**Tabla de contenido**

[NORMAS 2](#_Toc480235990)

[Definiciones y Siglas 2](#_Toc480235991)

[introducción 3](#_Toc480235992)

[7.5.3. EVALUACIÓN DEL RIESGO 3](#_Toc480235993)

[7.5.3.1 IDENTIFICACIÓN DEL RIESGO 3](#_Toc480235994)

[7.5.3.2 ANÁLISIS DEL RIESGO 4](#_Toc480235995)

[7.5.3.3. VALORACIÓN DEL RIESGO 6](#_Toc480235996)

[7.5.4. TRATAMIENTO DEL RIESGO 7](#_Toc480235997)

[Anexos 7](#_Toc480235998)

**GESTION DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN**

## NORMAS

ISO/IEC 31000: 2009

ISO/IEC 27005: 2011

Metodología Magerit

# Definiciones y Siglas

**Activo:** Es aquello que tiene valor para la institución y por tanto debe protegerse.

**Activo de Información:** En seguridad de la información, corresponde a aquellos datos, información, sistemas y elementos relacionados con la tecnología de la información que contiene o manipula información y tiene valor para la institución.

**Propietario o responsable del activo de información:** Es aquella persona que responde por la razonabilidad del sistema de información o por un proceso a su cargo y por ende define quién puede tener acceso a la información, quién y a quién se le puede entregar información. Es quién puede autorizar cualquier modificación a datos que se encuentran en ambiente de producción, previa evaluación y justificación de dicho cambio.

**Custodio del activo de información:** encargado de resguardar la información, debe seguir los lineamientos definidos por el propietario de la información para su protección.

**Confidencialidad:** Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados.

**Integridad:** Propiedad de salvaguardar la exactitud y estado completo de la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.

**Disponibilidad:** Propiedad de que la información sea accesible y utilizable en el tiempo y la forma que esta sea requerida**.**

**Riesgo:** Efecto de la incertidumbre sobre los objetivos (ISO 27000 2.68)

**Apetito de riesgo:** Cantidad o tipo de riesgo que una organización está dispuesta a perseguir o retener.

**Riesgo inherente:** Identificación de los riesgos sin tomar en cuenta los controles.

**Gestión del riesgo:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo (ISO 31000 2.2)

**Apreciación del riesgo:** Proceso global que comprende la identificación del riesgo, el análisis del riesgo y la evaluación del riesgo (ISO 31000 2.14)

**Identificación del riesgo:** Proceso para encontrar, reconocer y describir el riesgo (ISO 31000 2.15)

**Análisis del riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel del riesgo (ISO 31000 2.21)

**Evaluación del riesgo:** Proceso de comparación de los resultados del análisis del riesgo con los criterios de riesgo para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables. (ISO 31000 2.24)

**Tratamiento del riesgo:** proceso para modificar el riesgo (ISO 31000 2.25)

**Riesgo residual:** Riesgo remanente después del tratamiento del riesgo (ISO 31000 2.27)

**Comunicación y consulta:** Procesos iterativos y continuos que realiza una organización para proporcionar u obtener información y para establecer el diálogo con las partes interesadas, en relación con la gestión del riesgo (ISO 31000 2.12)

**Amenaza:** Causa potencial de un incidente no deseado que puede causar daño a un sistema o a una organización (ISO 27000 2.45)

**Fuente de riesgo:** elemento que solo o en combinación con otros, tiene el potencial intrínseco de generar un riesgo (ISO 31000 2.16)

**Vulnerabilidad:** debilidad de un activo o de un control que puede ser explotada por una amenaza (ISO 27000 2.46)

**Impacto/consecuencia:** Resultado de un suceso que afecta a los objetivos (ISO 31000 2.18)

**Probabilidad:** Posibilidad de que algún hecho se produzca (ISO 31000 2.19)

**Nivel de riesgo:** Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su probabilidad (ISO 31000 2.23)

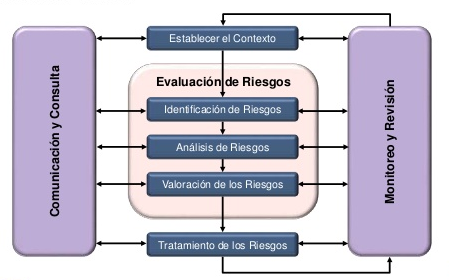
**Metodología Magerit:** Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

# introducción

Para desarrollar el documento nos basamos en el modelo de proceso de Gestión de riesgos en la Seguridad de la Información de la norma ISO/IEC 27005:2011, que es el mismo que la norma ISO 31000, ambas normas deben ser consideradas para gestionar los riesgos de acuerdo con los requisitos de la norma ISO/IEC 27001:2013.

La Figura 1 Muestra el modelo de proceso.

**Figura 1 Modelo de proceso según ISO/IEC 27005 e ISO/IEC 31000**



## EVALUACIÓN DEL RIESGO

## IDENTIFICACIÓN DEL RIESGO

Para la identificación del riesgo se deberá contar con un Inventario de activos de la información que administra el área de TI, este listado tendrá el formato expuesto en el punto 7.5.2.1

A partir de este inventario se realizarán entrevistas a los administradores, propietarios y diferentes partes interesadas de cada activo sobre la Confidencialidad, Integridad y Disponibilidad del Activo según la Tabla 1. Valoraciones a los activos de información.

Para obtener un mejor resultado en las entrevistas que se realicen al personal implicado, se pueden utilizar el método HAZOP, DELPHI u otro que nos permita obtener información consistente.

**Tabla 1 Valoraciones a los activos de la información**

|  |  |  |  |
| --- | --- | --- | --- |
| **Característica** | **Pregunta** | **Valoración** | **Entrevistados** |
| Confidencialidad | Que impacto se ocasiona si personas no autorizadas acceden a la información? | Muy Alto = 5  Alto = 4  Medio = 3  Bajo = 2  Muy Bajo = 1 | Administradores, propietarios y partes interesadas |
| Disponibilidad | Que impacto se ocasiona si el activo no estuviera disponible? | Muy Alto = 5  Alto = 4  Medio = 3  Bajo = 2  Muy Bajo = 1 | Administradores, propietarios y partes interesadas |
| Integridad | Que impacto se ocasiona si se modifica la información sin control? | Muy Alto = 5  Alto = 4  Medio = 3  Bajo = 2  Muy Bajo = 1 | Administradores, propietarios y partes interesadas |

A partir de este inventario y de su valoración en términos de Confidencialidad, Integridad y Disponibilidad se obtiene la Criticidad del activo, bajo la fórmula:

***Criticidad= Redondear [(Confidencialidad + Integridad + Disponibilidad)/3]***

Con este valor de criticidad se obtendrá el Inventario de Activos Críticos administrador por el área de TI, Anexo B.

A partir de este inventario de activos críticos se elaborará la Identificación de riesgos de los Activos administrados por el área de TI, Anexo C. Esta identificación consta de un listado exhaustivo del riesgo por cada activo de información, en esta etapa aún no se conoce la probabilidad y el impacto de los riesgos identificados.

Para la clasificación de los activos se utiliza como referencia la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información MAGERIT (Anexo D) para Tipos de activos, Catálogo de Amenazas y Catálogo de vulnerabilidades.

## ANÁLISIS DEL RIESGO

En esta etapa se deberá evaluar el impacto y la probabilidad de incidentes para finalmente determinar el Nivel de Riesgos

La forma de expresar las consecuencias y la probabilidad, así como la manera en que éstas se combinan para determinar un nivel de riesgo, debería corresponder al tipo de riesgo, a la información disponible y al objetivo para el que se utiliza el resultado de la apreciación del riesgo.

Para obtener datos en esta etapa se puede seguir el Cuestionario 1 en las entrevistas a los Administradores, propietarios y partes interesadas en el Activo, sin embargo este puede cambiar de acuerdo al tipo de organización y sus procesos.

**Cuestionario 1.**

|  |  |
| --- | --- |
| Código del Activo |  |
| Descripción |  |
| Administrador principal |  |
| Administrador de respaldo |  |
| Propietario del Activo |  |
| Proceso de la organización a la que pertenece |  |

El Sistema/aplicación/servicio es monitoreado?

Tipo de información que procesa

Tiene impacto en el SGSI?

Tiene requerimiento legales?

Cuenta con segregación adecuada de funciones?

Es centro de conflictos?

Ha sido objeto de reclamaciones/sanciones?

Partes interesadas que hacen uso

Cuenta con documentación completa?

Cuenta con un sistema de Alta disponibilidad?

Dependen de él otros activos?

Oportunidades de mejora identificados

Finalmente para obtener las vulnerabilidades el nivel de riesgo se combinarán los valores de Probabilidad e Impacto mediante la Matriz de Riesgos (Fig 2):

**Fig. 2 Matriz de riesgos**



El análisis del Riesgo finaliza con la valoración del riesgo (Crítico, Alto, Medio, Bajo e Irrelevante) por cada activo de información

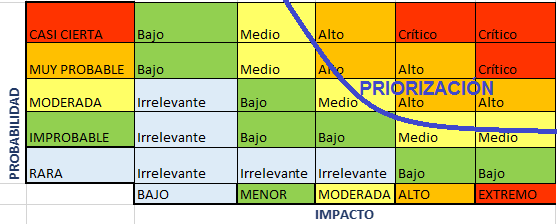
## VALORACIÓN DEL RIESGO

De esta etapa debe obtenerse como resultado la priorización de los riesgos obtenidos en el análisis del riesgo, la evaluación ayudará a la toma de decisiones, determinando los riesgos a tratar y a la prioridad para implementar el tratamiento.

Por ejemplo se puede decidir realizar un tratamiento a solamente los niveles Alto y Crítico y dejando a los niveles Medio, Bajo e irrelevante como riesgos menores o triviales, esto dependerá del análisis que se realice la alta dirección de una organización en coordinación con el área de TI.

La priorización puede ser establecida a partir del apetito de riesgo que previamente defina la organización, ver Fig. 3.

**Fig. 3 Priorización del riesgo**



## TRATAMIENTO DEL RIESGO

Una vez concluida la apreciación del riesgo, el tratamiento consiste en llegar a un acuerdo sobre una o más opciones relevantes para cambiar la probabilidad de ocurrencia, el impacto, o ambos.

En este contexto se deberá elegir Evitar, Retener, aumentar, compartir, remover o modificar el riesgo este nuevo análisis debe tomar en cuenta considerando el costo/beneficio de cada riesgo.

El Líder del área de TI en coordinación con las partes interesadas (administrador y propietarios de los activos) deberá tomar la decisión sobre las opciones de tratamiento del riesgo, esta decisión puede incluir:

* Las razones que justifican la selección de las opciones de tratamiento incluyendo los beneficios previstos.
* Las personas responsables de la aprobación del plan y las personas responsables de la implementación del plan.
* Las acciones propuestas.
* Las necesidades de recursos, incluyendo las contingencias.
* Las medidas del desempeño y las restricciones.
* Los requisitos en materia de información y de seguimiento.
* Indicadores de efectividad del control.
* Presupuesto destinado para el control
* El calendario y la programación

Una vez tomada esta decisión, se deberá identificar y planificar las actividades para la aplicación de estas decisiones, mismas que deben ser clasificadas por orden de prioridad.

El entregable para esta etapa es el Plan de tratamiento del riesgo (Anexo E), que toma en cuenta aspectos tales como las actividades para el tratamiento, persona responsable de la implementación, recursos, métodos de evaluación y plazos de cumplimientos.

# Anexos

|  |  |  |
| --- | --- | --- |
| **Nro.** | **Anexo** | **Título del Anexo** |
| 1 | A | Formato para el Inventario de Activos |
| 2 | B | Inventario de Activos Críticos |
| 3 | C | Identificación de riesgos de los Activos |
| 4 | D | Tablas Magerit |
| 5 | E | Plan de tratamiento del Riesgo |

**ANEXO A: Formato para el Inventario de Activos**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Código interno** | **Nombre del Activo** | **Descripción** | **Tipo de Activo** | **Ubicación** | **Unidad Responsable** | **Responsable** | **Custodio** | **Confidencialidad** | **Disponibilidad** | **Integridad** | **Criticidad** | **Fecha de ingreso** | **Fecha de Salida** | **Observaciones** |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

**ANEXO B: Inventario de Activos Críticos**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Código interno** | **Nombre del Activo** | **Descripción** | **Tipo de Activo** | **Ubicación** | **Unidad Responsable** | **Responsable** | **Custodio** | **Criticidad** | **Fecha de ingreso** | **Fecha de Salida** | **Observaciones** |
|  |  |  |  |  |  |  |  |  |  |  |  |

**ANEXO C: Identificación de riesgos de los Activos**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  | **Riesgo Inherente** | | |  | **Degradación del Activo** | | | **Riesgo Residual** | | |  |  |  |
| **Activo** | **Tipo de Activo** | **Amenaza** | **Situación** | **Vulnerabilidad** | **Probabilidad** | **Impacto** | **Nivel de Riesgo** | **Descripción controles establecidos** | **Disponibilidad** | **Integridad** | **Confidencialidad** | **Probabilidad** | **Impacto** | **Nivel de exposición** |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

**ANEXO D: Tablas Magerit**

Tipos de Datos e información

|  |  |  |  |
| --- | --- | --- | --- |
| DATOS E INFORMACIÓN | Nomenclatura | Tipos de datos/información | Los datos son el corazón que permite a una organización prestar sus servicios. La información es un activo abstracto que será almacenado en equipos o soportes de información (normalmente agrupado como ficheros o bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos. |
| [files] | ficheros |
| [backup] | copias de respaldo |
| [conf] | datos de configuración |
| [int] | datos de gestión interna |
| [password] | credenciales (ej. contraseñas) |
| [auth] | datos de validación de credenciales |
| [acl] | datos de control de acceso |
| [log] | registro de actividad |
| [source] | código fuente |
| [exe] | código ejecutable |
| [test] | datos de prueba |
| CLAVES CRIPTOGRÁFICAS | Nomenclatura | Claves criptográficas | Las criptografía se emplea para proteger el secreto o autenticar a las partes. Las claves criptográficas, combinando secretos e información pública, son esenciales para garantizar el funcionamiento de los mecanismos criptográficos. (1) Por ejemplo, DES, 3-DES, AES, etc. (2) (2) Por ejemplo, RSA, Diffie-Hellman, curvas elípticas, etc. |
| [info] | Protección de la información |
| [encrypt] | claves de cifra |
| [shared\_secret] | secreto compartido (clave simétrica) (1) |
| [public\_encryption] | clave pública de cifra (2) |
| [public\_decryption] | clave privada de descifrado (2) |
| [sign] | claves de firma |
| [shared\_secret] | secreto compartido (clave simétrica) |
| [public\_signature] | clave privada de firma (2) |
| [public\_verification] | clave pública de verificación de firma (2) |
| [com] | protección de las comunicaciones |
| [channel] | claves de cifrado del canal |
| [authentication] | claves de autenticación |
| [verification] | claves de verificación de autenticación |
| [disk] | cifrado de soportes de información |
| [encrypt] | claves de cifra |
| [x509] | certificados de clave pública |
| SERVICIOS | Nomenclatura | Tipos de servicios | Función que satisface una necesidad de los usuarios (del servicio). Esta sección contempla servicios prestados por el sistema. (1) Localización de personas (páginas blancas), empresas o servicios (páginas amarillas); Permitiendo la identificación y facilitando los atributos que caracterizan al elemento determinado (2) Servicios que permiten altas y bajas de usuarios de los sistemas, incluyendo su caracterización Y activando los servicios de aprovisionamiento asociados a sus cambios de estado respecto de la organización. (3) Servicios asociados a sistemas de criptografía de clave pública, incluyendo especialmente la gestión de certificados |
| [anon] | anónimo (sin requerir identificación del usuario) |
| [pub] | al público en general (sin relación contractual) |
| [ext] | a usuarios externos (bajo una relación contractual) |
| [int] | interno (a usuarios de la propia organización) |
| [www] | world wide web |
| [telnet] | acceso remoto a cuenta local |
| [email] | correo electrónico |
| [file] | almacenamiento de ficheros |
| [ftp] | transferencia de ficheros |
| [edi] | intercambio electrónico de datos |
| [dir] | sevicio de directorio (1) |
| [idm] | gestión de identidades (2) |
| [ipm] | gestión de privilegios |
| [pki] | PKI – Infraestructura de clave pública (3) |
| APLICACIONES SOFTWARE | Nomenclatura | Tipos de Aplicaciones (Software) | Con múltiples denominaciones (programas, aplicativos, desarrollos, etc.) se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios. No preocupa en este apartado el denominado “código fuente” o programas que serán datos de Interés comercial, a valorar y proteger como tales. Dicho código aparecería como datos. |
| [prp] | desarrollo propio (in house) |
| [sub] | desarrollo a medida (subcontratado) |
| [std] | estándar (off the shelf) |
| [browser] | navegador web |
| [www] | servidor de presentación |
| [app] | servidor de aplicaciones |
| [email\_client] | cliente de correo electrónico |
| [email\_server] | servidor de correo electrónico |
| [file] | servidor de ficheros |
| [dbms] | sistema de gestión de bases de datos |
| [tm] | monitor transaccional |
| [office] | ofimática |
| [av] | anti virus |
| [os] | sistema operativo |
| [hypervisor] | gestor de máquinas virtuales |
| [ts] | servidor de terminales |
| [backup] | sistema de backup |
| EQUIPOS INFORMÁTICOS (HARDWARE) | Nomenclatura | Tipos de equipos informáticos (hardware) | Dícese de los medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos. (1) Se caracterizan por haber pocos, frecuentemente uno sólo, ser económicamente gravosos y requerir un entorno específico para su operación. Son difícilmente reemplazables en caso de destrucción. (2) Se caracterizan por haber varios, tener un coste económico medio tanto de adquisición como de mantenimiento e imponer requerimientos estándar como entorno de operación. No es difícil reemplazarlos en caso de destrucción. (3) Se caracterizan por ser multitud, tener un coste económico relativamente pequeño e imponer solamente unos requerimientos mínimos como entorno de operación. Son fácilmente reemplazables en caso de destrucción. (4) Se caracterizan por ser equipos afectos a la clasificación como informática personal que, además, son fácilmente transportables de un sitio a otro, pudiendo estar tanto dentro del recinto propio de la organización como en cualquier otro lugar. (5) Son aquellos equipos preparados para hacerse cargo inmediato de los equipos en producción. (6) Dícese de impresoras y servidores de impresión. (7) Son los equipos que se instalan entre dos zonas de confianza. (8) Dícese de equipamiento necesario para transmitir datos: routers, módems, etc. |
| [host] | grandes equipos (1) |
| [mid] | equipos medios (2) |
| [pc] | informática personal (3) |
| [mobile] | informática móvil (4) |
| [pda] | agendas electrónicas |
| [vhost] | equipo virtual |
| [backup] | equipamiento de respaldo (5) |
| [peripheral] | periféricos |
| [print] | medios de impresión (6) |
| [scan] | escáneres |
| [crypto] | dispositivos criptográficos |
| [bp] | dispositivo de frontera (7) |
| [network] | soporte de la red (8) |
| [modem] | módems |
| [hub] | concentradores |
| [switch] | conmutadores |
| [router] | encaminadores |
| [bridge] | pasarelas |
| [firewall] | cortafuegos |
| [wap] | punto de acceso inalámbrico |
| [pabx] | centralita telefónica |
| [ipphone] | teléfono IP |
| REDES DE COMUNICACIONES | Nomenclatura | Tipos de redes de comunicaciones |  |
| [PSTN] | red telefónica |
| [ISDN] | rdsi (red digital) |
| [X25] | X25 (red de datos) |
| [ADSL] | ADSL |
| [pp] | punto a punto |
| [radio] | comunicaciones radio |
| [wifi] | red inalámbrica |
| [mobile] | telefonía móvil |
| [sat] | por satélite |
| [LAN] | red local |
| [MAN] | red metropolitana |
| [Internet] | Internet |
| SOPORTES DE INFORMACIÓN | Nomenclatura | Tipos de soportes de información | En este epígrafe se consideran dispositivos físicos que permiten almacenar información de forma permanente o, Al menos, durante largos periodos de tiempo. |
| [electronic] | electrónicos |
| [disk] | discos |
| [vdisk] | discos virtuales |
| [san] | almacenamiento en red |
| [disquette] | disquetes |
| [cd] | cederrón (CD-ROM) |
| [usb] | memorias USB |
| [dvd] | DVD |
| [tape] | cinta magnética |
| [mc] | tarjetas de memoria |
| [ic] | tarjetas inteligentes |
| [non\_electronic] | no electrónicos |
| [printed] | material impreso |
| [tape] | cinta de papel |
| [film] | microfilm |
| [cards] | tarjetas perforadas |
| EQUIPAMIENTO AUXILIAR | Nomenclatura | Tipos de equipamiento auxiliar | En este epígrafe se consideran otros equipos que sirven de soporte a los sistemas de información, sin estar Directamente relacionados con datos. |
| [power] | fuentes de alimentación |
| [ups] | sistemas de alimentación ininterrumpida |
| [gen] | generadores eléctricos |
| [ac] | equipos de climatización |
| [cabling] | cableado |
| [wire] | cable eléctrico |
| [fiber] | fibra óptica |
| [robot] | robots |
| [tape] | ... de cintas |
| [disk] | ... de discos |
| [supply] | suministros esenciales |
| [destroy] | equipos de destrucción de soportes de información |
| [furniture] | mobiliario: armarios, etc |
| [safe] | cajas fuertes |
| INSTALACIONES | Nomenclatura | Tipos de instalaciones | En este epígrafe entran los lugares donde se hospedan los sistemas de información y comunicaciones. |
| [site] | recinto |
| [building] | edificio |
| [local] | cuarto |
| [mobile] | plataformas móviles |
| [car] | vehículo terrestre: coche, camión, etc. |
| [plane] | vehículo aéreo: avión, etc. |
| [ship] | vehículo marítimo: buque, lancha, etc. |
| [shelter] | contenedores |
| [channel] | canalización |
| [backup] | instalaciones de respaldo |
| PERSONAS | Nomenclatura | Tipos de Pesonal | En este epígrafe aparecen las personas relacionadas con los sistemas de información. |
| [ue] | usuarios externos |
| [ui] | usuarios internos |
| [op] | operadores |
| [adm] | administradores de sistemas |
| [com] | administradores de comunicaciones |
| [dba] | administradores de BBDD |
| [sec] | administradores de seguridad |
| [des] | desarrolladores / programadores |
| [sub] | subcontratas |
| [prov] | proveedores |

**Catálogo de Amenazas:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Catálogo de Amenazas (MAGERIT)** | **Degradación del Activo** | | |
| **Disponibilidad** | **Integridad** | **Confidencialidad** |
| **Desastres Naturales** |  |  |  |
| Fuego (Incendios) | x |  |  |
| Daños por agua (Inundaciones) | x |  |  |
| Desastres Naturales | x |  |  |
| **De origen industrial** |  |  |  |
| Fuego (Incendios) | x |  |  |
| Daños por agua (Inundaciones) | x |  |  |
| Desastres industriales | x |  |  |
| Contaminación mecánica | x |  |  |
| Contaminación electromagnética | x |  |  |
| Avería de origen físico o lógico | x |  |  |
| Corte del suministro eléctrico | x |  |  |
| Condiciones inadecuadas de temperatura o humedad | x |  |  |
| Fallo de servicios de comunicaciones | x |  |  |
| Interrupción de otros servicios y suministros esenciales | x |  |  |
| Degradación de los soportes de almacenamiento de la información | x |  |  |
| Emanaciones electromagnéticas |  |  | x |
| **Errores y fallos no intencionados** |  |  |  |
| Errores de los usuarios | x | x | x |
| Errores del administrador | x | x | x |
| Errores de monitorización (log) |  | x |  |
| Errores de configuración |  | x |  |
| Deficiencias en la organización | x |  |  |
| Difusión de software dañino | x | x | x |
| Errores de [re-]encaminamiento |  |  | x |
| Errores de secuencia |  | x |  |
| Escapes de información |  | x | x |
| Alteración accidental de la información |  | x |  |
| Destrucción de información | x |  |  |
| Fugas de información |  |  | x |
| Vulnerabilidades de los programas (software) | x | x | x |
| Errores de mantenimiento / actualización de programas (software) |  | x | x |
| Errores de mantenimiento / actualización de equipos (hardware) | x |  |  |
| Caída del sistema por agotamiento de recursos | x |  |  |
| Pérdida de equipos | x |  | x |
| Indisponibilidad del personal | x |  |  |
| **Ataques intencionados** |  |  |  |
| Manipulación de los registros de actividad (log) |  | x |  |
| Manipulación de la configuración | x | x | x |
| Suplantación de la identidad del usuario | x | x | x |
| Abuso de privilegios de acceso | x | x | x |
| Uso no previsto | x | x | x |
| Difusión de software dañino | x | x | x |
| [Re-]encaminamiento de mensajes |  |  | x |
| Alteración de secuencia |  | x |  |
| Acceso no autorizado |  | x | x |
| Análisis de tráfico |  |  | x |

**Catálogo de Vulnerabilidades**

|  |  |
| --- | --- |
| **Tipo Activo** | **Vulnerabilidad** |
| Equipamiento informático | Susceptibilidad a la humedad, el polvo y la suciedad |
| Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento |
| Ausencia de esquemas de reemplazo periódico |
| Sensibilidad a la radiación electromagnética |
| Ausencia de un eficiente control de cambios en la configuración |
| Susceptibilidad a las variaciones de temperatura |
| Susceptibilidad a las variaciones de voltaje |
| Falta de cuidado en la disposición final |
| Almacenamiento sin protección |
| Copia no controlada |
| Software - Aplicaciones informáticas | Defectos bien conocidos de software |
| Ausencia o insuficiencia de pruebas de software |
| Ausencia de terminación de la sesión cuando se abandona la estación de trabajo |
| Ausencia de pistas de auditoría |
| Asignación errada de los derechos de acceso |
| Software ampliamente distribuido |
| Interfaz de usuario compleja |
| Ausencia de documentación |
| Configuración incorrecta de parámetros |
| Tablas de contraseñas sin protección |
| Habilitación de servicios innecesarios |
| Fechas incorrectas |
| Software nuevo o inmaduro |
| Especificaciones incompletas o no claras para los desarrolladores |
| Ausencia de control de cambios eficaz |
| En términos de tiempo utilización de datos errados en los programas de aplicación |
| Ausencia de mecanismos de identificación y autentificación como la autentificación de usuario |
| Gestión deficiente de las contraseñas |
| Falla en la producción de informes de gestión |
| Ausencia de copias de respaldo |
| Redes de comunicaciones | Ausencia de pruebas de envío o recepción de mensajes |
| Lineas de comunicación sin protección |
| Tráfico sensible sin protección |
| Conexión deficiente de los cables |
| Punto único de falla |
| Ausencia de identificación y autentificación de emisor y receptor |
| Arquitectura insegura de la red |
| Transferencia de contraseñas en claro |
| Gestión inadecuada de la red (Tolerancia a fallos en el enrutamiento) |
| Personal | Ausencia del personal |
| Procedimientos inadecuados de contratación |
| Entrenamiento insuficiente en seguridad |
| Uso incorrecto de software y hardware |
| Falta de conciencia acerca de la seguridad |
| Ausencia de mecanismos de monitoreo |
| Trabajo no supervisado de personal externo o de limpieza |
| Ausencia de políticas para el uso de los medios de telecomunicaciones y mensajería |
| Instalaciones | Uso inadecuado o descuidado del control de acceso físico a las edificaciones o recintos |
| Ubicación en un área susceptible de inundación |
| Red energética inestable |
| Ausencia de protección física de la edificación, puertas y ventanas |

**ANEXO E: Plan de tratamiento del Riesgo**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Activo y Riesgo | Tratamiento (evitar, mantener,etc) | Razones que justifican el tratamiento | Responsables dela aprobación del Plan | Descripción de Actividades | Recursos Generales y Financieros Necesarios | Persona Responsable de la implementación | Plazos de Inicio | Plazos de Finalización | Programa de capacitación y concienciación | Método para la Evaluación del Resultado/desempeño | Indicador de efectividad del control | Periodo de evaluación | Estado |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |