MUNICIPALIDAD PROVINCIAL DE
MAYNAS
Hagamos Historia

# "PLAN DE GESTIÓN DE RIESGOS DE TECNOLOGIAS DE LA INFORMACIÓN"

## MUNICIPALIDAD PROVINCIAL DE MAYNAS

Descripción breve

Este documento identifica los activos, amenazas, salvaguardas los posibles riesgos para poder realizar planes de contingencias y reducir el posible impacto en los procesos de la Municipalidad Provincial de Maynas (MPM) que está sometido este proyecto en seguridad TI.

OFICINA DE SISTEMAS Y TECNOLOGIAS DE LA INFORMACIÓN

# INDICE

## Contenido

# I. Introducción

## 1.1. Descripción general del documento

Un análisis y gestión de riesgo es un enfoque sistemático para identificar y gestionar las amenazas o vulnerabilidades que pueden comprometer la integridad, confidencialidad y disponibilidad de los activos de información de la Municipalidad Provincial de Maynas (MPM).

MAGERIT es una "Metodología de Análisis y Gestión de Riesgo de los Sistemas de Información" elaborado por el Consejo Superior de Administración Electrónica de España

MAGERIT se utiliza para identificar y evaluar los riesgos asociados a los sistemas de información y establecer medidas de seguridad adecuadas para en analizar el impacto que puede tener para la empresa u organización la violación de seguridad, buscando identificar las amenazas que puedan llegar afectar dicha organización, logrando así tener una identificación clara de las medidas preventivas y correctivas más adecuadas.

Proporciona un enfoque sistemático y estructurado para evaluar y gestionar los riesgos de seguridad de la información, lo que ayuda a las organizaciones a proteger sus activos de información y garantizar la continuidad de los servicios.

## 1.2. Objetivos:

Los objetivos de la Gestión de Riesgo de tecnologías de la información son los siguientes:

- Identificar y evaluar los potenciales riesgos a lo que está expuesto la Municipalidad Provincial de Maynas (MPM).
- Mitigar los riesgos que pueden afectar negativamente a la Municipalidad Provincial de Maynas (MPM).

# 2. Análisis de riesgos

## Activos

Se refiere a cualquier recurso o componente que tiene valor para una organización en términos de tecnología de la información. Un activo es aquel elemento que contiene o manipula información

### Tipos de Activos

**Información.** Son los datos confidenciales de la Organización (MPM) que se guardan o alojan en un servidor.

**Software**

- SGTM: La generación, distribución y cobro de los arbitrios.
- Trámite documentario: Registro, almacenamiento y recuperación de documentos.
- SIAF: Herramienta para ordenar la gestión administrativa de los gobiernos locales.
- SIGA: Sistema integrado de Gestión Administrativa es una herramienta informática que simplifica y automatiza los procesos administrativos en una entidad del Estado.

- KOHA: Sistema de bibliotecas de código abierto y gratuito.
- FREENAS: Plataforma de gestión de bibliotecas.
- Windows server 2010 PRO, server 2016, server 2019.

**Hardware**

- *Servidores*
  *Cantidad de Servidores: 5*

| IP | SERVIDORES | SERVICIOS | ESPACIO USADO | ESPACIO LIBRE |
|---|---|---|---|---|
| 192.168.1.6 | TRAMITE | TRAMITE, LOGISTICO, CARPETAS COMPARTIDAS | 1.98 TB | 1.65 TB |
| 192.168.100.33 | PRUEBA | SGTM, CONSOLA ANTIVIRUS | C: 918 GB | C: 1.10TB |
| | | | D: 1.63 TB | D: 370 GB |
| | | | E: 1.36 TB | E: 689 GB |
| | | | F: 1.06 TB | F: 220 GB |
| 192.168.7.2 | SIAF | SIAF, SIGA | C: 667 GB | C: 1.13 TB |
| | | | E/M: 866 GB | E/M: 996 GB |
| | | | F: 31.2 GB | F: 663 MB |
| 192.168.1.8 | VIRTUAL EsXI | WINDOWS SERVER 2016, WINDOWS 10 PRO, KOHA, FREENAS | 1.47 TB | 230.9 GB |
| 192.168.1.33 | BD SGTM | WINDOWS SERVER 2019 | C: 107 GB | C: 3.74 TB |
| | | | D: 3.70 TB | D: 3.57 TB |
| | | | E: 3.43 TB | E: 20.0 KB |

- *Computadora de escritorio*

| TIPO EQUIPO | MARCA | SISTEMA OPERATIVO |
|---|---|---|
| ALL - IN - ONE | HP | WIN 10 PRO |
| ALL - IN - ONE | HP | WIN 10 PRO |
| DESKTOP | ADVANCE | WIN 8.1 PRO |
| ALL-IN-ONE | HP | WIN 10 PRO |
| DESKTOP | ADVANCE | WIN 10 PRO |
| ALL - IN - ONE | HP | WIN 10 PRO |
| ALL - IN - ONE | HP | WIN 7 PRO |
| ALL - IN - ONE | HP | WIN 10 PRO |
| ALL - IN - ONE | HP | WIN 10 PRO |
| ALL - IN - ONE | HP | WIN 10 PRO |

| | | |
|---|---|---|
| DESKTOP | NEUTRO | WIN 7 PRO |
| DESKTOP | HP | WIN 10 PRO |
| ALL-IN-ONE | HP | WIN 10 PRO |
| ALL-IN-ONE | HP | WIN 10 PRO |
| DESKTOP | HP | WIN 10 PRO |
| DESKTOP | | WIN 10 PRO |
| DESKTOP | ECOTREND | WIN 7 PRO |
| DESKTOP | ADVANCE | WIN 7 PRO |
| DESKTOP | ECOTREND | WIN 10 PRO |
| DESKTOP | SAMSUNG | WIN 10 PRO |
| DESKTOP | CYBERTEL | WIN 10 PRO |
| DESKTOP | CYBERTEL | WIN 7 PRO |
| DESKTOP | DATRONE | WIN 10 PRO |
| DESKTOP | DATRONE | WIN 10 PRO |
| DESKTOP | DATRONE | WIN 10 PRO |
| DESKTOP | CYBERTEL | WIN 10 PRO |
| ALL - IN - ONE | HP | WIN 7 PRO |
| DESKTOP | DATRONE | WIN 10 PRO |
| DESKTOP | | WIN 10 PRO |
| DESKTOP | | WIN 10 PRO |
| DESKTOP | ADVANCE | WIN 7 PRO |
| DESKTOP | ADVANCE | WIN 7 PRO |
| ALL - IN - ONE | HP | WIN 10 PRO |
| ALL - IN - ONE | HP | WIN 10 PRO |
| ALL - IN - ONE | HP | WIN 10 PRO |
| ALL - IN - ONE | HP | WIN 10 PRO |
| ALL - IN - ONE | HP | WIN 7 PRO |
| ALL - IN - ONE | HP | WIN 10 PRO |
| ALL - IN - ONE | HP | WIN 10 PRO |
| DESKTOP | MICRONICS | WIN 7 PRO |
| DESKTOP | ALTRON | WIN 10 PRO |
| LAPTOP | HP | WIN 8.1 PRO |
| LAPTOP | HP | WIN 10 PRO |
| LAPTOP | HP | WIN 10 PRO |
| ALL - IN - ONE | HP | WIN 10 PRO |
| ALL - IN - ONE | HP | WIN 10 PRO |
| ALL - IN - ONE | HP | WIN 10 PRO |
| ALL - IN - ONE | HP | WIN 10 PRO |
| ALL - IN - ONE | HP | WIN 10 PRO |

| | | |
|---|---|---|
| ALL - IN - ONE | HP | WIN 10 PRO |
| ALL - IN - ONE | HP | WIN 10 PRO |
| ALL - IN - ONE | HP | WIN 10 PRO |
| ALL-IN-ONE | LENOVO | WIN 10 PRO |
| ALL-IN-ONE | LENOVO | WIN 10 PRO |
| DESKTOP | ALTRON | WIN 7 PRO |
| DESKTOP | NEUTRO | WIN 7 PRO |
| DESKTOP | HP | WIN 10 PRO |
| DESKTOP | MICRONICS | WIN 7 PRO |
| DESKTOP | MICRONICS | WIN 7 PRO |
| DESKTOP | DATATRONE | WIN 10 PRO |
| DESKTOP | ADVANCE | WIN 7 PRO |
| DESKTOP | ADVANCE | WIN 10 PRO |
| DESKTOP | ADVANCE | WIN 10 PRO |
| DESKTOP | ADVANCE | WIN 7 PRO |
| DESKTOP | TEROS | WIN 10 PRO |
| DESKTOP | HALION | WIN 7 PRO |
| DESKTOP | HALION | WIN 7 PRO |
| DESKTOP | NEUTRO | WIN 7 PRO |
| DESKTOP | ENKORE | WIN 10 PRO |
| DESKTOP | ENKORE | WIN 10 PRO |
| DESKTOP | ADVANCE | WIN 10 PRO |
| ALL-IN-ONE | THINK – CENTER | WIN 10 PRO |
| ALL-IN-ONE | THINK – CENTER | WIN 10 PRO |
| ALL-IN-ONE | THINK – CENTER | WIN 10 PRO |
| DESKTOP | TEROS | WIN 10 PRO |
| DESKTOP | TEROS | WIN 10 PRO |
| ALL-IN-ONE | THINK – CENTER | WIN 10 PRO |
| ALL-IN-ONE | THINK – CENTER | WIN 10 PRO |
| ALL-IN-ONE | THINK – CENTER | WIN 10 PRO |
| DESKTOP | NEUTRO | WIN 7 PRO |
| DESKTOP | ADVANCE | WIN 8.1 PRO |
| DESKTOP | AVATEC | WIN 8.1 PRO |
| DESKTOP | ADVANCE | WIN 8.1 PRO |
| DESKTOP | HP | WIN 10 PRO |
| DESKTOP | HP | WIN 10 PRO |
| ALL - IN - ONE | HP | WIN 10 PRO |
| ALL-IN-ONE | HP | WIN 10 PRO |
| DESKTOP | COOLER-MASTER | WIN 10 PRO |
| DESKTOP | HP | WIN10 PRO |
| DESKTOP | LG | WIN 10 PRO |
| DESKTOP | LENOVO | WIN 10 PRO |
| DESKTOP | ADVANCE | WIN 10 PRO |
| DESKTOP | ADVANCE | WIN 7 PRO |
| DESKTOP | VASTEC | WIN 10 PRO |

| | | |
|---|---|---|
| DESKTOP | VASTEC | WIN 10 PRO |
| DESKTOP | LG | WIN 10 PRO |
| DESKTOP | ADVANCE | WIN 8.1 PRO |
| DESKTOP | HP | WIN 10 PRO |
| DESKTOP | ADVANCE | WIN 8.1 PRO |
| DESKTOP | ADVANCE | WIN 10 PRO |
| DESKTOP | ADVANCE | WIN 8.1 PRO |
| ALL - IN -ONE | HPº | WIN 10 PRO |
| DESKTOP | ADVANCE | WIN 7 PRO |
| DESKTOP | VASTEC | WIN 10 PRO |
| DESKTOP | HP | WIN 10 PRO |
| DESKTOP | ADVANCE | WIN 7 PRO |
| ALL - IN -ONE | HP | WIN 10 PRO |
| DESKTOP | HP | WIN 10 PRO |
| DESKTOP | ADVANCE | WIN 8.1 PRO |
| DESKTOP | HP | WIN 10 PRO |
| DESKTOP | ADVANCE | WIN 8.1 PRO |
| DESKTOP | HP | WIN 10 PRO |
| DESKTOP | HP | WIN 10 PRO |
| ALL-IN-ONE | HP | WIN 10 PRO |
| DESKTOP | VASTEC | WIN 10 PRO |
| DESKTOP | HP | WIN 10 PRO |
| DESKTOP | VIEWSONIC | WIN 10 PRO |
| DESKTOP | HP | WIN 10 PRO |
| DESKTOP | CYBERTEL | WIN 7 PRO |
| ALL-IN-ONE | HP | WIN 10 PRO |
| ALL-IN-ONE | HP | WIN 10 PRO |
| ALL-IN-ONE | HP | WIN 10 PRO |
| ALL-IN-ONE | HP | WIN 10 PRO |
| ALL-IN-ONE | HP | WIN 10 PRO |
| DESKTOP | MICRONICS | WIN 10 PRO |
| ALL-IN-ONE | HP | WIN 10 PRO |
| ALL-IN-ONE | HP | WIN 10 PRO |
| ALL-IN-ONE | HP | WIN 10 PRO |
| ALL-IN-ONE | HP | WIN 10 PRO |
| ALL-IN-ONE | HP | WIN 10 PRO |
| ALL-IN-ONE | HP | WIN 10 PRO |
| ALL-IN-ONE | HP | WIN 10 PRO |
| ALL-IN-ONE | HP | WIN 10 PRO |
| ALL-IN-ONE | HP | WIN 10 PRO |
| DESKTOP | DATRONE | WIN 10 PRO |
| DESKTOP | HP | WIN 10 PRO |
| DESKTOP | HP | WIN 10 PRO |
| ALL-IN-ONE | HP | WIN 10 PRO |

| | | |
|---|---|---|
| DESKTOP | ADVANCE | WIN 10 PRO |
| DESKTOP | HP | WIN 10 PRO |
| DESKTOP | ECOTREND | WIN 7 PRO |
| ALL-IN-ONE | HP | WIN 10 PRO |
| DESKTOP | HP | WIN 8.1 PRO |
| DESKTOP | ALTRON | WIN 10 PRO |
| ALL-IN-ONE | HP | WIN 10 PRO |
| ALL-IN-ONE | HP | WIN 10 PRO |
| ALL-IN-ONE | HP | WIN 10 PRO |
| DESKTOP | HP | WIN10 PRO |
| DESKTOP | ADVANCE | WIN 7 PRO |
| ALL-IN-ONE | HP | WIN 10 PRO |
| ALL-IN-ONE | HP | WIN 10 PRO |
| ALL-IN-ONE | HP | WIN 10 PRO |
| ALL-IN-ONE | HP | WIN 10 PRO |
| ALL-IN-ONE | HP | WIN 10 PRO |
| ALL-IN-ONE | HP | WIN 10 PRO |
| ALL-IN-ONE | HP | WIN 10 PRO |
| ALL-IN-ONE | HP | WIN 10 PRO |
| ALL-IN-ONE | HP | WIN 10 PRO |
| ALL-IN-ONE | HP | WIN 10 PRO |
| ALL-IN-ONE | HP | WIN 10 PRO |
| ALL-IN-ONE | HP | WIN 10 PRO |
| DESKTOP | ENKORE | WIN 10 PRO |

*Cantidad de ordenadores: 163*

- *Impresoras*

| MARCA | MODELO |
|---|---|
| HP | LASERJET M630 MFP |
| HP | LASERJET ENTERPRISE M631 MFP |
| HP | LASERJET PRO-400 |
| HP | LASERJET PRO MFP M426 - M427 |
| HP | LASERJET PRO MFP M427 |
| HP | LASERJET PRO 400 |
| KYOCERA | ECOSYS M4132idn |
| HP | LASERJET ENTERPRISE M631 MFP |
| HP | LASERJET PRO 400 |
| HP | LASERJET ENTERPRISE M631 MFP |
| HP | LASERJET PRO P1606dn |
| HP | LASERJET PRO 400 |
| HP | LASERJET M630 MFP |
| HP | LASERJET ENTERPRISE M631 MFP |
| HP | LASERJET ENTERPRISE M631 MFP |
| KYOCERA | ECOSYS M3655idn |

| | |
|---|---|
| HP | LASERJET M630 MFP |
| HP | LASERJET PRO 400 |
| HP | LASERJET M630 MFP |
| HP | LASERJET PRO P1606dn |
| HP | LASERJET PRO P1102w |
| HP | LASERJET M630 MFP |
| HP | LASERJET PRO 400 |
| HP | LASERJET ENTERPRISE M631 MFP |
| HP | LASERJET PRO 400 |
| KYOCERA | ECOSYS M3655idn |
| KYOCERA | ECOSYS M2040dn/L |
| HP | LASERJET PRO MFP M426 - M427 |
| HP | LASERJET PRO MFP M426 - M427 |
| HP | LASERJET ENTERPRISE M631 MFP |
| HP | LASERJET M630 MFP |
| HP | LASERJET PRO MFP M426 - M427 |
| HP | LASERJET PRO P1606dn |
| HP | LASERJET PRO MFP M426 - M427 |
| HP | LASERJET PRO MFP M426 - M427 |
| HP | LASERJET PRO M521dn |
| HP | LASERJET PRO P1606dn |
| HP | LASERJET M630 MFP |
| HP | LASERJET ENTERPRISE M631 MFP |
| HP | LASERJET PRO P1102w |
| HP | LASERJET PRO M102w |
| HP | LASERJET M630 MFP |
| HP | LASERJET ENTERPRISE M631 MFP |
| HP | LASERJET ENTERPRISE M631 MFP |
| HP | LASERJET ENTERPRISE M631 MFP |
| HP | LASERJET M630 MFP |
| HP | LASERJET PRO400 |
| HP | LASERJET PRO MFP M426 - M427 |
| HP | LASERJET M630 MFP |
| HP | LASERJET PRO MFP M426 - M427 |
| KYOCERA | ECOSYS M3655idn |
| HP | LASERJET PRO M227 fsw MFP |
| HP | LASERJET ENTERPRISE M631 MFP |
| EPSON | L3150 |
| HP | LASERJET PRO MFP M426 - M427 |
| CANON | PIXMA G3000 |
| HP | LASERJET PRO MFP M426 - M427 |
| HP | LASERJET M630 MFP |
| HP | LASERJET PRO MFP M426 - M427 |
| HP | LASERJET PRO MFP M426 - M427 |
| HP | LASERJET PRO 400 |

| | |
|---|---|
| HP | LASERJET ENTERPRISE M631 MFP |
| HP | LASERJET PRO MFP M426 - M427 |
| HP | LASERJET ENTERPRISE M631 MFP |

*Cantidad de Impresoras: 64*

- *Estabilizador*

| MARCA | COD. PATRIMONIAL |
|---|---|
| CDP | S/C |
| POWER | 462225215048 |
| APC | 4622200500116 |
| APC | 462200500181 |
| APC | 462200500173 |
| APC | 462200500174 |
| APC | 462200500029 |
| CDP | 462252150155 |
| APC | 462200500141 |
| APC | 462200500172 |
| APC | S/C |
| APC | 462200500152 |
| APC | 462200500183 |
| FORZA | S/C |
| AFASE | 462252150041 |
| APC | 462200500131 |
| APC | - |
| APC | 462200500047 |
| APC | 462200500011 |
| CDP | S/C |
| CDP | S/C |
| APC | S/C |
| APC | S/C |
| APC | 462200500106 |
| APC | 462200500127 |
| APC | 462200500082 |
| APC | 462200500088 |
| APC | 462200500084 |
| APC | S/C |
| APC | S/C |
| FORZA | 746452150162 |
| FORZA | 762252150165 |
| APC | 462252150169 |

*Cantidad de Estabilizador: 33*

- *ROUTER: 5*

- *UPS (Sistema de Alimentación Ininterrumpida): 1*

**COMUNICACIONES**

*-Red LAN*

*-Red inalámbrica*

*-Internet*

## Dependencia de Activos

- ❖ **Aplicaciones**
- ➢ Servicio tributario.
  - ✓ Servidor de Prueba.
    - o Arquitecto de TI
- ➢ Tramite documentario
  - ✓ Servidor de Tramite.
    - o Arquitecto de TI.
- ➢ SIAF
  - ✓ Servidor de SIAF.
    - o Arquitecto de TI.
- ➢ SIGA
  - ✓ Servidor de SIAF
    - o Arquitecto de TI.
- ➢ KOHA
  - ✓ Servidor virtual ESxi
    - o Arquitecto de TI.
- ➢ FREENAS
  - ✓ Servidor virtual ESxi
    - o Arquitecto de TI.
- ➢ Windows server 2010
  - ✓ Servidor virtual ESxi
    - o Arquitecto de TI
- ➢ Windows server 2016
  - ✓ Servidor virtual ESxi
    - o Arquitecto de TI
- ➢ Windows server 2019
  - ✓ Servidor de BD SGTM
    - o Arquitecto de TI
- ➢ Consola Antivirus
  - ✓ Servidor de Prueba
    - o Arquitecto de TI
- ❖ **Equipos**
- ➢ Servidor de trámite
  - ✓ Arquitecto de TI
    - o UPS
    - o Estabilizador
- ➢ Servidor de Prueba

- ✓ Arquitecto de TI
  - UPS
  - Estabilizador
- ➢ Servidor SIAF
  - ✓ Arquitecto de TI
    - UPS
    - Estabilizador
- ➢ Servidor Virtual ESxi
  - ✓ Arquitecto de TI
    - UPS
    - Estabilizador
- ➢ Servidor BD SGTM
  - ✓ Arquitecto de TI
    - UPS
    - Estabilizador

❖ **Centro de Cableado**

- ➢ Red LAN
  - ✓ Especialista en HELPDESK.
    - Especialista en Soporte de TI
      - Cable UTP
- ➢ Red Inalámbrica
  - ✓ Jefe de Área de OSTI
    - Arquitecto de TI
      - Router

**Dimensiones de Activos**

***[A]Autenticidad:*** ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?

Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

***[C]Confidencialidad:*** ¿Qué daño causaría que lo conociera quien no debe?

Propiedad o característica en el que la información(activo) ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

***[I]Integridad:*** Propiedad o características en el que los activos de información no han sido alterados de manera no autorizada.

***[D]Disponibilidad:*** ¿qué daño causaría no tenerlo o no poderlo usar?

Propiedad o características de los activos con acceso al mismo cuando lo requieran.

***[T]Trazabilidad del servicio y de los datos*** ¿qué daño causaría no saber a quién se le presta tal servicio? ¿qué daño causaría no saber quién accede a qué datos y qué hace con ellos?

**Valoración de Activos**

Para cada valoración se debe tener en cuenta la siguiente información:

-Criterio de valoración y dimensiones

*Escala de valoración de activos*

| N° | VALORACIÓN | CRITERIO |
|---|---|---|
| 10 | EXTREMO | Daño extremadamente grave |
| 9 | MUY ALTO | Daño Muy grave |
| 6-8 | ALTO | Daño grave |
| 3-5 | MEDIO | Daño importante |
| 1-2 | BAJO | Daño menor |
| 0 | DESPRECIABLE | Irrelevante |

| Activos | Dimensiones | | | | |
|---|---|---|---|---|---|
| | [D] | [I] | [C] | [A] | [T] |
| **Información** | 10 | 10 | 10 | 10 | 10 |
| **Software** | | | | | |
| SGTM | 9 | 9 | 9 | 9 | 9 |
| SIAF | 9 | 9 | 9 | 9 | 9 |
| SIGA | 9 | 9 | 9 | 9 | 9 |
| Antivirus | | | | | 7 |
| Sistemas Operativos | 9 | 9 | 9 | 9 | 9 |
| Servicio Tributario | 9 | 9 | 9 | 9 | 9 |
| Tramite Documentario | 9 | 9 | 9 | 9 | 9 |
| KOHA | 9 | 9 | 9 | 9 | 9 |
| FREENAS | 9 | 9 | 9 | 9 | 9 |
| **Hardware** | | | | | |
| Servidor de Tramite | 10 | 10 | 10 | 10 | 10 |
| Servidor de Prueba | 10 | 10 | 10 | 10 | 10 |
| Servidor SIAF | 10 | 10 | 10 | 10 | 10 |
| Servidor Virtual | 10 | 10 | 10 | 10 | 10 |
| Servidor BD SGTM | 10 | 10 | 10 | 10 | 10 |
| Computadora de escritorio | | | | | 8 |
| Impresora | | | | | 6 |
| Router | | | | | 8 |
| Estabilizador | | | | | 8 |
| UPS | | | | | 9 |
| **Comunicaciones** | | | | | |
| Red LAN | 8 | 8 | 8 | | 8 |
| Red Inalámbrica | 8 | 8 | 8 | | 8 |
| Internet | 8 | 8 | 8 | | 8 |

## 3.- AMENAZAS

### 3.1.- Clasificación de las Amenazas

- ✓ *[DN]Desastres Naturales (temblor, rayo, tormenta eléctrica).*
- ✓ *[OI]De Origen Industrial*

Incendios.

- ✓ *[E]Errores y fallos no intencionados*
  Mala manipulación de los sistemas de información por parte de las personas.
- ✓ *[A]Ataques intencionados*
  Robo de información, causar daño a la organización para el bienestar propio.

### 3.2.- Identificación de las Amenazas

| ACTIVOS | AMENAZAS |
|---|---|
| **INFORMACIÓN** | (DN) Desastres naturales. |
| | (OI.1) Corte de fluido eléctrico. |
| | (E.12) Información no actualizada o incorrecta. |
| **SOFTWARE** | |
| SGTM | (E.1) Error de mantenimiento / actualización de programas.<br>(E.2) Manipulación de programas.<br>(E.3) Vulnerabilidad de los programas.<br>(A.1) Difusión de software dañino.<br>(A.2) Acceso no autorizado.<br>(A.3) Modificación de Información<br>(A.4) Introducción de falsa información<br>(E.7) Destrucción de la información.<br>(A.6) Divulgación de la información<br>(E.4) Errores del administrador.<br>(E.5) Errores del Usuario.<br>(E.6) Abuso de privilegios de acceso. |
| SIAF | (E.1) Error de mantenimiento / actualización de programas.<br>(E.2) Manipulación de programas.<br>(E.3) Vulnerabilidad de los programas.<br>(A.1) Difusión de software dañino.<br>(A.2) Acceso no autorizado.<br>(A.3) Modificación de Información<br>(A.4) Introducción de falsa información<br>(E.7) Destrucción de la información.<br>(A.6) Divulgación de la información<br>(E.4) Errores del administrador.<br>(E.5) Errores del Usuario.<br>(E.6) Abuso de privilegios de acceso. |

| | |
|---|---|
| SIGA | (E.1) Error de mantenimiento / actualización de programas.<br>(E.2) Manipulación de programas.<br>(E.3) Vulnerabilidad de los programas.<br>(A.1) Difusión de software dañino.<br>(A.2) Acceso no autorizado.<br>(A.3) Modificación de Información<br>(A.4) Introducción de falsa información<br>(E.7) Destrucción de la información.<br>(A.6) Divulgación de la información<br>(E.4) Errores del administrador.<br>(E.5) Errores del Usuario.<br>(E.6) Abuso de privilegios de acceso. |
| ANTIVIRUS | (A.1) Difusión de software dañino.<br>(E.3) Vulnerabilidad de los programas.<br>(E.1) Error de mantenimiento / actualización de programas. |
| Sistemas Operativos | (E.1) Error de mantenimiento / actualización de programas.<br>(E.2) Manipulación de programas.<br>(E.3) Vulnerabilidad de los programas.<br>(A.1) Difusión de software dañino.<br>(A.2) Acceso no autorizado.<br>(A.3) Modificación de Información<br>(A.4) Introducción de falsa información<br>(E.7) Destrucción de la información.<br>(A.6) Divulgación de la información<br>(E.4) Errores del administrador.<br>(E.5) Errores del Usuario.<br>(E.6) Abuso de privilegios de acceso. |
| Servicio Tributario | (E.1) Error de mantenimiento / actualización de programas.<br>(E.2) Manipulación de programas.<br>(E.3) Vulnerabilidad de los programas.<br>(A.1) Difusión de software dañino.<br>(A.2) Acceso no autorizado.<br>(A.3) Modificación de Información<br>(A.4) Introducción de falsa información<br>(E.7) Destrucción de la información.<br>(A.6) Divulgación de la información<br>(E.4) Errores del administrador.<br>(E.5) Errores del Usuario.<br>(E.6) Abuso de privilegios de acceso. |

| | |
|---|---|
| Tramite Documentario | (E.1) Error de mantenimiento / actualización de programas.<br>(E.2) Manipulación de programas.<br>(E.3) Vulnerabilidad de los programas.<br>(A.1) Difusión de software dañino.<br>(A.2) Acceso no autorizado.<br>(A.3) Modificación de Información<br>(A.4) Introducción de falsa información<br>(E.7) Destrucción de la información.<br>(A.6) Divulgación de la información<br>(E.4) Errores del administrador.<br>(E.5) Errores del Usuario.<br>(E.6) Abuso de privilegios de acceso. |
| KOHA | (E.1) Error de mantenimiento / actualización de programas.<br>(E.2) Manipulación de programas.<br>(E.3) Vulnerabilidad de los programas.<br>(A.1) Difusión de software dañino.<br>(A.2) Acceso no autorizado.<br>(A.3) Modificación de Información<br>(A.4) Introducción de falsa información<br>(E.7) Destrucción de la información.<br>(A.6) Divulgación de la información<br>(E.4) Errores del administrador.<br>(E.5) Errores del Usuario.<br>(E.6) Abuso de privilegios de acceso. |
| FREENAS | (E.1) Error de mantenimiento / actualización de programas.<br>(E.2) Manipulación de programas.<br>(E.3) Vulnerabilidad de los programas.<br>(A.1) Difusión de software dañino.<br>(A.2) Acceso no autorizado.<br>(A.3) Modificación de Información<br>(A.4) Introducción de falsa información<br>(E.7) Destrucción de la información.<br>(A.6) Divulgación de la información<br>(E.4) Errores del administrador.<br>(E.5) Errores del Usuario.<br>(E.6) Abuso de privilegios de acceso. |
| **HARDWARE** | |

| | |
|---|---|
| Servidor de Tramite | (DN.1) Desastres naturales.<br>(OI.2) Incendios.<br>(OI.3) Avería de origen físico y lógico.<br>(OI.1) Corte de fluido eléctrico.<br>(O1.4) Condiciones inadecuadas de temperatura o humedad.<br>(A.7) Perdida de equipos.<br>(E.7) Errores de mantenimiento / actualización de equipos(hardware).<br>(E.8) Caída del sistema por agotamiento de recursos.<br>(A.2) Acceso no autorizado.<br>(A.8) Manipulación del hardware.<br>(A.9) Robo de equipos.<br>(A.10) Ataque destructivo. |
| Servidor de Prueba | (DN.1) Desastres naturales.<br>(OI.2) Incendios.<br>(OI.3) Avería de origen físico y lógico.<br>(OI.1) Corte de fluido eléctrico.<br>(O1.4) Condiciones inadecuadas de temperatura o humedad.<br>(A.7) Perdida de equipos.<br>(E.7) Errores de mantenimiento / actualización de equipos(hardware).<br>(E.8) Caída del sistema por agotamiento de recursos.<br>(A.2) Acceso no autorizado.<br>(A.8) Manipulación del hardware.<br>(A.9) Robo de equipos.<br>(A.10) Ataque destructivo. |

| | |
|---|---|
| Servidor SIAF | (DN.1) Desastres naturales.<br>(OI.2) Incendios.<br>(OI.3) Avería de origen físico y lógico.<br>(OI.1) Corte de fluido eléctrico.<br>(O1.4) Condiciones inadecuadas de temperatura o humedad.<br>(A.7) Perdida de equipos.<br>(E.7) Errores de mantenimiento / actualización de equipos(hardware).<br>(E.8) Caída del sistema por agotamiento de recursos.<br>(A.2) Acceso no autorizado.<br>(A.8) Manipulación del hardware.<br>(A.9) Robo de equipos.<br>(A.10) Ataque destructivo. |
| Servidor Virtual | (DN.1) Desastres naturales.<br>(OI.2) Incendios.<br>(OI.3) Avería de origen físico y lógico.<br>(OI.1) Corte de fluido eléctrico.<br>(O1.4) Condiciones inadecuadas de temperatura o humedad.<br>(A.7) Perdida de equipos.<br>(E.7) Errores de mantenimiento / actualización de equipos(hardware).<br>(E.8) Caída del sistema por agotamiento de recursos.<br>(A.2) Acceso no autorizado.<br>(A.8) Manipulación del hardware.<br>(A.9) Robo de equipos.<br>(A.10) Ataque destructivo. |

| | |
|---|---|
| Servidor BD SGTM | (DN.1) Desastres naturales.<br>(OI.2) Incendios.<br>(OI.3) Avería de origen físico y lógico.<br>(OI.1) Corte de fluido eléctrico.<br>(OI.4) Condiciones inadecuadas de temperatura o humedad.<br>(A.7) Perdida de equipos.<br>(E.7) Errores de mantenimiento / actualización de equipos(hardware).<br>(E.8) Caída del sistema por agotamiento de recursos.<br>(A.2) Acceso no autorizado.<br>(A.8) Manipulación del hardware.<br>(A.9) Robo de equipos.<br>(A.10) Ataque destructivo. |
| Computadora de Escritorio | (DN) Desastres naturales.<br>(OI.3) Avería de origen físico y lógico.<br>(OI.4) Condiciones inadecuadas de temperatura o humedad.<br>(E.7) Errores de mantenimiento / actualización de equipos(hardware).<br>(E.8) Caída del sistema por agotamiento de recursos.<br>(A.11) Abuso privilegios de accesos.<br>(A.12) Uso no previsto. |
| Impresoras | (OI.3) Avería de origen físico y lógico.<br>(DN) Incendios.<br>(E.7) Errores de mantenimiento/ actualización de equipos(hardware).<br>(DN) Desastres Naturales. |
| Router | (DN) Desastres Naturales.<br>OI.3) Avería de origen físico y lógico.<br>(OI.4) Condiciones inadecuadas de temperatura o humedad. |
| Estabilizador | (DN) Desastres naturales.<br>(E.9) Manipulación inadecuada del equipo.<br>(A.9) Robo de equipo. |
| UPS | (DN) Desastres naturales.<br>(E.9) Manipulación inadecuada del equipo.<br>(A.9) Robo de equipo. |
| **COMUNICACIONES** | |
| | (OI.5) Fallo de servicio de comunicaciones.<br>(A.13) Suplantación de la identidad del usuario. |

| | |
|---|---|
| Red LAN | (A.2) Acceso no autorizado.<br>(E.9) Errores de re-encaminamiento.<br>(E.10) Errores de secuencias. |
| Red Inalámbrica | (OI.5) Fallo de servicio de comunicaciones.<br>(E.9) Errores de re-encaminamiento. |
| Internet | (OI.5) Fallo de servicio de comunicaciones.<br>(E.11) Alteración de Información. |

### 3.3.- Descripción de amenazas sobre los activos

**Información**

- Desastres naturales: Incidentes que se producen sin intervención humana. Rayos, tormentas eléctricas, terremoto, etc.
- Corte de fluido eléctrico: Un desastre de origen industrial.
- Información no actualizada o incorrecta: afectara directamente a la dimensión de integridad en un nivel muy alto ya que arrojaría información errónea a la hora de las consultas y transacciones en cada uno de los procesos dentro de las labores de la municipalidad provincial de Maynas.

**Software**

- Error de mantenimiento / actualización de programas: Defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.
- Acceso no autorizado: El atacante consigue ingresar a los recursos del sistema sin tener autorización sobre ello.
- Modificación de Información: Afectara directamente la dimensión de integridad de la información en un nivel muy alto. Porque se verán afectados los datos almacenados en los activos pertenecientes a este grupo causando un caos informático.
- Errores del administrador: Equivocaciones de personas con responsabilidades de instalación y operación.
- Errores de Usuario: Equivocaciones de las personas cuando usan los servicios, datos, etc.
- Abuso de privilegios de acceso: Mal uso de derechos especiales otorgados a cuentas privilegiadas, accidental o intencionalmente.
- Vulnerabilidad de los programas: Defectos en el código que dan pie a un posible atacante comprometer la integridad y confidencialidad de la información.
- Destrucción de la información: Perdida accidental de información.
- Divulgación de la información: afectaría considerablemente la dimensión de confidencialidad.

**Hardware (Servidores)**

- Desastres naturales: incidentes que se producen sin intervención humana. Rayos, tormentas eléctricas, terremoto, etc.
- Incendios: Incidentes que se producen con intervención humana.

- Avería de origen físico y lógico: Fallos en los equipos y/o programas puede ser debido a un defecto de origen.
- Corte de fluido eléctrico: Un desastre de origen industrial.
- Condiciones inadecuadas de temperatura o humedad: Deficiencias en la aclimatación de los locales. Se debe a la ubicación en la cual no son apropiadas de los equipos informáticos.
- Errores de mantenimiento: Mala manipulación del mantenimiento físico por parte de las personas autorizadas.
- Acceso no autorizado: El atacante consigue ingresar a los recursos del sistema sin tener autorización sobre ello.
- Caída del sistema por agotamiento de recursos: Las carencias de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
- Manipulación del hardware: Alteración intencionada del funcionamiento de los equipos, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.
- Robo de equipos: Personas externas no autorizadas sustraen los equipos informáticos para beneficio propio.
- Ataque destructivo: Ocasiona daños en los equipos informáticos por medio de los malware dañando los discos duros, procesador, placa, etc.

**Computadora de escritorio**

- Desastres naturales: incidentes que se producen sin intervención humana. Rayos, tormentas eléctricas, terremoto, etc.
- Avería de origen físico y lógico: Fallos en los equipos y/o programas puede ser debido a un defecto de origen o sobrevenida durante el funcionamiento del sistema.
- Condiciones inadecuadas de temperatura o humedad: Deficiencias en la aclimatación de los locales. Se debe a la ubicación en la cual no son apropiadas de los equipos informáticos.
- Errores de mantenimiento/actualización de equipos(hardware): Mala manipulación del mantenimiento físico por parte de las personas autorizadas.
- Caída del sistema por agotamiento de recursos: Las carencias de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
- Abuso de privilegios de acceso: Mal uso de derechos especiales otorgados a cuentas privilegiadas, accidental o intencionalmente.
- Uso no previsto: utilización de los recursos del sistema para fines no previstos, típicamente de interés personal.

**Impresoras**

- Avería de origen físico y lógico: Fallos en los equipos y/o programas puede ser debido a un defecto de origen o sobrevenida durante el funcionamiento del sistema
- Incendios: Posibilidad de que el fuego acabe con los recursos del sistema.
- Errores de mantenimiento/ actualización de equipos(hardware): Mala manipulación del mantenimiento físico por parte de las personas autorizadas.
- Desastres Naturales: Incidentes que se producen sin intervención humana. Rayos, tormentas eléctricas, terremoto, etc.

**Router**

- Desastres Naturales: Incidentes que se producen sin intervención humana. Rayos, tormentas eléctricas, terremoto, etc.
- Avería de origen físico y lógico: Fallos en los equipos y/o programas puede ser debido a un defecto de origen o sobrevenida durante el funcionamiento del sistema.
- Condiciones inadecuadas de temperatura o humedad: Deficiencias en la aclimatación de los locales. Se debe a la ubicación en la cual no son apropiadas de los equipos informáticos.

**Estabilizador**

- Desastres naturales: Incidentes que se producen sin intervención humana. Rayos, tormentas eléctricas, terremoto, etc.
- Manipulación inadecuada del equipo: Alteración intencionada del funcionamiento de los equipos sin ninguna capacitación previa.
- Robo de equipo: Personas externas no autorizadas sustraen los equipos informáticos para beneficio propio.

**UPS**

- Desastres naturales: Incidentes que se producen sin intervención humana. Rayos, tormentas eléctricas, terremoto, etc.
- Manipulación inadecuada del equipo: Alteración intencionada del funcionamiento de los equipos sin ninguna capacitación previa.
- Robo de equipo: Personas externas no autorizadas sustraen los equipos informáticos para beneficio propio.

**Comunicaciones**

**Red LAN**

- Fallo de servicio de comunicaciones: Cese de la capacidad de transmitir datos de un sitio a otro.
- Suplantación de la identidad del usuario: Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios.
- Acceso no autorizado: El atacante consigue ingresar a los recursos del sistema sin tener autorización sobre ello.
- Errores de re-encaminamiento: Envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información donde o por donde no es debido.
- Errores de secuencias: Alteración accidental del orden de los mensajes transmitidos.

**Red inalámbrica**

- Fallo de servicio de comunicaciones: Cese de la capacidad de transmitir datos de un sitio a otro.
- Errores de re-encaminamiento: Envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información donde o por donde no es debido.

**Internet**

- Fallo de servicio de comunicaciones: Cese de la capacidad de transmitir datos de un sitio a otro.
- Alteración de la Información: Alteración accidental de la información.

**3.4.- Valoración de las amenazas**

La probabilidad de ocurrencia es más compleja de determinar y expresar. A veces se modela numéricamente como una frecuencia de ocurrencia. Es habitual usar 1 año como referencia de forma que se recurre a la tasa anual de ocurrencia como medida de la probabilidad de que algo ocurra.

*Dimensiones*

[D] Disponibilidad.

[I] Integridad de los datos.

[C] Confidencialidad de los datos.

[A] Autenticidad de los usuarios y la información.

[T] Trazabilidad del servicio y de los datos.

*Probabilidad de Ocurrencia*

| | | |
|---|---|---|
| 100 | Muy frecuente | A diario |
| 10 | Frecuente | Mensualmente |
| 1 | Normal | Una vez al año |
| 0,1 | Poco frecuente | Cada varios años |
| 0,01 | Muy poco frecuente | Siglos |

Tabla: Valoración de los Activos vs Amenazas

| ACTIVOS | AMENAZAS | FRECUENCIA |
|---|---|---|
| INFORMACIÓN | (DN) Desastres naturales. | 0,1 |
| | (OI.1) Corte de fluido eléctrico. | 10 |
| | (E.12) Información no actualizada o incorrecta. | 10 |
| | (E.1) Error de mantenimiento / actualización de programas. | 1 |
| | (E.2) Manipulación de programas. | 1 |
| | (E.3) Vulnerabilidad de los programas. | 1 |
| | (A.1) Difusión de software dañino. | 1 |
| | (A.2) Acceso no autorizado. | 1 |
| | (A.3) Modificación de Información | 1 |

| | | |
|---|---|---|
| **SOFTWARE** | (A.4) Introducción de falsa información | 1 |
| | (A.5) Destrucción de la información. | 1 |
| | (A.6) Divulgación de la información | 1 |
| | (E.4) Errores del administrador. | 10 |
| | (E.5) Errores del Usuario. | 100 |
| | (E.6) Abuso de privilegios de acceso. | 10 |
| **Hardware** | | |
| SERVIDORES | (DN) Desastres naturales. | 0,1 |
| | (OI.2) Incendios. | 1 |
| | (OI.3) Avería de origen físico y lógico | 1 |
| | (OI.1) Corte de fluido eléctrico | 10 |
| | (OI.4) Condiciones inadecuadas de temperatura o humedad. | 1 |
| | (A.7) Perdida de equipos. | 1 |
| | (E.7) Errores de mantenimiento / actualización de equipos(hardware). | 1 |
| | (E.8) Caída del sistema por agotamiento de recursos. | 10 |
| | (A.2) Acceso no autorizado. | 1 |
| | (A.8) Manipulación del hardware. | 1 |
| | (A.9) Robo de equipos. | 1 |
| | (A.10) Ataque destructivo. | 1 |
| Computadora de Escritorio | (DN) Desastres naturales. | 0,1 |
| | (OI.3) Avería de origen físico y lógico | 1 |
| | (OI.4) Condiciones inadecuadas de temperatura o humedad. | 1 |
| | (E.7) Errores de mantenimiento / actualización de equipos (hardware). | 1 |
| | (E.8) Caída del sistema por agotamiento de recursos | 1 |
| | (A.11) Abuso de privilegios de accesos | 1 |
| | (A.12) Uso no Previsto | 10 |
| IMPRESORAS | (DN) Desastres naturales. | 0,1 |
| | (OI.3) Avería de origen físico y lógico. | 1 |
| | (DN) Incendios. | 1 |
| | (E.7) Errores de mantenimiento/ actualización de equipos. | 10 |
| ROUTER | (DN) Desastres Naturales | 1 |
| | (OI.3) Avería de origen físico y lógico | 10 |
| | (OI.4) Condiciones inadecuadas de temperatura o humedad | 1 |
| ESTABILIZADORES | (DN) Desastres naturales. | 0,1 |
| | (E.9) Manipulación inadecuada del equipo | 1 |
| | (A.9) Robo de equipo. | 1 |
| | (DN) Desastres naturales. | 1 |

| | | |
|---|---|---|
| UPS | (E.9) Manipulación inadecuada del equipo | 1 |
| | (A.9) Robo de equipo. | 1 |
| **COMUNICACIONES** | | |
| Red LAN | (A.2) Acceso no autorizado. | 1 |
| | (E.9) Errores de re-encaminamiento. | 1 |
| | (E.10) Errores de secuencias. | 1 |
| | OI.5) Fallo de servicio de comunicaciones. | 10 |
| | (A.13) Suplantación de la identidad del usuario. | 1 |
| Red Inalámbrico | (OI.5) Fallo de servicio de comunicaciones. | 10 |
| | (E.9) Errores de re-encaminamiento. | 1 |
| Internet | (OI.5) Fallo de servicio de comunicaciones. | 10 |
| | (E.11) Alteración de Información. | 1 |

## 4.- DETERMINACIÓN DEL IMPACTO POTENCIAL

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo el impacto que estas tendrían sobre el sistema.

4.1.- **Clasificación del Impacto Potencial.** – El impacto potencial se muestra en la siguiente escala con colores que indican su severidad.

Escala de impacto potencial

| Valoración | Criterio |
|---|---|
| 4 | MUY ALTO |
| 3 | ALTO |
| 2 | MEDIO |
| 1 | BAJO |

### 4.2.- Identificación del Impacto Potencial

| ACTIVOS | AMENAZAS | [D] | [I] | [C] | [A] | [T] |
|---|---|---|---|---|---|---|
| **Información** | (DN)Desastres naturales. | 4 | | | | |
| | (OI.2) Corte de fluido eléctrico. | 4 | | | | |
| | (E.12) Información no actualizada o incorrecta. | 4 | 4 | 4 | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| Software | (E.1) Error de mantenimiento / actualización de programas. | | | | | |
| | (E.2) Manipulación de programas. | | 4 | 4 | | |
| | (E.3) Vulnerabilidad de los programas. | | 4 | 4 | | |
| | (A.1) Difusión de software dañino. | 4 | 4 | 4 | | |
| | (A.2) Acceso no autorizado. | | 4 | 4 | 4 | |
| | A.3) Modificación de Información. | | 4 | 4 | | |
| | (A.4) Introducción de falsa información. | | 4 | | | |
| | (A.5) Destrucción de la información. | 4 | 4 | | | |
| | (A.6) Divulgación de la información | | | 4 | | |
| | (E.4) Errores del administrador. | 4 | 4 | | | |
| | (E.5) Errores del Usuario. | | | | | |
| | (E.6) Abuso de privilegios de acceso. | 4 | 4 | | | |
| **Hardware** | | | | | | |
| Servidores | (DN) Desastres naturales. | 4 | 4 | | | |
| | (OI.2) Incendios. | 4 | 4 | | | |
| | (OI.1) Corte de fluido eléctrico. | 4 | | | | |
| | (OI.3) Avería de origen físico y lógico. | 4 | | | | |
| | (A.2) Acceso no autorizado. | 4 | | | | |
| | (OI.4) Condiciones inadecuadas de temperatura o humedad. | 4 | | | | |
| | (A.7) Perdida de equipos. | 4 | | | | |
| | (E.7) Errores de mantenimiento / actualización de equipos(hardware). | 2 | | | | |
| | (E.8) Caída del sistema por agotamiento de recursos. | 4 | | | | |
| | (A.8) Manipulación del hardware. | 4 | | | | |
| | (A.9) Robo de equipos. | 4 | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | (A.10) Ataque destructivo. | 4 | | | | |
| Computadora de Escritorio | (DN) Desastres naturales. | 2 | | | | |
| | (OI.3) Avería de origen físico y lógico. | 2 | | | | |
| | (OI.4) Condiciones inadecuadas de temperatura o humedad. | 2 | | | | |
| | (E.7) Errores de mantenimiento / actualización de hardware. | 2 | | | | |
| | (E.8) Caída del sistema por agotamiento de recursos. | 4 | | | | |
| | (A.11) Abuso de privilegios de accesos. | 4 | | | | |
| | (A.12) Uso no previsto. | 3 | | | | |
| Impresoras | (DN) Desastres naturales. | 2 | | | | |
| | (OI.3) Avería de origen físico y lógico. | 2 | | | | |
| | (DN) Incendios. | 2 | | | | |
| | (E.7) Errores de mantenimiento/ actualización de equipos. | 2 | | | | |
| Router | (DN) Desastres naturales. | 4 | | | | |
| | (OI.3) Avería de origen físico y lógico. | 3 | | | | |
| | (OI.4) Condiciones inadecuadas de temperatura o humedad. | 3 | | | | |
| Estabilizadores | (DN) Desastres naturales. | 4 | | | | |
| | (E.9) Manipulación inadecuada del equipo. | 4 | | | | |
| | (A.9) Robo de equipo. | 4 | | | | |
| UPS | (DN) Desastres naturales. | 4 | | | | |
| | (E.9) Manipulación inadecuada del equipo. | 4 | | | | |
| | (A.9) Robo de equipo. | 4 | | | | |
| **Comunicaciones** | | | | | | |
| | (A.2) Acceso no autorizado. | | 2 | | | |
| | (E.9) Errores de encaminamiento. | | 2 | | | |
| | (E.10) Errores de secuencias | 3 | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| Red LAN | (OI.5) Fallo de servicio de comunicaciones. | 4 | | | | |
| | (A.13) Suplantación de la identidad del usuario. | 4 | 4 | 4 | | |
| Red Inalámbrica | (OI.5) Fallo de servicio de comunicaciones. | 4 | | | | |
| | (E.9) Errores de Re encaminamiento | 4 | 4 | | | |
| Internet | (OI.5) Fallo de servicio de comunicaciones. | 4 | | | | |
| | (E.11) Alteración de información. | 4 | | | | |

## 5.- DETERMINACIÓN DEL RIESGO POTENCIAL

**5.1.- Clasificación del Riesgo Potencial.** – El riesgo potencial se muestra en la siguiente escala con colores que indican su grado crítico.

Escala de Riesgos

| Valoración | Criterio |
|---|---|
| 4 | Muy alto |
| 3 | Alto |
| 2 | Medio |
| 1 | Bajo |

### 5.2.- Identificación del Riesgo Potencial

*Valoración riesgo potencial*

| ACTIVOS | AMENAZAS | [D] | [I] | [C] | [A] | [T] |
|---|---|---|---|---|---|---|
| **Información** | (DN)Desastres naturales. | 4 | | | | |
| | (OI.1) Corte de fluido eléctrico. | 4 | | | | |
| | (E.12) Información no actualizada o incorrecta. | 4 | 4 | 4 | | |
| | (E.1) Error de mantenimiento / actualización de programas. | | | | | |
| | (E.2) Manipulación de programas. | | 4 | 4 | | |
| | (E.3) Vulnerabilidad de los programas. | | 4 | 4 | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| Software | (A.1) Difusión de software dañino. | 4 | 4 | 4 | | |
| | (A.2) Acceso no autorizado. | | 4 | 4 | 4 | |
| | A.3) Modificación de Información. | | 4 | 4 | | |
| | (A.4) Introducción de falsa información. | | 4 | | | |
| | (A.5) Destrucción de la información. | 4 | 4 | | | |
| | (A.6) Divulgación de la información | | | 4 | | |
| | (E.4) Errores del administrador. | 4 | 4 | | | |
| | (E.5) Errores del Usuario. | | | | | |
| | (E.6) Abuso de privilegios de acceso. | 4 | 4 | | | |
| **Hardware** | | | | | | |
| Servidores | (DN) Desastres naturales. | 4 | 4 | | | |
| | (OI.2) Incendios. | 4 | 4 | | | |
| | (OI.1) Corte de fluido eléctrico. | 4 | | | | |
| | (OI.3) Avería de origen físico y lógico. | 4 | | | | |
| | (A.2) Acceso no autorizado. | 4 | | | | |
| | (OI.4) Condiciones inadecuadas de temperatura o humedad. | 4 | | | | |
| | (A.7) Perdida de equipos. | 4 | | | | |
| | (E.7) Errores de mantenimiento / actualización de equipos(hardware). | 2 | | | | |
| | (E.8) Caída del sistema por agotamiento de recursos. | 4 | | | | |
| | (A.8) Manipulación del hardware. | 4 | | | | |
| | (A.9) Robo de equipos. | 4 | | | | |
| | (A.10) Ataque destructivo. | 4 | | | | |
| | (DN) Desastres naturales. | 2 | | | | |
| | (OI.3) Avería de origen físico y lógico. | 2 | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| Computadora de Escritorio | (OI.4) Condiciones inadecuadas de temperatura o humedad. | 2 | | | | |
| | (E.7) Errores de mantenimiento / actualización de hardware. | 2 | | | | |
| | (E.8) Caída del sistema por agotamiento de recursos. | 4 | | | | |
| | (A.11) Abuso de privilegios de accesos. | 4 | | | | |
| | (A.12) Uso no previsto. | 3 | | | | |
| Impresoras | (DN) Desastres naturales. | 2 | | | | |
| | (OI.3) Avería de origen físico y lógico. | 2 | | | | |
| | (DN) Incendios. | 2 | | | | |
| | (E.7) Errores de mantenimiento/ actualización de equipos. | 2 | | | | |
| Router | (DN) Desastres naturales. | 4 | | | | |
| | (OI.3) Avería de origen físico y lógico. | 3 | | | | |
| | (OI.4) Condiciones inadecuadas de temperatura o humedad. | 3 | | | | |
| Estabilizadores | (DN) Desastres naturales. | 4 | | | | |
| | (E.9) Manipulación inadecuada del equipo. | 4 | | | | |
| | (A.9) Robo de equipo. | 4 | | | | |
| UPS | (DN) Desastres naturales. | 4 | | | | |
| | (E.9) Manipulación inadecuada del equipo. | 4 | | | | |
| | (A.9) Robo de equipo. | 4 | | | | |
| **Comunicaciones** | | | | | | |
| Red LAN | (A.2) Acceso no autorizado. | | 2 | | | |
| | (E.9) Errores de encaminamiento. | | 2 | | | |
| | (E.10) Errores de secuencias | 3 | | | | |
| | (OI.5) Fallo de servicio de comunicaciones. | 4 | | | | |
| | (A.13) Suplantación de la identidad del usuario. | 4 | 4 | 4 | | |
| | (OI.5) Fallo de servicio de comunicaciones. | 4 | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| Red Inalámbrica | (E.9) Errores de Re encaminamiento | 4 | 4 | | | |
| Internet | (OI.5) Fallo de servicio de comunicaciones. | 4 | | | | |
| | (E.11) Alteración de información. | 4 | | | | |

## 6.- ANÁLISIS DE SALVAGUARDAS

### 6.1.- Clasificación de Salvaguardas

| Nivel | Estado | Significado |
|---|---|---|
| L0 | Inexistente | Inexistente |
| L1 | Inicial / ad hoc | Iniciado |
| L2 | Reproducible pero intuitivo | Parcialmente realizado |
| L3 | Proceso definido | En funcionamiento |
| L4 | Gestionado y medible | Monitorizado |
| L5 | Optimizado | Mejora continua |

### 6.2.- Identificación de Salvaguardas

**Protección de la información**

- Inventario de activos de información.
- Clasificación de la información
- Aseguramiento de la disponibilidad.
- Protección criptográfica de la información.

**Protección de las aplicaciones**

- Inventario de aplicaciones.
- Normativa sobre el uso correcto de las aplicaciones.
- Procedimiento de uso de las aplicaciones.
- Se protegen los derechos de propiedad intelectual de las aplicaciones.
- Copia de seguridad.
- Se aplican perfiles de seguridad.
- Se controla la integridad del código ejecutable.
- Seguridad de aplicaciones.
- Seguridad de los ficheros de datos de las aplicaciones.
- Seguimiento permanente de las actualizaciones y parches.
- Control de versiones de todas las actualizaciones de software.
- Realización por personal debidamente autorizado.
- Se retienen copias de las versiones anteriores se software como medida de precaución para contingencia.
- Registro de toda actualización.
- Documentación.

**Protección de los equipos informáticos**

- Normativa sobre el uso correcto de los equipos.
- Protección de los equipos.
- Inventario de equipos.
- Procedimiento de uso de equipamiento.
- Aseguramiento de la disponibilidad.
- Se aplican perfiles de seguridad.
- El mantenimiento lo realiza personal debidamente autorizado.
- Se ejecutan regularmente las rutinas de diagnóstico.
- Se monitorizan fallos e incidentes.
- Se registran los fallos reales de mantenimiento preventivo y correctivo.
- Se hacen copias de seguridad de las configuraciones.
- Formación del personal en configuración del equipo.
- Los usuarios están concienciados y reciben formación sobre el uso seguro de sistemas y recursos disponibles.

**Protección de Comunicaciones**

Para garantizar las comunicaciones cuando están utilizando el internet es necesario utilizar las siguientes salvaguardas:

- Herramienta de control de contenido con filtros actualizados
- Se controla la configuración de los navegadores
- Se registra la descarga
- Se registra la navegación web
- Se dispone la normativa sobre el uso de Internet
- Herramienta de monitorización de trafico

**Protección de los Estabilizadores**

- Se dispondrá de un inventario.
- Se siguen las indicaciones de los fabricantes y proveedores.
- Climatización.
- Medidas frente a posibles robos.

**Protección del UPS**

- Se dispondrá de un inventario.
- Se siguen las indicaciones de los fabricantes y proveedores.
- Climatización
- Medida frente a posibles robos.

### 6.3.- Valoración de las salvaguardas

| Salvaguardar | TIPO |
|---|---|
| **Aplicaciones** | |
| Inventario de aplicaciones. | L3 |
| Normativa sobre el uso correcto de las aplicaciones | L2-L3 |
| Procedimientos de uso de las aplicaciones. | L2 |

| | |
|---|---|
| Se protegen los derechos de propiedad intelectual de las aplicaciones. | L2-L3 |
| Copias de seguridad. | L2-L3 |
| Se aplican perfiles de seguridad | L3 |
| Se controla la integridad del código ejecutable. | L3 |
| Seguridad de las aplicaciones. | L2-L3 |
| Seguridad de los ficheros de datos de las aplicaciones. | L3 |
| Se hace un seguimiento permanente de actualizaciones y parches. | L3 |
| Control de versiones de todas las actualizaciones de software. | L3 |
| Realización por personal debidamente autorizado | L2 |
| Se retienen copias de las versiones anteriores de software como medidas de precaución para contingencia. | L2 |
| Registro de toda actualización | L2 |
| Documentación | L2 |
| **Hardware** | |
| Normativa sobre el uso correcto de los equipos | L2-L3 |
| Inventario de equipos. | L2 |
| Procedimientos de uso del equipamiento. | L2 |
| Se aplican perfiles de seguridad. | L3 |
| El mantenimiento lo realiza personal debidamente autorizado. | L3 |
| Se ejecutan regularmente las rutinas de diagnóstico. | L2 |
| Se monitorizan fallos e incidentes. | L3 |
| Se registran los fallos reales de mantenimiento preventivo y correctivo. | L3 |
| Se hacen copias de seguridad de la configuración. | L3 |
| Formación del personal en configuración del equipo. | L3 |
| Los usuarios están concienciados y reciben formación sobre el uso seguro de sistemas y recursos disponibles. | L2 |
| **Comunicaciones** | |
| Herramienta de control de contenido con filtros actualizados. | L2 |
| Se controla la configuración de los navegadores | L2-L3 |
| Se registra la descarga | L3 |
| Se registra la navegación web | L3-L4 |
| Se dispone la normativa sobre el uso de Internet | L3 |
| Herramienta de monitorización de trafico | L3 |
| **Estabilizador** | |
| Se dispondrá de un inventario | L3 |
| Se siguen las indicaciones del fabricante y proveedor | L3 |
| Climatización | L3 |
| Medidas frente a posibles robos | L3 |
| **UPS** | |
| Se dispondrá de un inventario | L3 |
| Se siguen las indicaciones del fabricante y proveedor | L3 |
| Climatización | L3 |
| Medidas frente a posibles robos | L3 |

## 7.- DETERMINACIÓN DEL IMPACTO RESIDUAL

**7.1.- Clasificación del Impacto Residual.** El impacto residual se muestra en la siguiente escala con colores que indican su severidad.

Escala de impacto residual

| Valoración | Criterio |
|---|---|
| 4 | MUY ALTO |
| 3 | ALTO |
| 2 | MEDIO |
| 1 | BAJO |

**7.2.- Identificación del Impacto Residual**

| ACTIVOS | AMENAZAS | [D] | [I] | [C] | [A] | [T] |
|---|---|---|---|---|---|---|
| **Información** | (DN)Desastres naturales. | 3 | | | | |
| | (OI.1) Corte de fluido eléctrico. | 3 | | | | |
| | (E.12) Información no actualizada o incorrecta. | 3 | 3 | 3 | | |
| Software | (E.1) Error de mantenimiento / actualización de programas. | 3 | | | | |
| | (E.2) Manipulación de programas. | | 3 | 3 | | |
| | (E.3) Vulnerabilidad de los programas. | | 3 | | | |
| | (A.1) Difusión de software dañino. | 3 | 3 | 3 | | |
| | (A.2) Acceso no autorizado. | 3 | 3 | 3 | 3 | |
| | A.3) Modificación de Información. | 3 | 3 | 3 | | |
| | (A.4) Introducción de falsa información. | 2 | 3 | | | |
| | (A.5) Destrucción de la información. | 3 | 3 | | | |
| | (A.6) Divulgación de la información | | | 3 | | |
| | (E.4) Errores del administrador. | 3 | 3 | | | |
| | (E.5) Errores del Usuario. | 2 | 2 | | | |
| | (E.6) Abuso de privilegios de acceso. | 3 | 3 | 3 | | |
| **Hardware** | | | | | | |
| | (DN) Desastres naturales. | 3 | 3 | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| Servidores | (OI.2) Incendios. | 3 | 3 | | | |
| | (OI.1) Corte de fluido eléctrico. | 3 | | | | |
| | (OI.3) Avería de origen físico y lógico. | 3 | | | | |
| | (A.2) Acceso no autorizado. | 3 | | | | |
| | (OI.4) Condiciones inadecuadas de temperatura o humedad. | 3 | | | | |
| | (A.7) Perdida de equipos. | 3 | | | | |
| | (E.7) Errores de mantenimiento / actualización de equipos(hardware). | 1 | | | | |
| | (E.8) Caída del sistema por agotamiento de recursos. | 3 | | | | |
| | (A.8) Manipulación del hardware. | 3 | | | | |
| | (A.9) Robo de equipos. | 3 | | | | |
| | (A.10) Ataque destructivo. | 3 | | | | |
| Computadora de Escritorio | (DN) Desastres naturales. | 1 | | | | |
| | (OI.3) Avería de origen físico y lógico. | 1 | | | | |
| | (OI.4) Condiciones inadecuadas de temperatura o humedad. | 1 | | | | |
| | (E.7) Errores de mantenimiento / actualización de hardware. | 1 | | | | |
| | (E.8) Caída del sistema por agotamiento de recursos. | 3 | | | | |
| | (A.11) Abuso de privilegios de accesos. | 3 | | | | |
| | (A.12) Uso no previsto. | 2 | | | | |
| Impresoras | (DN) Desastres naturales. | 1 | | | | |
| | (OI.3) Avería de origen físico y lógico. | 1 | | | | |
| | (DN) Incendios. | 1 | | | | |
| | (E.7) Errores de mantenimiento/ actualización de equipos. | 1 | | | | |
| | (DN) Desastres naturales. | 3 | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| Router | (OI.3) Avería de origen físico y lógico. | 2 | | | | |
| | (OI.4) Condiciones inadecuadas de temperatura o humedad. | 2 | | | | |
| Estabilizadores | (DN) Desastres naturales. | 3 | | | | |
| | (E.9) Manipulación inadecuada del equipo. | 3 | | | | |
| | (A.9) Robo de equipo. | 3 | | | | |
| UPS | (DN) Desastres naturales. | 3 | | | | |
| | (E.9) Manipulación inadecuada del equipo. | 3 | | | | |
| | (A.9) Robo de equipo. | 3 | | | | |
| **Comunicaciones** | | | | | | |
| Red LAN | (A.2) Acceso no autorizado. | | 1 | | | |
| | (E.9) Errores de encaminamiento. | | 1 | | | |
| | (E.10) Errores de secuencias | 2 | | | | |
| | (OI.5) Fallo de servicio de comunicaciones. | 3 | | | | |
| | (A.13) Suplantación de la identidad del usuario. | 3 | 3 | 3 | | |
| Red Inalámbrica | (OI.5) Fallo de servicio de comunicaciones. | 3 | | | | |
| | (E.9) Errores de Re encaminamiento | 3 | 3 | | | |
| Internet | (OI.5) Fallo de servicio de comunicaciones. | 3 | | | | |
| | (E.11) Alteración de información. | 3 | 3 | 3 | | |

## 8 DETERMINACIÓN DEL RIESGO RESIDUAL

**8.1.- Clasificación del Riesgo Residual.** - El riesgo residual se muestra en la siguiente escala con colores que indican su criticidad.

*Escala de riesgo residual*

| Valoración | Criterio |
|---|---|
| 4 | MUY ALTO |
| 3 | ALTO |
| 2 | MEDIO |
| 1 | BAJO |

**8.2.- Identificación del Riesgo Residual**

| ACTIVOS | AMENAZAS | [D] | [I] | [C] | [A] | [T] |
|---|---|---|---|---|---|---|
| **Información** | (DN)Desastres naturales. | 3 | | | | |
| | (OI.1) Corte de fluido eléctrico. | 3 | | | | |
| | (E.12) Información no actualizada o incorrecta. | 3 | 3 | | | |
| Software | (E.1) Error de mantenimiento / actualización de programas. | 2 | | | | |
| | (E.2) Manipulación de programas. | | 3 | 3 | | |
| | (E.3) Vulnerabilidad de los programas. | | 3 | 3 | | |
| | (A.1) Difusión de software dañino. | 3 | 3 | 3 | | |
| | (A.2) Acceso no autorizado. | | 3 | 3 | 3 | |
| | A.3) Modificación de Información. | | 3 | 3 | | |
| | (A.4) Introducción de falsa información. | | 2 | | | |
| | (A.5) Destrucción de la información. | 3 | 3 | | | |
| | (A.6) Divulgación de la información | | | 3 | | |
| | (E.4) Errores del administrador. | 3 | 3 | | | |
| | (E.5) Errores del Usuario. | | | | | |
| | (E.6) Abuso de privilegios de acceso. | 3 | 3 | 3 | | |
| **Hardware** | | | | | | |
| S | (DN) Desastres naturales. | 2 | 2 | | | |
| | (OI.2) Incendios. | 2 | 2 | | | |
| | (OI.1) Corte de fluido eléctrico. | 2 | | | | |
| | (OI.3) Avería de origen físico y lógico. | 2 | | | | |
| | (A.2) Acceso no autorizado. | | | | 3 | |
| Servidores | (OI.4) Condiciones inadecuadas de temperatura o humedad. | 3 | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | (A.7) Perdida de equipos. | 3 | | | | |
| | (E.7) Errores de mantenimiento / actualización de equipos(hardware). | 1 | | | | |
| | (E.8) Caída del sistema por agotamiento de recursos. | 2 | | | | |
| | (A.8) Manipulación del hardware. | | | 3 | | |
| | (A.9) Robo de equipos. | 3 | | | | |
| | (A.10) Ataque destructivo. | 2 | | | | |
| Computadora de Escritorio | (DN) Desastres naturales. | 1 | | | | |
| | (OI.3) Avería de origen físico y lógico. | 1 | | | | |
| | (OI.4) Condiciones inadecuadas de temperatura o humedad. | 1 | | | | |
| | (E.7) Errores de mantenimiento / actualización de hardware. | 1 | | | | |
| | (E.8) Caída del sistema por agotamiento de recursos. | 2 | | | | |
| | (A.11) Abuso de privilegios de accesos. | 2 | | | | |
| | (A.12) Uso no previsto. | | 3 | 3 | | |
| Impresoras | (DN) Desastres naturales. | 1 | | | | |
| | (OI.3) Avería de origen físico y lógico. | 1 | | | | |
| | (DN) Incendios. | 1 | | | | |
| | (E.7) Errores de mantenimiento/ actualización de equipos. | 1 | | | | |
| Router | (DN) Desastres naturales. | 2 | | | | |
| | (OI.3) Avería de origen físico y lógico. | 2 | | | | |
| | (OI.4) Condiciones inadecuadas de temperatura o humedad. | 2 | | | | |
| Estabilizadores | (DN) Desastres naturales. | 2 | | | | |
| | (E.9) Manipulación inadecuada del equipo. | 2 | | | | |
| | (A.9) Robo de equipo. | 2 | | | | |
| | (DN) Desastres naturales. | 2 | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| UPS | (E.9) Manipulación inadecuada del equipo. | 2 | | | | |
| | (A.9) Robo de equipo. | 2 | | | | |
| **Comunicaciones** | | | | | | |
| Red LAN | (A.2) Acceso no autorizado. | | 1 | | | |
| | (E.9) Errores de Re encaminamiento. | | | 2 | | |
| | (E.10) Errores de secuencias | | | | | |
| | (OI.5) Fallo de servicio de comunicaciones. | 2 | | | | |
| | (A.13) Suplantación de la identidad del usuario. | 2 | 2 | 2 | | |
| Red Inalámbrica | (OI.5) Fallo de servicio de comunicaciones. | 2 | | | | |
| | (E.9) Errores de Re encaminamiento | 2 | 2 | | | |
| Internet | (OI.5) Fallo de servicio de comunicaciones. | 2 | | | | |
| | (E.11) Alteración de información. | 2 | | | | |

# III. PROCESO DE GESTIÓN DE RIESGO

Después de haber analizado el análisis de riesgo queda a la vista los impactos y riesgos que está expuesta la organización.

Lo que ha llegado a una calificación de cada riesgo significativo, determinándose:

- Si es crítico en el sentido de que requiere atención urgente.
- Es grave en el sentido de que requiere atención.
- Es apreciable en el sentido de que pueda ser objeto de estudio para su tratamiento.

## 3.1 Identificación de riesgos críticos

En toda organización los activos están expuestos a riesgos, pero lo importante es conocer cuáles de los activos poseen mayor nivel de riesgo con el fin de implementar salvaguardas para evitar que las amenazas se materialicen.

**Selección de activos con mayor nivel de riesgo.**

| ACTIVOS | [D] | [I] | [C] | [A] | [T] |
|---|---|---|---|---|---|
| **Información** | | | | | |
| (DN) Desastres Naturales | 3 | | | | |
| (OI.2) Corte de fluido eléctrico. | 3 | | | | |
| (E) Información no actualizada o incorrecta | 3 | 3 | 3 | | |
| **Hardware** | | | | | |
| **Servidores** | | | | | |
| (A.2) Acceso no autorizado. | | | | 3 | |

| | | | | | |
|---|---|---|---|---|---|
| (OI.4) Condiciones inadecuadas de temperatura o humedad. | 3 | | | | |
| A.7) Perdida de equipos. | 3 | | | | |
| (A.9) Robo de equipos. | 3 | | | | |
| (A.8) Manipulación del hardware. | | | 3 | | |
| **Computadora de Escritorio** | | | | | |
| (A.12) Uso no previsto. | | 3 | 3 | | |
| **Software** | | | | | |
| **Aplicaciones** | | | | | |
| (E.2) Manipulación de programas. | | 3 | 3 | | |
| (E.3) Vulnerabilidad de los programas. | | 3 | 3 | | |
| (A.1) Difusión de software dañino. | 3 | 3 | 3 | | |
| (A.2) Acceso no autorizado. | | 3 | 3 | 3 | |
| A.3) Modificación de Información. | | 3 | 3 | | |
| (A.5) Destrucción de la información. | 3 | 3 | | | |
| (A.6) Divulgación de la información. | | | 3 | | |
| (E.4) Errores del administrador. | 3 | 3 | | | |
| (E.6) Abuso de privilegios de acceso. | 3 | 3 | 3 | | |

## a. Calificación del Riesgo

- Información. Es el activo más esencial en la organización y su amenaza de más alto nivel es la de un **Desastre Natural** afectando a la disponibilidad de la información.

Las medidas para poder reducir el riesgo de este activo son:

  - Copias de seguridad(backup).
  - Cloud backup ya que es mucho más económico, no se necesita de un lugar físico para implementarlo. Se puede acceder de cualquier lugar y en cualquier momento. Es mucho más seguro ya que cuentan con un alto estándar de ciberseguridad en sus instalaciones e interfaces web.
  - Centro de datos secundario en una de las periferias de la cual el MPM está a cargo.

- Corte de fluido eléctrico es una amenaza con una alta posibilidad que se presente, a pesar de ello no depende al 100% de la MPM por qué se puede dar por problemas de la empresa eléctrica.
  La medida para poder reducir este riesgo es:
  - **Adquisición de UPS** de mayor duración de horas para prolongar las horas de soporte en caso de pérdida o corte del fluido eléctrico.
- Computadora de escritorio. La amenaza que tiene un nivel de riesgo alto es la de Uso no previsto. Esta es una causa común ya que algunos empleados puedan instalar programas que no tengan que ver con el trabajo sino con su uso personal como juegos, etc. Distrayendo sus actividades en horarios laborales.

Las medidas para poder reducir el riesgo actual de este activo son:

  - La de bloquear los accesos de puerto USB ya que los Hackers manejan malware personalizados que apuntan a unidades USB.
  - Concientizar a los usuarios de la municipalidad provincial de Maynas sobre la Seguridad de la Información.

- Aplicaciones es un activo que pertenece a la capa Software, las amenaza que tienen un nivel de alto riesgo es manipulación de los programas, vulnerabilidad de los programas, difusión de software dañino, acceso no autorizado, modificación de información, destrucción de la información, divulgación de la información, errores del administrador, abuso de privilegios de acceso que afectan a la disponibilidad, integridad, confidencialidad y autentificación.

Las medidas para reducir el riesgo de este activo son:

  - La adquisición de software con licencia.
  - Instalaciones de parches y actualizaciones.
  - Control de acceso a los programas a través de claves de usuarios.

- Servidores es un activo que pertenece a la capa de Hardware, las amenaza que tiene un nivel de alto riesgo es la manipulación de Hardware, acceso no autorizado, perdida de equipo, condiciones inadecuadas de temperatura/humedad. Estas amenazas están latentes porque no existe un lugar adecuado donde solo ingrese el personal autorizado permitiendo que cualquier empleado pueda hacer uso de este equipo quedando inseguros.

La medida para reducir el riesgo de este activo es:

  - Implementación de un centro de datos con las políticas de seguridad que están establecidas en las ISO:
    - ✓ 27001 (Sistema de Gestión de la Seguridad de la Información)
    - ✓ 9001 (Gestión de la Calidad)
    - ✓ 14001 (Gestión Medioambiental)

# IV. Conclusiones

- Identificación de los activos, amenazas y se estableció las salvaguardas necesarias para la continuidad de los Sistemas de Información, Tecnologías de Información en la Municipalidad Provincial de Maynas (MPM).
- Determinar que el análisis y gestión de riesgo es indispensable para nuestro de negocio, empresa, organización, etc. Ya que así podemos identificar las posibles amenazas que dificultan la continuidad de nuestras operaciones periódicamente.

# V. Recomendaciones

- Realizar Plan de Continuidad y Contingencia de Tecnologías de la Información paralas amenazas identificadas mediante un análisis de vulnerabilidades.
- Seguir en continuidad con el Plan de Formación y Concientización en Seguridad de TI para todos los trabajadores de la Municipalidad Provincial de Maynas (MPM).