dispositivos de Trabajo – Impresoras
**Valor del Activo:** 4.3 / 10 **Nivel de Criticidad:** Bajo

| Amenaza | Degradación del activo | Probabilidad de ocurrencia | Impacto | Riesgo | Salvaguarda | Probabilidad Residual | Impacto Residual | Riesgo Residual | Control seleccionado (Anexo 1 - ISO 27001) |
|---|---|---|---|---|---|---|---|---|---|
| Mal funcionamiento del equipo | Impedimento para utilizar el dispositivo | Baja | Bajo | Trivial | Realizar el mantenimiento preventivo del dispositivo. Cambio del dispositivo | Baja | Bajo | Trivial | 7.13 Mantenimiento de equipos |
| Mantenimiento inadecuado | Impedimento para utilizar el dispositivo | Baja | Bajo | Trivial | Cambio del dispositivo | Baja | Bajo | Trivial | 7.13 Mantenimiento de equipos |

**Subcomponente:** Dispositivos de Comunicaciones – *Switch*
**Valor del Activo:** 4.5 / 10 **Nivel de Criticidad:** Bajo

| Amenaza | Degradación del activo | Probabilidad de ocurrencia | Impacto | Riesgo | Salvaguarda | Probabilidad Residual | Impacto Residual | Riesgo Residual | Control seleccionado (Anexo 1 - ISO 27001) |
|---|---|---|---|---|---|---|---|---|---|
| Mal funcionamiento del equipo | Impedimento para utilizar el dispositivo | Baja | Bajo | Trivial | Cambio del dispositivo | Baja | Bajo | Trivial | 7.13 Mantenimiento de equipos |
| Caída de las fuentes de energía | Impedimento para utilizar el dispositivo y los vinculados a éste | Baja | Alto | Moderado | Puesta en funcionamiento inmediata y automática de la UPS. Monitoreo continuo de fase y tensión de la línea estabilizada. | Baja | Medio | Tolerable | 5.29 Seguridad de la información durante la interrupción |

**Subcomponente:** Dispositivos de Comunicaciones - Dispositivo para conexión a internet (modem, router, etc)
**Valor del Activo:** 4.8 / 10 **Nivel de Criticidad:** Bajo

| Amenaza | Degradación del activo | Probabilidad de ocurrencia | Impacto | Riesgo | Salvaguarda | Probabilidad Residual | Impacto Residual | Riesgo Residual | Control seleccionado (Anexo 1 - ISO 27001) |
|---|---|---|---|---|---|---|---|---|---|
| Mal funcionamiento del equipo | Impedimento para utilizar el dispositivo | Baja | Bajo | Trivial | Cambio del dispositivo | Baja | Bajo | Trivial | 7.13 Mantenimiento de equipos |
| Caída de las fuentes de energía | Impedimento para utilizar el dispositivo y los vinculados a éste | Baja | Alto | Moderado | Puesta en funcionamiento inmediata y automática de la UPS. Monitoreo continuo de fase y tensión de la línea estabilizada. | Baja | Medio | Tolerable | 5.29 Seguridad de la información durante la interrupción |

**Subcomponente:** Soportes Estructurales (*Racks*, Cableado de datos y comunicaciones)
**Valor del Activo:** 5.0 / 10 **Nivel de Criticidad:** Bajo

| Amenaza | Degradación del activo | Probabilidad de ocurrencia | Impacto | Riesgo | Salvaguarda | Probabilidad Residual | Impacto Residual | Riesgo Residual | Control seleccionado (Anexo 1 - ISO 27001) |
|---|---|---|---|---|---|---|---|---|---|
| Instalación inadecuada o fallas de los soportes estructurales | Parada total o parcial de la operatividad del laboratorio | Baja | Alto | Moderado | Revisión y ajuste según normas de cableado estructurado | Baja | Medio | Tolerable | 7.8 Emplazamiento y protección de equipos<br>7.12 Seguridad del cableado<br>8.8 Gestión de vulnerabilidades<br>8.16 Actividades de supervisión |
| Fallas en la seguridad física de las instalaciones | Parada total o parcial de la operatividad del laboratorio | Media | Alto | Importante | Actualización y refuerzo de la seguridad física de las instalaciones | Baja | Medio | Tolerable | 7.1 Perímetros de seguridad física<br>7.2 Entrada física<br>7.3 Asegurar oficinas, habitaciones e instalaciones<br>7.4 Monitoreo de seguridad física |

**DATOS**
**Subcomponente:** Datos para la Gestión Interna de las actividades forenses (agenda de causas, ciclo de vida de actividad forense, etc.)
**Valor del Activo:** 8.5 / 10 **Nivel de Criticidad:** Muy Alto

| Amenaza | Degradación del activo | Probabilidad de ocurrencia | Impacto | Riesgo | Salvaguarda | Probabilidad Residual | Impacto Residual | Riesgo Residual | Control seleccionado (Anexo 1 - ISO 27001) |
|---|---|---|---|---|---|---|---|---|---|
| Caída de la red o del puesto de trabajo | Impedimento de acceso a los datos o aplicaciones | Baja | Alto | Moderado | Monitoreo continuo del funcionamiento de la red y de los puestos de trabajo | Baja | Medio | Tolerable | Los asignados a la infraestructura de comunicaciones |
| Errores o desactualización del *software* | Mal funcionamiento del software con impacto indirecto en las actividades forenses | Baja | Alto | Moderado | Corrección y/o actualización del *software*.<br>Utilización de un *software* alternativo | Baja | Medio | Tolerable | 8.5 Autenticación segura<br>8.8 Gestión de vulnerabilidades técnicas<br>8.9 Gestión de la configuración<br>8.12 Prevención de fuga de datos<br>8.16 Actividades de supervisión<br>8.26 Requisitos de seguridad de las aplicaciones |

**Subcomponente:** Imágenes Forenses
**Valor del Activo:** 10 / 10 **Nivel de Criticidad:** Muy Alto

| Amenaza | Degradación del activo | Probabilidad de ocurrencia | Impacto | Riesgo | Salvaguarda | Probabilidad Residual | Impacto Residual | Riesgo Residual | Control seleccionado (Anexo 1 - ISO 27001) |
|---|---|---|---|---|---|---|---|---|---|
| Caída de la red o del puesto de trabajo | Impedimento de acceso a los datos o aplicaciones | Baja | Alto | Moderado | Monitoreo continuo del funcionamiento de la red y de los puestos de trabajo | Baja | Medio | Tolerable | Los asignados a la infraestructura de comunicaciones |
| Errores o desactualización del *software* | Mal funcionamiento del software con impacto directo en las actividades forenses | Media | Alto | Importante | Corrección y/o actualización del software. Utilización de un software alternativo | Baja | Medio | Tolerable | 8.5 Autenticación segura<br>8.8 Gestión de vulnerabilidades técnicas<br>8.9 Gestión de la configuración<br>8.12 Prevención de fuga de datos<br>8.16 Actividades de supervisión<br>8.26 Requisitos de seguridad de las aplicaciones |

**Subcomponente:** Cadena de Custodia
**Valor del Activo:** 10 / 10 **Nivel de Criticidad:** Muy Alto

| Amenaza | Degradación del activo | Probabilidad de ocurrencia | Impacto | Riesgo | Salvaguarda | Probabilidad Residual | Impacto Residual | Riesgo Residual | Control seleccionado (Anexo 1 - ISO 27001) |
|---|---|---|---|---|---|---|---|---|---|
| Acceso no autorizado | Acceso a información no autorizada o pérdida/destrucción de esta. | Alta | Alto | Crítico | Monitoreo continuo del sistema de defensa del elemento. Resguardo seguro del elemento. | Media | Medio | Moderado | 5.15 Control de acceso<br>5.17 Información de autenticación<br>5.18 Derechos de acceso<br>8.3 Restricción de acceso a la información |

**Subcomponente:** Certificación de Firma de Documentos
**Valor del Activo:** 8.5 / 10 **Nivel de Criticidad:** Muy Alto

| Amenaza | Degradación del activo | Probabilidad de ocurrencia | Impacto | Riesgo | Salvaguarda | Probabilidad Residual | Impacto Residual | Riesgo Residual | Control seleccionado (Anexo 1 - ISO 27001) |
|---|---|---|---|---|---|---|---|---|---|
| Acceso no autorizado | Acceso a información no autorizada o pérdida/destrucción de esta | Alta | Alto | Crítico | Resguardo seguro del dispositivo | Media | Medio | Moderado | 5.15 Control de acceso<br>5.17 Información de autenticación<br>5.18 Derechos de acceso<br>8.3 Restricción de acceso a la información |

**RECURSOS HUMANOS**
**Subcomponente:** Formación, Conocimientos y Experiencia en Informática Forense
**Valor del Activo:** 7.7 / 10 **Nivel de Criticidad:** Alto

| Amenaza | Degradación del activo | Probabilidad de ocurrencia | Impacto | Riesgo | Salvaguarda | Probabilidad Residual | Impacto Residual | Riesgo Residual | Control seleccionado (Anexo 1 - ISO 27001) |
|---|---|---|---|---|---|---|---|---|---|
| Conocimientos insuficientes o inadecuados | Impacta en la conformación de un equipo forense actualizado y experto | Media | Alto | Importante | Capacitación continua | Baja | Medio | Tolerable | 6.2 Términos y condiciones de empleo<br>6.6 Acuerdos de confidencialidad o no divulgación<br>6.3 Concienciación, educación y capacitación sobre seguridad de la información |

**Subcomponente:** Formación, Conocimientos y Experiencia en Ciencias del Derecho
**Valor del Activo:** 5.0 / 10
**Nivel de Criticidad:** Bajo

| Amenaza | Degradación del activo | Probabilidad de ocurrencia | Impacto | Riesgo | Salvaguarda | Probabilidad Residual | Impacto Residual | Riesgo Residual | Control seleccionado (Anexo 1 - ISO 27001) |
|---|---|---|---|---|---|---|---|---|---|
| Conocimientos insuficientes o inadecuados | Impacta en la conformación de un equipo forense actualizado y experto | Media | Bajo | Tolerable | Capacitación continua | Baja | Bajo | Trivial | 6.2 Términos y condiciones de empleo<br>6.6 Acuerdos de confidencialidad o no divulgación<br>6.3 Concienciación, educación y capacitación sobre seguridad de la información |

**Subcomponente:** Formación, Conocimientos y Experiencia en Investigación Criminal
**Valor del Activo:** 5.0 / 10 **Nivel de Criticidad:** Bajo

| Amenaza | Degradación del activo | Probabilidad de ocurrencia | Impacto | Riesgo | Salvaguarda | Probabilidad Residual | Impacto Residual | Riesgo Residual | Control seleccionado (Anexo 1 - ISO 27001) |
|---|---|---|---|---|---|---|---|---|---|
| Conocimientos insuficientes o inadecuados | Impacta en la conformación de un equipo forense actualizado y experto | Alta | Alto | Crítico | Capacitación continua | Baja | Medio | Tolerable | 6.2 Términos y condiciones de empleo<br>6.6 Acuerdos de confidencialidad o no divulgación<br>6.3 Concienciación, educación y capacitación sobre seguridad de la información |

**Subcomponente:** Comportamiento Profesional y Ético
**Valor del Activo:** 7.7 / 10 **Nivel de Criticidad:** Alto

| Amenaza | Degradación del activo | Probabilidad de ocurrencia | Impacto | Riesgo | Salvaguarda | Probabilidad Residual | Impacto Residual | Riesgo Residual | Control seleccionado (Anexo 1 - ISO 27001) |
|---|---|---|---|---|---|---|---|---|---|
| Hace vulnerable el sistema y las actividades forenses | Se promueve la comisión de delitos relacionados con la actividad forense | Baja | Alto | Moderado | Verificación de antecedentes previo a la designación en el cargo | Baja | Medio | Tolerable | 6.2 Términos y condiciones de empleo<br>6.6 Acuerdos de confidencialidad o no divulgación<br>6.3 Concienciación, educación y capacitación sobre seguridad de la información |

**INFRAESTRUCTURA EDILICIA**
**Subcomponente:** Aire Acondicionado
**Valor del Activo:** 6.0 / 10 **Nivel de Criticidad:** Alto

| Amenaza | Degradación del activo | Probabilidad de ocurrencia | Impacto | Riesgo | Salvaguarda | Probabilidad Residual | Impacto Residual | Riesgo Residual | Control seleccionado (Anexo 1 - ISO 27001) |
|---|---|---|---|---|---|---|---|---|---|
| Mal funcionamiento del equipo | Impedimento para utilizar el dispositivo | Media | Alto | Importante | Realizar el mantenimiento preventivo del dispositivo. Cambio del dispositivo | Baja | Medio | Tolerable | 7.13 Mantenimiento de equipos |
| Mantenimiento inadecuado | Impedimento para utilizar el dispositivo | Media | Alto | Importante | Cambio del dispositivo | Baja | Medio | Tolerable | 7.13 Mantenimiento de equipos |
| Caída de las fuentes de energía | Parada total o parcial de la operatividad del laboratorio | Media | Alto | Importante | Puesta en funcionamiento inmediata y automática de la UPS. Monitoreo continuo de fase y tensión de la línea estabilizada. | Baja | Medio | Tolerable | 7.12 Seguridad del cableado<br>5.30 Preparación de las TIC para la continuidad de las actividades |

**Subcomponente:** Infraestructura Eléctrica
**Valor del Activo:** 6.3 / 10 **Nivel de Criticidad:** Alto

| Amenaza | Degradación del activo | Probabilidad de ocurrencia | Impacto | Riesgo | Salvaguarda | Probabilidad Residual | Impacto Residual | Riesgo Residual | Control seleccionado (Anexo 1 - ISO 27001) |
|---|---|---|---|---|---|---|---|---|---|
| Mantenimiento inadecuado | Impedimento para utilizar el dispositivo | Baja | Alto | Moderado | Cambio del dispositivo | Baja | Medio | Tolerable | 7.13 Mantenimiento de equipos |
| Caída de las fuentes de energía | Parada total o parcial de la operatividad del laboratorio | Media | Alto | Importante | Puesta en funcionamiento inmediata y automática de la UPS. Monitoreo continuo de fase y tensión de la línea estabilizada. | Baja | Medio | Tolerable | 7.12 Seguridad del cableado<br>5.30 Preparación de las TIC para la continuidad de las actividades |

**Subcomponente:** Alarma Monitoreada
**Valor del Activo:** 5.3 / 10 **Nivel de Criticidad:** Alto

| Amenaza | Degradación del activo | Probabilidad de ocurrencia | Impacto | Riesgo | Salvaguarda | Probabilidad Residual | Impacto Residual | Riesgo Residual | Control seleccionado (Anexo 1 - ISO 27001) |
|---|---|---|---|---|---|---|---|---|---|
| Acceso no autorizado | Acceso a información no autorizada o pérdida/destrucción de esta | Baja | Alto | Moderado | Monitoreo continuo del sistema de defensa del elemento. Resguardo seguro del elemento. | Baja | Medio | Tolerable | 5.15 Control de acceso 5.17 Información de autenticación 5.18 Derechos de acceso 8.3 Restricción de acceso a la información |
| Fallas en la seguridad física de las instalaciones | Acceso a información no autorizada o pérdida/destrucción de esta | Baja | Alto | Moderado | Actualización y refuerzo de la seguridad física de las instalaciones | Baja | Medio | Tolerable | 7.1 Perímetros de seguridad física 7.2 Entrada física 7.3 Asegurar oficinas. habitaciones e instalaciones 7.4 Monitoreo de seguridad física |
| Caída de las fuentes de energía | Impedimento para utilizar el dispositivo y los vinculados a éste | Baja | Alto | Moderado | Puesta en funcionamiento inmediata y automática de la UPS. Monitoreo continuo de fase y tensión de la línea estabilizada. | Baja | Medio | Tolerable | 7.12 Seguridad del cableado 5.30 Preparación de las TIC para la continuidad de las actividades |

**Subcomponente:** Seguridad Física de los Efectos (anaquel con llave)
**Valor del Activo:** 4.0 / 10 **Nivel de Criticidad:** Bajo

| Amenaza | Degradación del activo | Probabilidad de ocurrencia | Impacto | Riesgo | Salvaguarda | Probabilidad Residual | Impacto Residual | Riesgo Residual | Control seleccionado (Anexo 1 - ISO 27001) |
|---|---|---|---|---|---|---|---|---|---|
| Acceso no autorizado | Acceso a información no autorizada o pérdida/destrucción de esta | Alta | Medio | Importante | Monitoreo continuo del sistema de defensa del elemento. Resguardo seguro del elemento. | Media | Bajo | Tolerable | 5.15 Control de acceso 5.17 Información de autenticación 5.18 Derechos de acceso 8.3 Restricción de acceso a la información |
| Fallas en la seguridad física de las instalaciones | Acceso a información no autorizada o /destrucción de esta | Baja | Alto | Moderado | Actualización y refuerzo de la seguridad física de las instalaciones | Baja | Medio | Tolerable | 7.1 Perímetros de seguridad física 7.2 Entrada física 7.3 Asegurar oficinas, habitaciones e instalaciones 7.4 Monitoreo de seguridad física |

**Subcomponente:** Herramientas de Taller
**Valor del Activo:** 4.0 / 10 **Nivel de Criticidad:** Bajo

| Amenaza | Degradación del activo | Probabilidad de ocurrencia | Impacto | Riesgo | Salvaguarda | Probabilidad Residual | Impacto Residual | Riesgo Residual | Control seleccionado (Anexo 1 - ISO 27001) |
|---|---|---|---|---|---|---|---|---|---|
| Pérdida o robo | Imposibilidad de realizar tareas manuales | Baja | Bajo | Trivial | Mantener inventario y resguardo de los elementos | Baja | Bajo | Trivial | 7.1 Perímetros de seguridad física 7.2 Entrada física 7.3 Asegurar oficinas, habitaciones e instalaciones 7.4 Monitoreo de seguridad física |