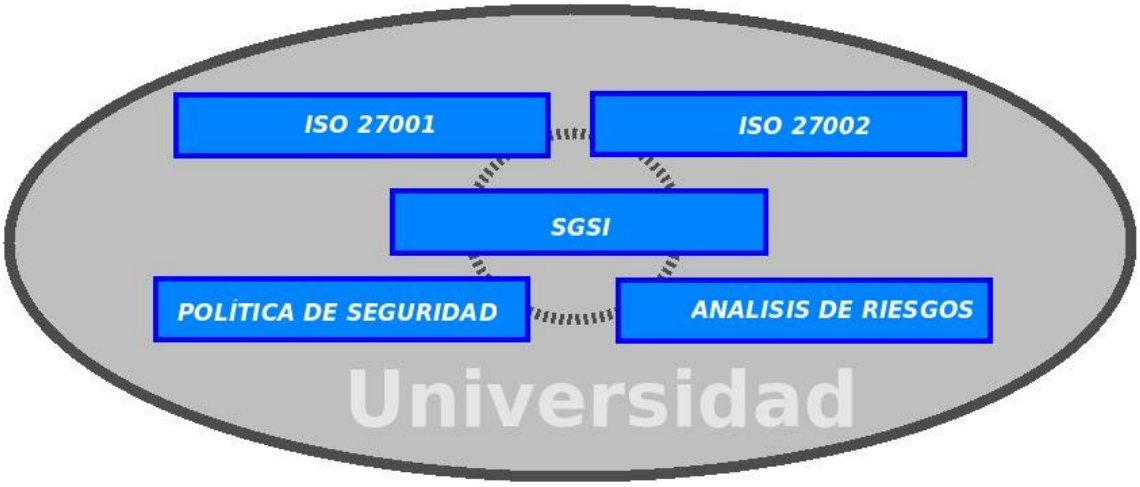
# Máster Interuniversitario en Seguridad de las TIC (MISTIC)

# Trabajo de Final de Máster




## Memoria

## Elaboración de un Plan de Implementación de la ISO/IEC 27001:2013

**Roberto Bazán Sancho**
**05-06-2015**

| | |
|---|---|
| **Título del Trabajo** | **Elaboración de un plan de implementación de la ISO27001:2013** |
| **Nombre del autor** | **Roberto Bazán Sancho** |
| **Nombre del consultor** | **Antonio José Segovía Henares** |
| **Fecha de entrega** | **10/06/2015** |
| **Área del trabajo final** | **Sistemas de Gestión de la Seguridad de la Información** |
| **Titulación** | **Master Interuniversitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)** |

***Agradecimientos***

*A mi mujer y mis dos hijos, que siempre te ofrecen una sonrisa, hasta en esos momentos complicados.*

*Al tutor, José Segovía, apoyando, animando e indicando en todo momento los pasos y correcciones a realizar.*

*Resumen*

*Todas las organizaciones disponen y gestionan información que las hace diferentes y únicas.*
*La información es su valor, identificando su estrategia y su razón de ser.*
*Por este motivo, resulta imprescindible implantar mecanismos que permitan establecer y medir un proceso de gestión de la seguridad de la información, con el fin de conocer los activos estratégicos de la organización, valorarlos, evaluar sus riesgos, tomar las medidas oportunas que permitan mitigar el riesgo, y controlar el cumplimiento. Todo ello tiene que ser acompañado por un compromiso de la alta dirección que marque la estrategia a seguir.*

*Abstract*

*All organizations have and manage information that makes them different and unique.Information is their value , identifying strategy and rationale.*
*For this reason, it is essential to implement mechanisms to establish and measure process information security,* in order to meet the strategic assets of the organization, evaluate them , assess their risks , take appropriate measures to mitigate risk, and monitor compliance. All this must be accompanied by a commitment of senior management to check the strategy.

# Índice

# Índice de figuras

# 1. Introducción al Proyecto

El presenta trabajo final de master (TFM) realizará un análisis de riesgos e implementación de un sistema de gestión de la seguridad de la información ( en adelante SGSI) enfocado al sector educativo superior.

La motivación para la realización de este proyecto, es doble, por un lado una motivación personal de aprender y comprender la seguridad desde el punto de vista de la gestión. Por otro lado, y profesionalmente hablando, ayudar a mi organización con los conocimientos adquiridos y trabajados a la implantación de un Sistema de gestión de la seguridad que le permita contar con un instrumento para una posible certificación y mejora continua de la seguridad.

El proyecto se enfoca en el sector educativo superior español y concretamente en las universidades españolas y sus departamentos de Tecnologías de la Información ( en adelante TIC).

Las universidades son entornos muy complejos, principalmente debido a la diversidad de departamentos, servicios, tecnologías, roles y jerarquías que la componen.

Hay que destacar que la misión principal de la Universidad es servir a la sociedad, creando y transmitiendo conocimiento a las personas.

El conocimiento finalmente es consecuencia de la información asimilada.

Este factor implica que la información para las universidades es un activo estratégico, que al igual que las instalaciones, los recursos humanos o financieros, debe estar controlado, asegurado y conocer las amenazas a las que está expuesto.

Esto va a permitir asegurar la calidad y continuidad de su negocio, cumpliendo con la normativa legal y dando imagen de seriedad y efectividad.

En este entorno, dentro de las universidades juega un papel clave los Departamentos de Tecnologías de la Información y de la Comunicación, como elementos concentradores de servicios e información.

En definitiva, para las universidades, ofrecer garantía de calidad es fundamental, esta calidad no es completa si no se garantiza la seguridad de la información enmarcada en un proceso de Planificar, Hacer, Verificar y Actuar, y que permita asegurar la confidencialidad, integridad y disponibilidad de la información.

# 2. Planificación

A continuación se detalla, mediante un diagrama de Gantt, el plan previsto para la realización de las diferentes fases de las que se compone el proyecto.

En él se especifican las fases de proyecto que se deben realizar y su distribución en el tiempo.

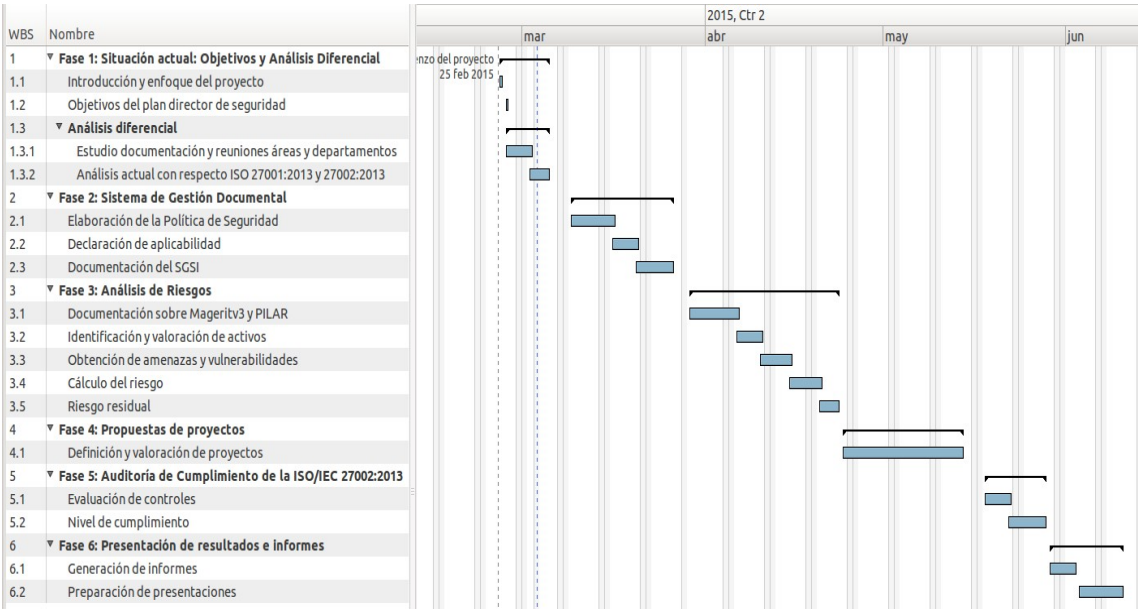



*Figura nº 1: Planificación del proyecto*

# 3. Contextualización de la organización

El objeto del proyecto se centra concretamente en una universidad privada, no virtual, joven y de tamaño pequeño, adaptada totalmente al Espacio de Educación Superior de Bolonia.

## 3.1 Datos de la Universidad

Universidad fundada en 1995, sin ánimo de lucro, privada y no virtual, con un Campus Universitario formado por tres edificios y siete centros.

La universidad imparte 38 titulaciones y actualmente están matriculados un total de 2000 alumnos.

Su plantilla está formada por un total de 604 empleados, de los cuales 491 se corresponde con Personal Docente e Investigador y 113 con Personal Técnico de Gestión.

| Estudio | Nº Alumnos |
|---|---|
| Grado | 1800 |
| Master | 200 |

*Figura nº 2: Relación de tipo de estudio y alumnos matriculados*

| Estudio | Nº de titulaciones |
|---|---|
| Grado | 20 |
| Master | 12 |
| Títulos propios | 6 |

*Figura nº 3: Relación de tipo de estudio y nº titulaciones*

| Campus |
|---|
| Edificio Rectorado / ETSA |
| Facultad de Comunicación |
| Facultad de Ciencias de la Salud |
| Campus Deportivo |

*Figura nº 4: Relación de Facultades*

| Centros | |
|---|---|
| Faculcates y escuelas | |
| | Facultad de Comunicación |
| | Facultad de Ciencias de la Salud |
| | Escuela Politécnica Superior |
| | Escuela Técnica Superior de Arquitectura |
| | Escuela de Gobierno y Liderazgo |
| Institutos | |
| | Instituto Humanismo y Sociedad |
| | Instituto de Medio Ambiente |
| | Instituto de Lenguas Modernas |

*Figura nº 5: Relación de Centros e Institutos*

| Personal | Nº Empleados |
|---|---|
| PDI | 113 |
| PTG | 491 |

*Figura nº 6: Relación de empleados por perfil*

# 3.2 Estructura organizativa

A continuación se presenta la estructura organizativa general de la Universidad.

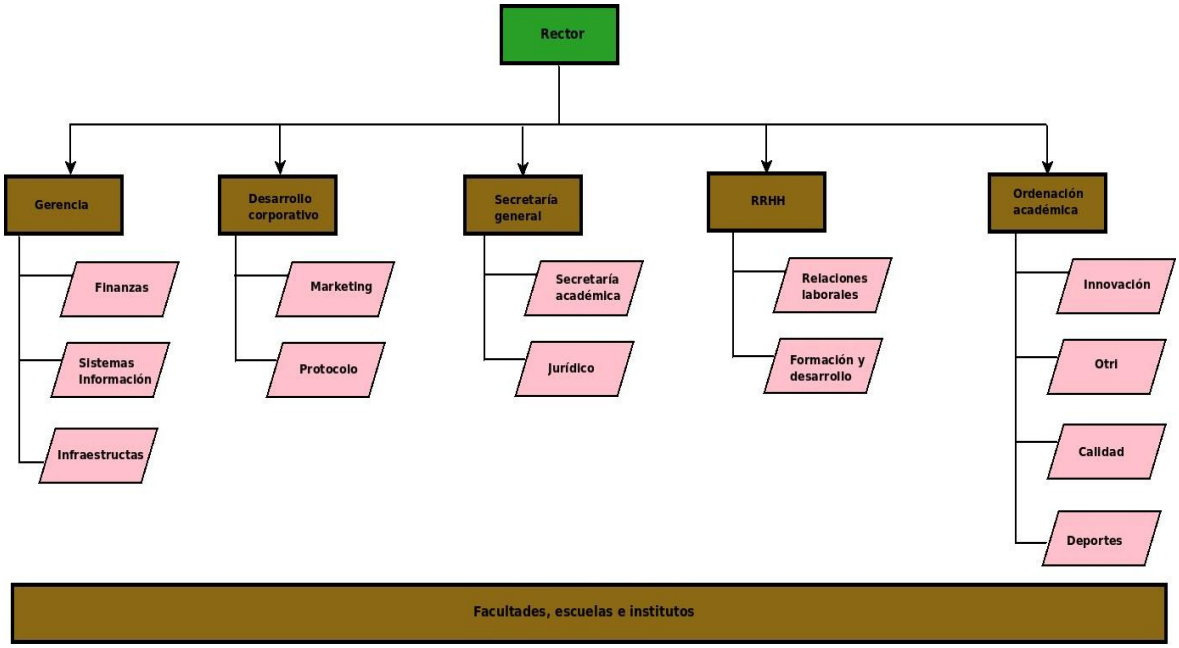



*Figura nº 7: Estructura organizativa*

## 3.2.1 Estructura e Infraestructura TIC

La Universidad cuenta con un Departamento de Sistemas de la Información (en adelante DSI) propio, que se encarga de diseñar, implantar y gestionar toda la infraestructura de sistemas, comunicaciones, aplicaciones y soporte al usuario.

El Departamento se compone de un Director TI responsable de la gestión y dirección del departamento y de cuatro áreas especializadas.

A continuación se presenta su estructura organizativa:

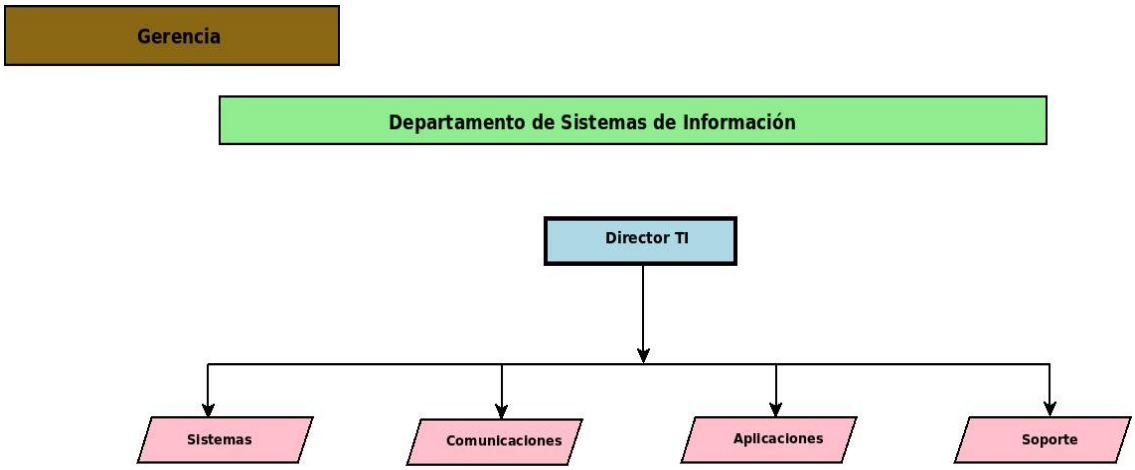



*Figura nº 8: Estructura del Departamento de Sistemas de Información*

El departamento cuenta con servicios de desarrollo, y parte del servicio de soporte a alumnos se encuentra externalizado en terceros.

No existe un área de seguridad como tal, sino que cada área del Departamento, implementa y gestiona la seguridad de su área.

La infraestructura tecnológica del Campus, así como los servicios TIC que presta la Universidad a sus usuarios, está totalmente gestionada por el Departamento TIC de la Universidad.

A continuación, se presenta la imagen con la topología de red del Campus:

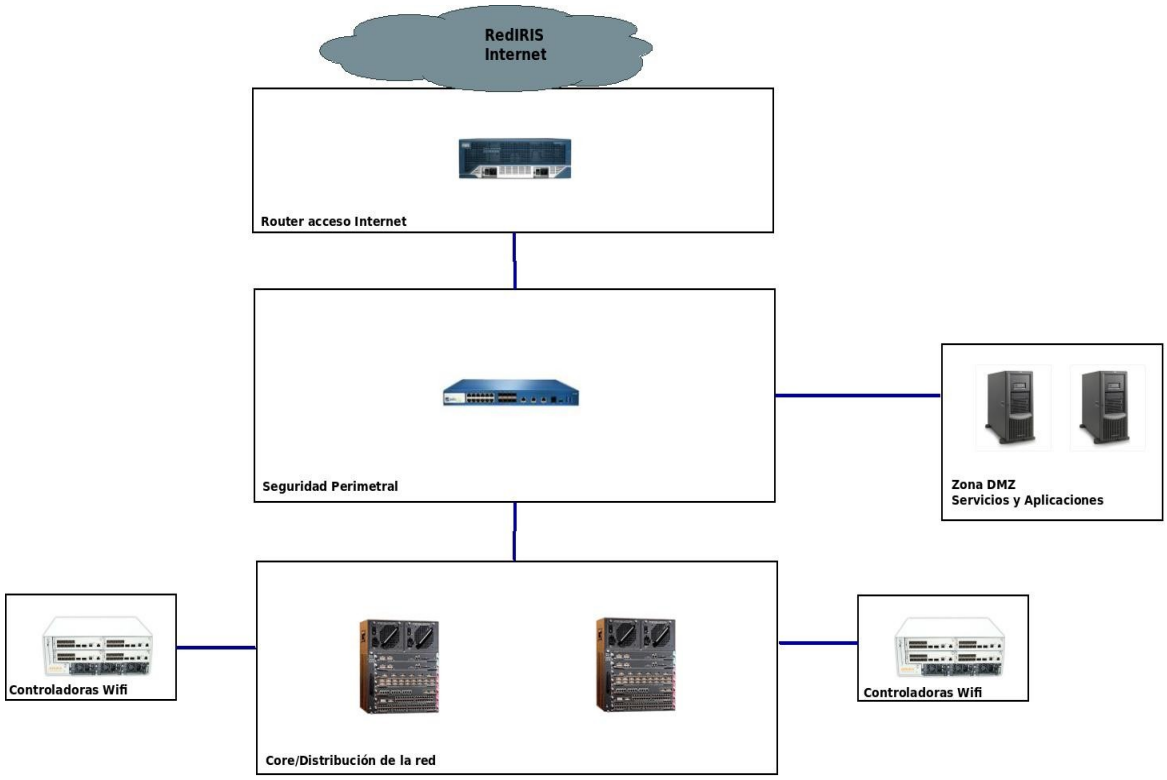



*Figura nº 9: Infraestructura de red*

La infraestructura de red en el acceso se basa en una topología en estrella, con dos equipos de Core o distribución encargados de la conmutación y encaminamiento del tráfico entre redes (Vlanes).

El campus dispone de cobertura 100% inalámbrica, este servicio nació como un elemento estratégico y diferencial, su intención es promover la movilidad y facilitar el acceso a los servicios TIC ofrecidos por la Universidad desde cualquier ubicación del campus.

El sistema Wifi se basa en una arquitectura centralizada con doble Controladora Wifi en modo Activo/Activo y 168 puntos de acceso Wifi ligeros desplegados principalmente dentro de las diferentes Aulas del campus.

Los diferentes servicios TIC ofrecidos por la Universidad, se encuentran en un segmento de red protegido por un Firewall de nivel aplicación.

El Firewall controla el acceso desde la red interna y desde Internet a los servicios y establece las diferentes políticas a nivel aplicación.

El acceso a Internet del Campus se proporciona por RedIRIS, a través de un enlace de fibra de Operador con su nodo. Un router se encarga de encaminar todo el tráfico.

Los servicios más importantes ofrecidos por la Universidad a su personal y alumnos son los siguientes:

- **Plataforma Docente Universitaria (PDU):** Servicio web de ayuda a la docencia. La PDU interviene en todos los procesos de interacción formativa entre alumno y docente.
- **ERP universitario:** Sistema de gestión universitaria, matriculación, expedientes.
- **ERP financiero:** Sistema de gestión financiera.
- **ERP RRHH:** Sistema de gestión de Recursos Humanos.
- **CRM:** Sistema de apoyo y seguimiento a la captación de alumnos.
- **Servicios de tratamiento de incidencias (SITIC):** Software para el tratamiento de incidencias TIC.
- **Servicio de repositorio bibliotecario**.
- **Servicio de webs institucionales.**
- **Servicio de correo:** correo institucional para todos los usuarios de la Universidad.
- **Servicio Ucloud:** Aplicaciones virtualizadas en la nube.
- **Servicio Internet.**
- **Servicio Wifi.**

Los servidores en su mayoría se basan en S.O Linux y entorno virtualizado sobre Debian XEN, salvo necesidades específicas de aplicaciones propietarias.

Los diferentes servicios se apoyan en otros servicios y sistemas no menos importantes como son:

- Servicios DNS.
- Servicio LDAP.
- Servicios de Bases de Datos Oracle y MySQL.
- Servicios MTA , Imap y POP3.
- Sistemas de antispam en cloud.
- Servicios de gestores de contenidos Drupal, Wordpress.
- Sistemas de almacenamiento.

### Terminales de usuario

- Todos los alumnos y personal de la Universidad disponen de un ordenador personal.
- Los equipos son propiedad de la Universidad bajo garantía.
- Todos los equipos disponen de antivirus instalado y acceso con permisos de administrador al equipo.
- Adicionalmente, el personal de la universidad dispone de teléfono móvil de empresa.

# 4. Alcance del proyecto

Los Departamentos de Sistemas de Información son elementos estratégicos en el tratamiento y gestión de la información en la Universidad, soportando las actividades, servicios y procesos tecnológicos de la misma, por esta razón el alcance del proyecto se centrará en los activos del Departamento TI y los servicios estratégicos que ofrecen a través de las áreas de sistemas, redes, aplicaciones y soporte.

# 5. Sistema de Gestión de la Seguridad de la Información

El Sistema de Gestión de la Seguridad de la Información (en adelante SGSI) de la Universidad se apoya en la norma IS0/IEC 27001:2013 y en el código de buenas prácticas ISO27002:2013.

El modelo de seguridad implementa un conjunto de políticas, procedimientos y controles que buscan mantener el riesgo de los activos del Departamento de Sistemas de Información dentro de unos niveles aceptables por dirección, creando un ciclo de mejora continua de la seguridad de la información en los procesos estratégicos de la organización a través del proceso Plan-Do-Check-Act (en adelante PDCA).


*Figura nº 10: Proceso PDCA*

## 5.1 Alcance

El SGSI afecta inicialmente a todos los activos responsabilidad del Departamento de Sistemas de Información de la Universidad.

## 5.2 Objetivos

La Universidad define los siguientes objetivos:

- Incrementar la disponibilidad de la Plataforma Docente Universitaria.
- Reducir el impacto negativo en el acceso a la aplicación UXXI tras actualizaciones software.
- Redundar el acceso a Internet para mejorar la disponibilidad de la web principal de la Universidad en Internet.
- Implementar medidas de desarrollo seguro en las aplicaciones de desarrollo interno.
- Reducir la sustracción de credenciales de acceso de los usuarios.

Con el fin conocer la evolución y consecución de los objetivos marcados dentro del SGSI, se definen los siguientes indicadores para cada objetivo:

| | |
|---|---|
| Código de Indicador | ind_sgi_inc_acc_pdu |
| Descripción | Número de incidencias de acceso a la Plataforma Docente Universitaria en el año |
| Tipo de indicador | Entero |
| Valores | 0..x |
| Objetivo | 0 |

| | |
|---|---|
| Código de Indicador | ind_sgi_inc_acc_uxxi |
| Descripción | Número de incidencias en el acceso a la apli UXXI tras proceso de actualización |
| Tipo de indicador | Entero |
| Valores | 0..x |
| Objetivo | 0 |

| | |
|---|---|
| Código de Indicador | ind_sgi_inc_acc_web |
| Descripción | Número de incidencias de acceso a la Web principal de la Universidad desde Internet |
| Tipo de indicador | Entero |
| Valores | 0..x |
| Objetivo | 0 |

| | |
|---|---|
| Código de Indicador | ind_sgi_vul_des |
| Descripción | Número de vulnerabilidades detectadas en desarrollos propios en el año |
| Tipo de indicador | Entero |
| Valores | 0..x |
| Objetivo | 0 |

| | |
|---|---|
| Código de Indicador | ind_sgi_sus_cre |
| Descripción | Número de credenciales sustraidas en el año |
| Tipo de indicador | Entero |
| Valores | 0..x |
| Objetivo | 0 |

*Figura nº 11: Tablas indicadores de objetivos*

# 6. Normativa y metodología

La gestión de la seguridad de la información de cualquier empresa y por supuesto de una Universidad debe apoyarse en una serie de normas, estándares y buenas prácticas que aporten rigor a su desarrollo e implantación.

Durante la realización del proyecto se tomará como base para su desarrollo la norma ISO/IEC 27001:2013 y la ISO/IEC 27002:2013.

La ISO/IEC 27001 aglutina una especificación de requisitos que deben cumplir los sistemas de gestión de la seguridad. Esta norma es certificable.

La ISO/IEC 27002 es una guía de buenas prácticas en relación a la seguridad y en la cual se apoya la norma ISO/IEC 27001.

## 6.1 Familia de estándares ISO/IEC 27000

La seguridad de la información es clave para el éxito de las organizaciones, este hecho lo confirma la ISO y la IEC, que han desarrollado de forma conjunta la serie ISO/IEC 27000, que aglutina a un conjunto de normas, guías y estándares relacionados directamente con la seguridad.

La coordinación de la norma ISO 27000 es llevada a cabo por el subcomité 27 - SC27- dentro del JTC1: Joint Technical Committee 1) que lidera a un conjunto de expertos en materia de seguridad.

La familia de normas ISO/IEC 27001 se estructura atendiendo a una jerarquía:

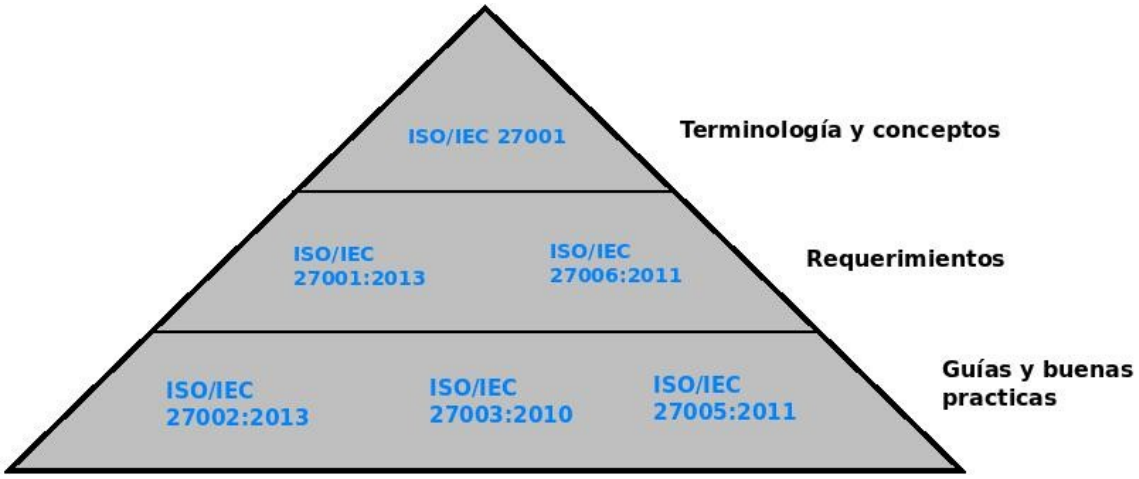



*Figura nº 12: Familia de normas ISO/IEC 27000*

- ISO/IEC 27000 proporciona una introducción y visión de conjunto de todo el marco ISO 27000 y facilita un glosario común

- ISO/IEC 27001:2013. Esta norma recoge las necesidades para la implantación de un sistema de gestión de la seguridad de la información. Esta norma puede certificarse.

- ISO/IEC 27002:2013. Esta guía es un código de buenas prácticas para la gestión de la seguridad de la información, incluye un conjunto de controles y buenas prácticas en temas de seguridad. La ISO/IEC 27001 se apoya en estos controles.

- ISO/IEC 27006:2011. Esta norma recoge las necesidades de las organizaciones de certificación acreditadas para certificar un sistema de gestión de la seguridad de acuerdo a la Norma ISO/IEC 27001.

- ISO/IEC 27005:2011. Esta guía cubre la gestión de los riesgos de seguridad de la información.

- ISO/IEC 27003:2010 Esta norma proporciona una guía para la implementación de un SGSI de acuerdo al estándar ISO/IEC 27001, haciendo foco en el método PDCA respecto al establecimiento, implementación, revisión y mejora del propio sistema.

## 6.2 Historia y evolución de la norma

Las normas ISO/IEC 27001 y 27002 tienen su base en los estándares británicos BS-7799 y BS-7799-2.

La organización británica de estandarización BSI (British Standard Institute) creó la Norma BS-7799 en 1995, que incluía una primera versión de buenas prácticas para la seguridad de la información.
Posteriormente se creó la BS-7799-2 que contenía los requerimientos para la gestión de la seguridad de la información apoyándose en la Norma BS-7799.

A raíz de las normas británicas, nació la Norma ISO/IEC 17799:2000, que fue revisada en 2005, dando lugar a la ISO/IEC 17799:2005. En el año 2007 se aprobó un cambio de denominación, pasando a llamarse ISO 27002:2005.

La última revisión de esta norma se ha aprobado en 2013, dando lugar a la ISO 27002:2013, esta revisión introduce ciertos cambios con respecto a su predecesora.

La nueva norma ISO/IEC 27002:2013 consta de 14 dominios, 35 objetivos de control y 114 controles.

La nueva normativa hace más hincapié en las Partes interesadas, Liderazgo, Sensibilización, Comunicación, Capacidades, Propietario del riesgo, Activos, Gestión de Riesgos y Oportunidades principalmente.

Las siguientes imágenes presentan los cambios introducidos en la normas con respecto a sus predecesoras.


*Figura nº 13: Evolución norma ISO27001:2005*

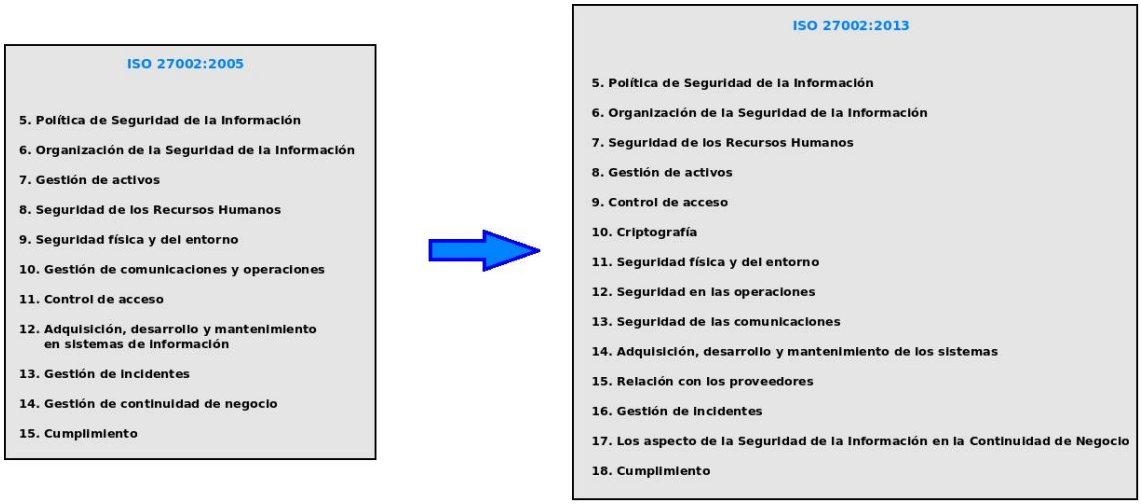



*Figura nº 14: Evolución norma ISO27002:2005*

# 7. Objetivos del Plan Director de Seguridad

Durante el desarrollo del Plan Director de Seguridad se deben fijar con claridad los hitos que conforman los objetivos.
Se adjunta anexo anexo_objetivos_analisis.pdf, donde se detalla en profundidad los objetivos del Plan Director de Seguridad.

# 8. Análisis diferencial de la Universidad

El análisis diferencial permite situar a la Universidad en su estado inicial frente a la norma.
Se adjunta documento anexo anexo_objetivos_análisis.pdf, donde se desarrolla el análisis.

# 9. Gestión documental

La norma ISO/IEC 27001:2013 indica que la organización, en este caso la Universidad, debe disponer al menos de una serie de documentos que permitan llevar a cabo de una forma adecuada la implantación del Sistema de Gestión de la Seguridad de la Información, en adelante (SGSI).

Estos documentos son:

- Política de Seguridad.
- Procedimiento de Auditorías Internas.
- Gestión de Indicadores.
- Procedimiento de revisión por dirección.
- Gestión de roles y responsabilidades.

En el siguiente apartado se detallan los diferentes documentos propuestos por la norma.

# 9.1. Política de Seguridad

Para cumplir con la gestión de la seguridad, la Universidad debe contar con una política de seguridad aprobada por la dirección y conocida por todo el personal.

El documento de política de seguridad refleja:

- La aplicación de la política.
- Los activos protegidos.
- Las funciones y responsabilidades del personal.
- La revisión por la alta dirección.

Se adjunta documento anexo, **anexo_doc_politica_seg.pdf** con la política de seguridad de la universidad.

## 9.1.1. Procedimientos y normas de seguridad

La Universidad dispone de procedimientos, políticas y normas en materia de seguridad de la información con el objetivo de estar alineada con los controles ISO/IEC 27002:2013 indicados por la norma ISO/IEC 27001:2013.

El documento anexo, **anexo_doc_política_seg.pdf** contiene las políticas y normas de seguridad de la Universidad.

# 9.2. Procedimiento de Auditorías Internas

El SGSI debe de ser evaluado internamente con una periodicidad anual, con el objetivo principal de verificar el cumplimiento del SGSI de acuerdo al modelo Plan-Do-Check-Act PDCA.

El Auditor elaborará un plan inicial de auditoría y el correspondiente informe posterior donde se comprobará el grado de cumplimiento de implantación del SGSI.

El plan de auditoría comprobará el cumplimiento del SGSI de acuerdo al modelo Plan-Do-Check-Act (en adelante PDCA):

- Verificará que la Universidad cuenta con un sistema para gestionar la seguridad de la información.
- Qué la Universidad cuenta con las herramientas necesarias para la implantación del sistema de forma adecuada.
- Qué la Universidad cuenta con la capacidad de mejorar el sistema de forma continua.

En la fase de auditoría “Plan”, se debe:

- Comprobar la corrección del análisis de riesgos en base a la metodología empleada y al alcance definido del SGSI.
- Comprobar que la alta dirección conoce el resultado del análisis.
- Comprobar que se han desarrollado las medidas adecuadas para la mitigación del riesgo detectado.
- Se tendrán en cuenta los resultados de auditorías anteriores.

En la fase del plan de auditoría “Do”, se debe:

- Revisar la implantación de los controles de acuerdo a la documentación de la norma ISO/IEC 27002:2013.
- En las siguientes fases del plan de auditoría se verificará como la organización mejora en base a los indicadores y métricas definidos.
- El resultado de la auditoría proporcionará un documento para la revisión de la Dirección.

Se adjunta documento anexo, **anexo_auditorias_internas.pdf** con el plan e informe de auditoría interna.

## 9.3. Gestión de Indicadores

El SGSI pone de manifiesto la necesidad de establecer un sistema de medición de la seguridad que permita conocer, comparar y mejorar nuestro sistema.

Los indicadores deberán medir la seguridad en base a:

- Implantación de las medidas de seguridad.
- Eficacia y eficiencia de las medidas de seguridad.

- Impacto de los incidentes de seguridad.

Los indicadores reflejaran el cumplimiento o no de los valores objetivos marcados.
Con el fin de obtener estos indicadores, es necesaria la toma de datos de los sistemas de una forma continuada en el tiempo, que dará lugar a las métricas.

Será necesario recopilar la siguiente información:

- Índice de madurez del SGSI.
- Grado de cumplimiento del SGSI.
- Datos relativos a incidentes.
- Datos relativos a vulnerabilidades.
- Disponibilidad de servicios.

El Comité de Seguridad será responsable de la definición con exactitud de los indicadores, y Sistemas de Información, de la operativa de implantación.

La información resultante quedará plasmada en un informe de resultados de indicadores, que será evaluado por el Comité de Seguridad, el cual podrá actuar ante un objetivo no cumplido y tomar las acciones que consideré adecuadas para solucionarlo.

Se adjunta documento anexo, **anexo_gestion_indicadores.pdf**.

## 9.4. Procedimiento Revisión por Dirección

Uno de los factores más importantes para el éxito del SGSI es la implicación de la Dirección.

La Dirección de la Universidad por lo tanto, debe asumir una vez al año la necesidad de una revisión por su parte del grado de cumplimiento del SGSI, así como ser conscientes de los activos críticos y riesgos a los que están expuestos.

Los documentos que deberán ser revisados por la Dirección serán:

- Resultados de las auditorías.
- Informe del estado del sistema y observaciones del Comité de Seguridad
- Informe de amenazas o vulnerabilidades no tratadas en análisis de riesgos.

- Informe sobre acciones realizadas por las partes involucradas en el sistema de gestión.
- Informe de incidencias reportadas y la solución de las mismas.
- Informe de indicadores con objetivos y grados de cumplimiento.
- Informe de cambios que afecte al SGSI.

La revisión de la información dará lugar a la toma de acciones:

- Actualización de la evaluación de riesgos.
- Mejora de la eficacia del SGSI.
- Mejora de los procedimientos y controles, así como la forma de medición.
- Necesidad de nuevos recursos.

| | | | | | |
|---|---|---|---|---|---|
| **Código Acta:** | act-rev-xxx | **ACTA DE REVISIÓN DEL SGSI POR DIRECCIÓN** | | | |
| **Fecha:** | dd/mm/aaaa | | | | |

| | | | | | |
|---|---|---|---|---|---|
| **Convoca Reunión:** | xxxxxxxxxxx | | | | |
| **Participantes:** | | | | | |
| **Acta nº** | xxx | **Tipo:** | Revisión SGSI | **De Caracter** | Ordinaria/extraordinaria |

| **Fecha Reunión** | **Lugar de reunión** | **Hora Inicio** | **Hora fin** |
|---|---|---|---|
| | | | |

| **ORDEN DEL DÍA** |
|---|
| Resultados de las auditorias.<br>Informe del estado del sistema y observaciones del Comité de Seguridad<br>Informe de amenazas o vulnerabilidades no tratadas en análisis de riesgos.<br>Informe sobre acciones realizadas por las partes involucradas en el sistema de gestión.<br>Informe de incidencias reportadas y la solución de las mismas.<br>Informe de indicadores con objetivos y grados de cumplimiento.<br>Informe de cambios que afecte al SGSI. |

| **Firma Dirección** | **Firma Comité de Seguridad** | **Firma Responsable de Seguridad** |
|---|---|---|
| | | |

*Figura 15: Ficha Acta Revisión por Dirección*

## 9.5. Gestión de Roles y Responsabilidades

La Universidad define una estructura organizativa para garantizar una adecuada gestión de la seguridad de la información, con las responsabilidades de cada uno de los roles participantes.

A continuación se presenta su estructura y funciones:


*Figura nº 16: Estructura organizativa de la seguridad*

- Consejo Rector: El consejo Rector se encargará de aportar la visión estratégica y los recursos necesarios.
- Comité de Seguridad: Formado por Responsables de Departamentos y cuya función será:
  - ✓ Comunicación entre la Unidad de Seguridad y Consejo Rector.
  - ✓ Gestionar el Riesgo.
  - ✓ Validar el plan director de seguridad y de continuidad de negocio.
  - ✓ Revisar las incidencias más destacas en materia de seguridad.

- Unidad de Seguridad de la Información: Dirigida por el Responsable de Seguridad de la Información, es un Área transversal encargada del control y gestión, y cuya principal prioridad es la aplicar la política de seguridad y verificar el cumplimiento de la misma.
- Sistemas de Información: Área totalmente operativa encargada de ejecutar los procedimientos.

Se adjunta documento anexo, **anexo_organizacion-seguridad.pdf**, con la descripción detallada de los roles que componen la estructura organizativa de la seguridad y sus responsabilidades.

## 9.6. Metodología de Análisis de Riesgos

El análisis de riesgos constituye el elemento central del SGSI, este va a permitir a la Universidad obtener las medidas de seguridad que se deben aplicar, con el fin de mitigar o en su defecto asumir el riesgo.

Para poder gestionar de la forma más adecuada los activos de una organización, es imprescindible conocer el riesgo al que están sometidos.

Debido a esto, es vital definir una correcta metodología, perdurable en el tiempo y sistemática, que permita desarrollar de forma correcta el análisis.

La Universidad y dada su relación con la administración pública, considera la metodología Mageritv3 como la más adecuada para obtener la valoración de los activos, amenazas y vulnerabilidades.
Destacar que la norma ISO 27001:2013 no exige una metodología concreta a seguir para la evaluación de los riesgos, pero en cualquier caso la ISO 27001:2013 exige una valoración de los riesgos consistente, válida y comparable.

Mageritv3 permite implementar la gestión del riesgo dentro de un marco de trabajo y con los siguientes objetivos:

- Concienciar a los responsables de la organización de los riesgos existentes y la necesidad de su gestión.
- Disponer de un método sistemático para la gestión del riesgo.
- Descubrir y planificar el tratamiento del riesgo.
- Modelo unificado de informes y hallazgos.

La metodología Mageritv3 se apoya en la herramienta de análisis de riesgos EAR/PILAR, que permite analizar los riesgos en varias dimensiones: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad y a nivel cualitativo y cuantitativo.

Magerit es una metodología desarrollada por el Consejo Superior de Administración Electrónica y actualizada en 2012 a su versión 3.
La versión 3 de Magerit se estructura en dos libros y una guía de técnicas:

- Libro I: Método
- Libro II: Catálogo de elementos
- Guía de técnicas.

Como herramienta de apoyo en el análisis y gestión del riesgo, la Universidad ha utilizado la herramienta PILAR.
PILAR es una aplicación desarrollada por el Centro Criptológico Nacional que implementa el análisis y gestión del riesgo en base a Magerit.

La metodología Magerit se divide en un conjunto de fases.

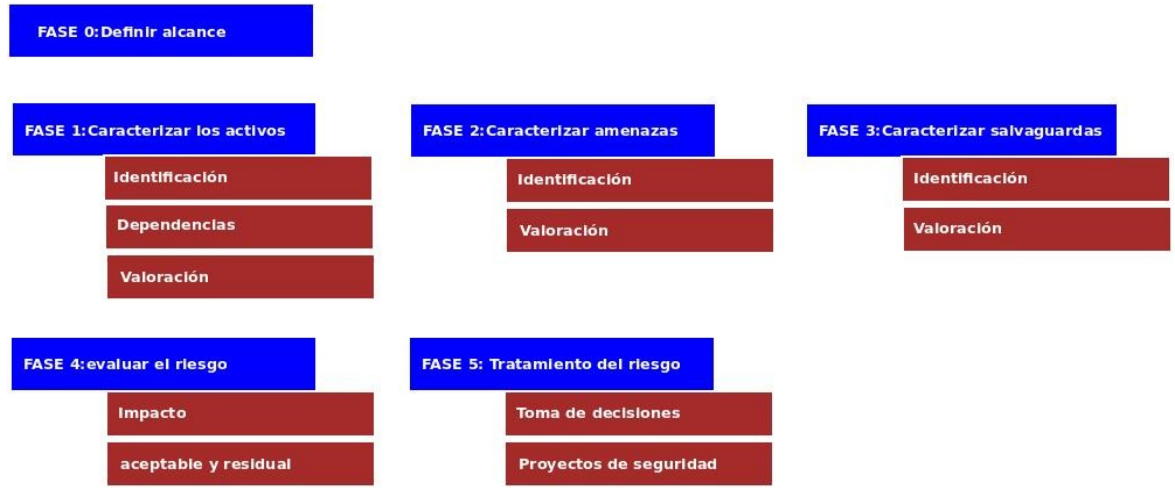



*Figura 17: Fases Magerit*

**Fase 0: Definir el alcance**

Esta fase propone establecer el alcance del análisis de riesgo. El alcance se definirá en función de la estrategia en materia de seguridad de la información marcada por la organización, por lo tanto cada organización deberá plantear hasta donde debe llegar su estudio de riesgos.

**Fase 1: Caracterizar los activos**

Una vez definido el alcance del análisis, se deben identificar cuales son los activos más importantes para la organización, así como los elementos o procesos de los cuales estos activos dependen.
Cada activo identificado deberá ser valorado, con el objetivo de disponer de la criticidad que cada activo representa para el negocio de la organización.
Así mismo todo activo debe tener un responsable asignado.

**Fase 2: Caracterizar amenazas**

Conociendo todos los activos objeto del análisis, el siguiente paso consiste en identificar todas las amenazas a las que se pueden ver expuestos.
Las amenazas son muchas y variadas por lo que la experiencia y el conocimiento del activo es un hecho vital para identificar de forma correcta y practica aquellas amenazas a las que un activo concreto esta expuesto.
Para esta fase Mageritv3 proporciona un catalogo de amenazas en las que apoyarse durante el desarrollo de esta fase.

**Fase 3: Caracterizar salvaguardas**

En la siguiente fase, Magerit propone analizar las características de los activos con el fin de identificar los puntos débiles y las posibles vulnerabilidades a las que están expuestos, así como el estudio de las medidas de seguridad o salvaguardas actuales de nuestros activos.
El desarrollo de esa fase aportará la información suficiente para la futura evaluación del riesgo.

**Fase 4: Evaluación del riesgo**

Para la evaluación del riesgo se tendrá en cuenta:

- Inventario de activos y su valoración.
- Amenazas a las que está expuesto el activo.
- Posibles vulnerabilidades asociadas a cada activo.
- Salvaguardas implantadas.

Partiendo de esta información se calculará para cada activo-amenaza la probabilidad de que la amenaza se materialice y el impacto que tendría sobre el negocio en caso de producirse.
El calculo se podrá realizar mediante un criterio cuantitativo o cualitativo.

Magerit proporciona diferentes técnicas para el análisis del riesgo:

- Utilización de tablas para la obtención de resultados simplificados.
- Técnicas basadas en algoritmos.
- Técnicas basadas en metodologías de ataque y razonamientos sobre sus posibles amenazas.

En este caso la Universidad se decanta por la utilización de técnicas de análisis basadas en la definición de tablas.

La metodología empleada en el análisis de riesgos de la Universidad y de acuerdo a este criterio define:

- Un inventario de activos agrupados por naturaleza (aplicaciones, servicios, comunicaciones, dispositivos y personal).
- Una tabla de valoración de activo: Se asignará un valor de 10-50 tomando como referencia para valorar el activo el impacto de un posible amenaza sobre el activo en la Universidad.
- Se define el parámetro frecuencia, como la posibilidad de repetición de una amenaza sobre el activo durante un rango de tiempo determinado.

| Valor de activo (Impacto) | Frecuencia |
|---|---|
| Muy alto - 50 | Muy alto - 5 |
| Alto - 40 | Alto - 4 |

| | |
|---|---|
| Medio - 30 | Medio - 3 |
| Bajo - 20 | Bajo - 2 |
| Muy bajo - 10 | Muy bajo - 1 |

*Figura nº 18: Tabla valor activo y valor frecuencia*

- Una tabla de enumeración de amenazas en base a su origen o naturaleza.
- Una tabla con el resultado del impacto potencial dado por el valor del activo en base al impacto (valores 10 a 50), multiplicado por la frecuencia de ocurrencia del impacto.
- Una tabla resultado de nivel de riesgo al cual esta sometido los activos por amenaza.

El nivel de riesgo se cuantificará de forma cualitativa en base al siguiente esquema de colores:

| Nivel de Riesgo |
|---|
| Muy Alto |
| Alto |
| Medio |
| Bajo |
| Muy bajo |

*Figura nº 19: Cuantificación del riesgo*

**Fase 5: Tratamiento del riesgo**

Conocido el valor del riesgo, se debe proceder a tratar todo aquel riesgo que la Dirección considera no asumible.
El riesgo puede ser tratado siguiendo diferentes estrategias:

- Transferir: El riesgo se traspasa a un tercero.
- Eliminar: Se elimina el proceso-activo que genera el riesgo.
- Asumir el riesgo, de forma justificada.
- Mitigar el riesgo, implantando medidas.

Se tendrá en cuenta que las medidas a implantar para mitigar el riesgo deberán pasar a formar parte del Plan Director de Seguridad y definir los niveles de prioridad a la hora de acometer los proyectos.

## 9.7. Declaración de Aplicabilidad

El documento de declaración de aplicabilidad es clave para la correcta implantación del SGSI.

El documento de declaración de aplicabilidad de la Universidad refleja todos aquellos controles de la ISO/IEC 27002:2013 que aplican o no aplican en el Sistema de Gestión.
Este documento permitirá al Auditor del Sistema de Gestión verificar si los controles marcados, están realmente aplicados.

Se adjunta documento anexo, **anexo_doc_aplicabilidad.pdf.**

# 10. Análisis de riesgos

## 10.1 Introducción

La Universidad, dependiente de sus sistemas de información y comunicación, pretende a través del análisis de riesgos obtener una visión concreta de cada componente de su Sistema de Información, con el fin de conocer el valor que posee, las amenazas a las que esta expuesto y de que salvaguardas se le dota.

La Universidad y de acuerdo a su deber de cumplimiento de La Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, en su artículo 9 (Seguridad de los datos) tiene la obligación de analizar el riesgo al que están expuestos los datos almacenados.

De acuerdo con la metodología comentada con anterioridad, se abordará las siguientes fases durante el análisis del riesgo:

- Definir los activos más importantes del Departamento de Sistemas de Información y sus propietarios.
- Definir las amenazas a las que están expuestos.
- Estimar el impacto, de acuerdo al daño que puede ocasionar una amenaza si se materializa.
- Estimar el riesgo o ponderación de la frecuencia y el impacto de la amenaza.
- Identificar el nivel de riesgo para los activos según la amenaza y definir los propietarios del riegos.

## 10.2 Inventario de activos

Los diferentes servicios que se proporcionan a la Universidad, así como los dispositivos o elementos que los soportan, además de las personas, son activos que pueden estar expuestos a diferentes amenazas, por lo tanto, para determinar el riesgo, es necesario conocer todos los activos con los que cuenta el Departamento de Sistemas de Información.

La metodología Magerit define activo como el recurso del sistema de información, o aquel relacionado con éste, necesario para que la Organización funcione correctamente y alcance los objetivos propuestos por su dirección.

Siguiendo la metodología de tablas de MAGERIT a continuación se enumera la relación de los activos del Departamento de Sistemas de Información de la Universidad.

Los activos se han agrupado con el fin de facilitar un análisis posterior en base a su naturaleza.

| APLICACIONES | | |
|---|---|---|
| ACTIVO | RESPONSABLE | **AGRUPACIÓN** |
| • OpenLdap<br>• FreeRadius<br>• DHCP<br>• Bind<br>• Nagios | • Adm. Aplicaciones<br>• Adm. Redes<br>• Adm. Redes<br>• Adm. Redes<br>• Adm. Redes | Comunicaciones |
| • Nagios<br>• check-mk<br>• OCSinventory<br>• Cacti<br>• HP Inside Manager<br>• HP IP Console Viewer | • Adm. Redes<br>• Adm. Redes<br>• Adm. Microinformática<br>• Adm. Sistemas<br>• Adm. Sistemas<br>• Adm. Sistemas | Monitorización |
| • Postfix<br>• Roundcube<br>• Spamina | • Adm. Sistemas<br>• Adm. Sistemas<br>• Adm. Sistemas | Correo |
| • CA ARC Server<br>• LVM<br>• RSYNC<br>• Keepalive<br>• IPVS | • Adm. Sistemas<br>• Adm. Sistemas<br>• Adm. Sistemas<br>• Adm. Sistemas<br>• Adm. Sistemas | Backup – Alta disponbilidad |
| • Oracle Portal<br>• UXXI – Académico<br>• GLPI<br>• People NET | • Adm. Aplicaciones<br>• Adm. Aplicaciones<br>• Adm. Microinformática<br>• Adm. Aplicaciones | Bases de Datos |
| • Debian<br>• XEN<br>• VMWare<br>• Red Hat Enterprise<br>• Windows Server | • Adm. Sistemas<br>• Adm. Sistemas<br>• Adm. Sistemas<br>• Adm. Sistemas<br>• Adm. Sistemas | Sistemas Operativos |

| SERVICIOS | | |
|---|---|---|
| ACTIVOS | RESPONSABLE | **AGRUPACIÓN** |
| • Servicio de datos<br>• Servicio de telefonía<br>• Servicio Wifi<br>• Servicio VPN<br>• Servicio DNS<br>• Servicio Autentificación<br>• Servicio Acceso a Internet<br>• Servicio seguridad de red<br>• Servicio cableado estructurado<br>• Servicio direccionamiento IP<br>• Servicio de monitorización | Adm. Comunicaciones | Servicios Comunicaciones |
| • Servicio de ficheros<br>• Servicio correo electrónico<br>• Servicio de soporte a usuarios<br>• Servicio intranet<br>• Servicios Web | Adm. Aplicaciones | Aplicaciones y soporte<br><br>Servicios Web |
| • Servicio ERP<br>• Servicio Gestión Académica<br>• Servicio plataforma docente<br>• Servicio de directorio<br>• Servicio de inventariado | Adm. Aplicaciones | Bases de Datos |
| • Servicio de copia de seguridad<br>• Servicio de CPD | Adm. Sistemas | Contingencia |

| COMUNICACIONES | | |
|---|---|---|
| ACTIVO | RESPONSABLE | AGRUPACIÓN |
| • Infraestructura cableado estructurado<br>• Fibra óptica acceso a Internet | | |

| | | |
|---|---|---|
| • Radio Enlace acceso a Internet<br>• Infraestrucura inalámbrica<br>• Acceso ADSL | Adm. Comunicaciones | Líneas de comunicaciones |
| • Servicio de acceso a Internet<br>• Servicio de telefonía | Adm. Comunicaciones | Servicios de proveedores |

| DISPOSITIVOS | | |
|---|---|---|
| ACTIVO | RESPONSABLE | |
| • Servidores<br>• Cabina de disco<br>• Librería de cintas<br>• Sistema de alimentación ininterrumpida SAI<br>• Aires Acondicionados<br>• Routers<br>• Firewalls<br>• Switches<br>• Controladores Wifi<br>• Antenas Wifi<br>• Teléfonos móviles | • Adm. Sistemas<br>• Adm. Sistemas<br>• Adm. Sistemas<br>• Adm. Sistemas<br>• Adm. Sistemas<br>• Adm. Comunicaciones<br>• Adm. Comunicaciones<br>• Adm. Comunicaciones<br>• Adm. Comunicaciones<br>• Adm. Comunicaciones<br>• Adm. Comunicaciones | Infraestructura hardware |

| PERSONAL | | |
|---|---|---|
| ACTIVO | RESPONSABLE | AGRUPACIÓN |
| • Administrador de sistemas<br>• Administrador de redes<br>• Administrador de BBDD<br>• Administrado de Aplicaciones<br>• Administrador Web<br>• Administrador de soporte<br>• Técnicos de soportes<br>• Jefe de Departamento de sistemas de información | • Director SI<br>• Director SI<br>• Director SI<br>• Director SI<br>• Director SI<br>• Director SI<br>• Director SI<br>• Gerencia | Personal de Sistemas de Información |

*Figura nº 20: Tablas de activos del Departamento de Sistemas de Información*

## 10.3 Valoración de activos

A continuación se define varias tablas con el criterio para la valoración de los activos en base a su impacto en la organización y la posible frecuencia con la que se puede materializar una amenaza en ellos.

| Valoración | Definición |
|---|---|
| MUY ALTO (50) | • Pérdida o inhabilitación temporal o permanente de activos considerados críticos no redundados o salvaguardados.<br>• Interrupción total de la prestación de los servicios y de los procesos que ofrece la Universidad.<br>• Deterioro de la imagen pública de la Universidad.<br>• Robo de información estratégica. |
| ALTO (40) | • Pérdida o inhabilitación temporal o permanente de activos considerados no críticos no redundados o salvaguardados.<br>• Interrupción parcial de la prestación de los servicios y de los procesos que ofrece la Universidad.<br>• Deterioro importante de la imagen pública de la Universidad .<br>• Robo de información confidencial pero no estratégica. |
| MEDIO (30) | • Pérdida o inhabilitación temporal o permanente de activos considerados críticos redundados o salvaguardados.<br>• No se produce interrupción de la prestación de los servicios ni de los procesos que ofrece la Universidad pero el rendimiento se ve altamente afectado.<br>• Deterioro leve de la imagen pública de la Universidad.<br>• Robo de información reservada no confidencial ni estratégica. |
| BAJO (20) | • Pérdida o inhabilitación temporal o permanente de activos considerados no críticos redundados o salvaguardados.<br>• No se produce interrupción de la prestación de los servicios ni de los procesos que ofrece la Universidad pero el rendimiento se ve sensiblemente afectado.<br>• No se produce deterioro de la imagen pública de la Universidad.<br>• Robo de información sensible pero no considerada reservada, confidencial ni estratégica. |
| MUY BAJO (10) | • Pérdida o inhabilitación temporal o permanente de activos de segundo nivel.<br>• No hay interrupción de la prestación de los servicios pero el rendimiento se puede ver afectado. |

| | |
|---|---|
| | • No se produce deterioro de la imagen pública de la Universidad.<br>• Robo de información no pública pero no considerada sensible. |

*Figura nº 21: Tabla valoración activos*

La frecuencia incorpora la variable tiempo en el análisis de riesgos.

Puede darse el caso de amenazas de consecuencias fatales para los activos de la Universidad, pero que su materialización sea improbable. Por otro lado podemos tener amenazas sin repercusiones significativas para los activos, pero que reiteradas de forma constante pueden dar lugar a un daño mayor.

| Frecuencia | Definición |
|---|---|
| MUY ALTA (5) | La amenaza puede surgir en periodos inferiores a 1 semana. |
| ALTA (4) | La amenaza puede surgir en periodos inferiores a 1 mes. |
| MEDIA (3) | La amenaza puede surgir en periodos inferiores a 6 meses. |
| BAJA (2) | La amenaza puede surgir en periodos inferiores a 1 año. |
| MUY BAJA (1) | La amenaza puede surgir en periodos superiores a 1 año. |

*Figura nº 22: Tabla Frecuencias de amenazas*

## 10.4 Análisis de amenazas

A continuación se presenta la clasificación de amenazas en base a su naturaleza u origen:

- Desastres naturales: incendios, inundaciones, terremotos.
- Desastres de origen industrial: fuego, fugas de agua, cortes eléctricos.
- Errores y fallos no intencionados.
- Ataques.

De acuerdo a esta clasificación se enumeran las amenazas a las que se ven sometidos los activos del Departamento de Sistemas de Información de la Universidad.

| AMENAZAS: DESASTRES NATURALES |
|---|
| Aquellos sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta. |
| • Fuego<br>• Daños por agua<br>• Tormentas eléctricas, caída de rayos<br>• Viento fuerte<br>• Terremotos<br>• Tornados<br>• Nieve o hielo extremo<br>• Frío extremo<br>• Calor extremo |

| AMENAZAS: DE ORIGEN INDUSTRIAL |
|---|
| Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. |
| • Fuego: incendio<br>• Daños por agua: escapes, fugas, inundaciones<br>• explosiones, derrumbes, fallos eléctricos<br>• Condiciones inadecuadas de temperatura o humedad<br>• Contaminación mecánica: vibraciones, polvo, suciedad<br>• Contaminación electromagnética: interferencias radio, campos magnéticos<br>• Avería de origen físico o lógico: fallos en equipos o programas<br>• Degradación de los soportes de almacenamiento de la información<br>• Obras: en el interior o exterior de los edificios<br>• Corte del suministro eléctrico: cese de la alimentación de potencia<br>• Interrupción de otros servicios y suministros: gasoil, toner, papel |

| AMENZAS: ERRORES Y FALLOS NO INTENCIONADOS |
|---|
| Fallos causados por las personas de forma no intencionada. Son prácticamente idénticos a los intencionados pero diferenciándose en el propósito. |
| • Errores de los usuarios: fallos de las personas cuando usan los servicios y datos.<br>• Errores del administrador: equivocaciones de personas con responsabilidades de instalación y gestión.<br>• Errores de monitorización: registro erróneo de actividades o falta de información.<br>• Errores de configuración: introducción de parámetros erróneos.<br>• Difusión de software dañino: difusión no consciente de virus, troyanos.<br>• Errores de encaminamiento: errores en la gestión de las rutas de red.<br>• Escapes de información: la información llega a personas equivocadas.<br>• Alteración de la información: cuando se produce de manera accidental.<br>• Introducción de información incorrecta: cuando se produce de manera accidental.<br>• Destrucción de la información: borrado accidental de datos. |

- Vulnerabilidades de los programas: defectos en la codificación de programas.
- Errores de mantenimiento - Actualización de programas: impiden la correcta ejecución.
- Errores de mantenimiento - Actualización de equipos.
- Caída del sistemas por agotamiento de recursos.
- Indisponibilidad del personal: ausencia por enfermedad, guerra.

**AMENAZAS: ATAQUES INTENCIONADOS**

- Manipulación de la configuración.
- Suplantación de la identidad del usuario.
- Abuso de privilegios de acceso: un usuario realiza tareas que no son de su competencia.
- Uso no previsto o indebido: uso de los recursos del sistema para uso personal.
- Difusión de software dañino: difusión intencionada de virus, troyanos.
- Acceso no autorizado: ataques que consiguen hacerse con el sistema.
- Análisis de tráfico: monitorización de tráfico.
- Interceptación de información: un atacante ve la información pero no la altera.
- Modificación de información: alteración de información para beneficio propio o perjuicio de tercero.
- Manipulación de programas: alteración intencionada de programas buscando beneficio indirecto.
- Denegación de servicio: provocación de la caída del sistema por falta de recursos.
- Robo de equipos.
- Ataque destructivo: vandalismo.
- Indisponibilidad deliberada del personal: absentismo, huelga.
- Ingeniería social.

*Figura nº 23: Tablas de amenazas*

# 10.5 Impacto potencial

El riesgo es la medida del daño probable sobre un activo. Conociendo el impacto de las amenazas sobre los activos, podemos obtener el riesgo teniendo en cuenta la frecuencia.

Se ha elaborado la siguiente tabla para cuantificar el riesgo adaptándolo a la realidad de la Universidad.

| IMPACTO / FRECUENCIA | MUY ALTO (50) | ALTO (40) | MEDIO (30) | BAJO (20) | MUY BAJO (10) |
|---|---|---|---|---|---|
| MUY ALTO (5) | Muy alto 50x5=250 | Alto 40x5=200 | Medio 30x5=150 | Bajo 20x5=100 | Muy bajo 10x5=50 |
| ALTO (4) | Alto 50x4=200 | Alto 40x4=160 | Medio 30x4=120 | Bajo 20x4=80 | Muy bajo 10x4=40 |
| MEDIO (3) | Medio 50x3=150 | Medio 40x3=120 | Bajo 30x3=90 | Bajo 20x3=60 | Muy bajo 10x3=30 |

| | | | | | |
|---|---|---|---|---|---|
| **BAJO (2)** | Bajo 50x2=100 | Bajo 40x2=80 | Bajo 30x2=60 | Muy bajo 20x2=40 | Muy bajo 10x2=20 |
| **MUY BAJO(1)** | Muy bajo 50x1=50 | Muy bajo 40x1=40 | Muy bajo 30x1=30 | Muy bajo 20x1=20 | Muy bajo 10x1=10 |

*Figura nº 24: Cuantificación del riesgo*

| Impacto x Frecuencia | Nivel de Riesgo |
|---|---|
| 200 < Impacto * Frecuencia <= 250 | **Muy Alto** |
| 200 < Impacto * Frecuencia <= 150 | **Alto** |
| 150 < Impacto * Frecuencia <= 100 | **Medio** |
| 100 < Impacto * Frecuencia <= 50 | **Bajo** |
| 50 < Impacto * Frecuencia <= 0 | **Muy bajo** |

*Figura nº 25: Nivel de riesgo en base al impacto*

Tomando como referencia las tablas anteriores se obtiene el riesgo potencial al que están sometidos los activos de la Universidad en base a las posibles amenazas y la relación impacto-frecuencia.

| **Amenaza: Desastres naturales** | **Sucesos que pueden ocurrir sin intervención de los seres humanos.** | | | | |
|---|---|---|---|---|---|
| **Amenaza** | **Activos afectados** | **Frecuencia** | **Impacto** | **Riesgo** | **Responsable** |
| Fuego | • Aplicaciones y soporte<br>• Gestión de las comunicaciones<br>• Servicios web<br>• BBDD<br>• Contingencia y Monitorización<br>• Software de comunicaciones<br>• Monitorización<br>• Correo electrónico<br>• Backup y contingencia<br>• Sistemas operativos<br>• Infraestructura hardware<br>• Líneas de comunicaciones<br>• Proveedores de servicios<br>• Personal informático | 1 | 50 | **50** | Resp.Infraestructuras |
| Agua | | 2 | 50 | **100** | Resp.Infraestructuras |
| Tormentas electricas | | 3 | 50 | **150** | Resp.Infraestructuras |
| Viento fuerte | | 2 | 10 | **20** | Resp.Infraestructuras |
| Terremotos | | 1 | 50 | **50** | Resp.Infraestructuras |
| Tornados | | 1 | 50 | **50** | Resp.Infraestructuras |
| Nieve – Hielo | | 1 | 50 | **50** | Resp.Infraestructuras |
| Frio extremo | | 1 | 50 | **50** | Resp.Infraestructuras |
| Calor extremo | | 3 | 50 | **150** | Resp.Infraestructuras |

| Amenaza: De origen industrial | Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. | | | | |
|---|---|---|---|---|---|
| **Amenaza** | **Activos afectados** | **Frecuencia** | **Impacto** | **Riesgo** | **Responsable** |
| Fuego | • Aplicaciones y soporte<br>• Gestión de las comunicaciones<br>• Servicios web<br>• BBDD<br>• Contingencia y Monitorización<br>• Software de comunicaciones<br>• Monitorización<br>• Correo electrónico<br>• Backup y contingencia<br>• Sistemas operativos<br>• Infraestructura hardware<br>• Líneas de comunicaciones<br>• Proveedores de servicios<br>• Personal informático | 1 | 50 | **50** | Resp.Infraestructuras |
| Agua | | 2 | 50 | **100** | Resp.Infraestructuras |
| Fallos eléctricos | | 2 | 20 | **40** | Resp.Infraestructuras |
| Fallos servicios comunicaciones | | 4 | 50 | **200** | Resp.Infraestructuras |
| Condiciones inadecuadas de temperatura o humedad | | 1 | 50 | **50** | Resp.Infraestructuras |
| Contaminación electromagnética | | 1 | 20 | **20** | Resp.Infraestructuras |
| Avería física de equipos o aplicaciones | | 3 | 40 | **120** | Dpto.Sistemas Inform. |
| Degradación soportes almacenamiento | | 2 | 30 | **60** | Resp.Sistemas |
| Obras interior - exterior | | 1 | 20 | **20** | Resp.Infraestructuras |
| Corte suministro eléctrico | | 2 | 20 | **40** | Resp.Infraestructuras |
| Interrupción otros suministros | | 2 | 20 | **40** | Resp.Infraestructuras |

| Amenaza: errores y fallos no intencionados | Fallos causados por las personas pero sin intención manifiesta. | | | | |
|---|---|---|---|---|---|
| **Amenaza** | **Activos afectados** | **Frecuencia** | **Impacto** | **Riesgo** | **Responsable** |
| Errores de los usuarios: errores de las personas cuando usan los servicios y datos. | • Aplicaciones y soporte<br>• Gestión de las comunicaciones<br>• Servicios web<br>• BBDD<br>• Contingencia y Monitorización<br>• Software de comunicaciones | 4 | 40 | **160** | Usuarios |
| Errores del administrador: errores de personas responsables de la instalación y operación. | | 2 | 50 | **100** | Adm. Dpto Sist.Información |

| | | | | | |
|---|---|---|---|---|---|
| Errores de monitorización: registro erróneo de actividades o falta de información. | • Monitorización<br>• Correo electrónico<br>• Backup y contingencia<br>• Sistemas operativos<br>• Infraestructura hardware<br>• Líneas de comunicaciones<br>• Proveedores de servicios | 4 | 20 | **80** | Adm. Dpto Sist.Información |
| Errores de configuración: introducción de parámetros erróneos. | | 4 | 50 | **200** | Adm.Dpto Sist.Información |
| Difusión de software dañino: difusión no consciente de virus. | | 5 | 50 | **250** | Adm.Dpto Sist.Información |
| Escapes de información: la información llega a personas equivocadas. | | 2 | 50 | **100** | usuarios |
| Alteración de la información de manera accidental. | | 2 | 50 | **100** | usuarios |
| Introducción de información incorrecta accidentalmente. | | 2 | 40 | **20** | Adm.Dpto.Sistemas Información |
| Destrucción de información: borrado accidental de datos | | 4 | 20 | **80** | usuarios |
| Vulnerabilidades de los programas: defectos en la codificación de programas | | 4 | 50 | **200** | Adm.Dpto.Sistemas de Información |
| Errores de mantenimiento. Actualización de programas. | | 3 | 50 | **150** | Adm.Dpto.Sistemas de Información |
| Sustracción de credenciales | | 5 | 50 | **250** | usuarios |
| Caída del sistema por agotamiento de recursos | | 3 | 50 | **150** | Adm.Sistemas |
| Indisponibilidad del personal: | | 2 | 20 | **40** | Director Sistemas Información. |

| | | | | | |
|---|---|---|---|---|---|
| enfermedad, guerra | | | | | |
| Bajas no cursadas | | 5 | 50 | **250** | RRHH/Sist.Infor. |

| **Amenaza: ataques intencionados** | **Fallos intencionados y premeditados causados por las personas.** | | | | |
|---|---|---|---|---|---|
| **Amenaza** | **Activos afectados** | **Frecuencia** | **Impacto** | **Riesgo** | **Responsable** |
| Manipular la configuración | • Aplicaciones y soporte<br>• Gestión de las comunicaciones<br>• Servicios web<br>• BBDD<br>• Contingencia y Monitorización<br>• Software de comunicaciones<br>• Monitorización<br>• Correo electrónico<br>• Backup y contingencia<br>• Sistemas operativos<br>• Infraestructura hardware<br>• Líneas de comunicaciones<br>• Proveedores de servicios | 1 | 50 | **50** | Adm.Dpto.Sistemas Información |
| Suplantación de la identidad del usurario | | 2 | 50 | **100** | Adm.Dpto.Sistemas Información |
| Escalada de privilegios | | 1 | 50 | **50** | Adm.Sistemas |
| Uso de recursos para uso personal | | 1 | 30 | **30** | Adm.Sistemas |
| Difusión de software dañino: virus, troyanos. | | 3 | 50 | **150** | Adm.Sistemas |
| Escapes de información: sustracción de información | | 1 | 50 | **50** | Adm.Dpto.Sistemas de Información |
| Acceso no autorizado | | 1 | 50 | **50** | Adm.Dpto.Sistemas Información |
| Alteración de la información | | 1 | 50 | **50** | Adm.Dpto.Sistemas Información |
| Intercepción del tráfico | | 1 | 50 | **50** | Adm.Comunicaciones |
| Modificación de información | | 1 | 50 | **50** | Adm.Comunicaciones |
| Manipulación de programas | | 1 | 50 | **50** | Adm.Dpto.Sistemas Información |
| Denegación de servicio | | 4 | 50 | **200** | Adm.Dpto.Sistemas |
| Sustracción de credenciales | | 5 | 50 | **250** | Adm.Sistemas |
| Robo de equipos | | 3 | 50 | **150** | Adm.Microinformática |
| Vandalismo | | 2 | 20 | **40** | Resp.Infraestructuras |
| Indisponibilidad deliberada del personal: huelgas, absentismo. | | 1 | 50 | **50** | Director Sistemas Información |

*Figura nº 27: Tablas de Riesgo*

# 10.6 Nivel de riesgo aceptable y residual

La dirección de la Universidad expone que conoce el análisis de riesgos de la Universidad y en coordinación con el Comité de Seguridad de la Información acuerda que:

**Debe ser tratado todo aquel riesgo de nivel Alto o Muy Alto (riesgo igual o superior al valor de 150)**

La dirección junto con el Comité de Seguridad ha estimado que el coste de no reducir o mitigar el riesgo de estos niveles implicaría un coste mucho mayor para la Universidad que el que supone establecer las salvaguardas oportunas para su tratamiento.
Las salvaguardas tienen como objetivo principal limitar el impacto y/o la mitigación del riesgo.

MAGERIT identifica cuatro tipos de salvaguardas:

- Procedimientos.
- Política de personal.
- Soluciones técnicas: Aplicaciones, software, dispositivos físicos ó protección de las comunicaciones.
- Seguridad físicas de las áreas de trabajo.

De acuerdo al resultado obtenido del análisis de riesgos, se han establecido las correspondientes salvaguardas para aquellas amenazas que suponen un riesgo alto o muy alto para los activos de la Universidad.

| Amenaza: Desastres naturales | Riesgo | Salvaguarda |
|---|---|---|
| Tormentas eléctricas | 150 | Instalación de supresores para sobretensiones en los repartidores de líneas analógicas y digitales. |
| Calor extremo | 150 | Equipos de Aire Acondicionado redundantes en CPDs |

| Amenaza: Desastres origen industrial | Riesgo | Salvaguarda |
|---|---|---|
| Fallos líneas comunicaciones | 200 | Enlace de Acceso a Internet de backup basado en un medio físico de acceso diferente al acceso principal. |

| Amenaza: Errores y fallos no intencionados | Riesgo | Salvaguarda |
|---|---|---|
| Errores de los usuarios: errores de las personas cuando usan los servicios y datos. | 160 | Se desarrolla procedimiento donde se recoge el plan de copias de seguridad de todos los sistemas. Ver: IT-004 Rev.0 Instrucción Técnica de Realización de Copias de Seguridad |
| Difusión de software dañino: difusión no consciente de virus. | 250 | Implantación de consola central de Antivirus para el control de la actualización de antivirus en los equipos cliente. |
| Errores de configuración: introducción de parámetros erróneos. | 200 | Se desarrolla procedimiento donde se recoge el plan de copias de seguridad de todos los sistemas. Ver: IT-004 Rev.0 Instrucción Técnica de Realización de Copias de Seguridad |
| Vulnerabilidades de los programas: defectos en la codificación de programas | 200 | Elaboración de programa formativo de acuerdo a la guía OWASP. |
| Errores de mantenimiento. Actualización de programas. | 150 | Se desarrolla procedimiento donde se recoge el plan de copias de seguridad de todos los sistemas. Ver: IT-004 Rev.0 Instrucción Técnica de Realización de Copias de Seguridad |
| Sustracción de credenciales | 250 | Incorporación de cifrado de conexiones en los accesos a servicios con requerimiento de credenciales e integración de AD en la red para logon de sesión. |
| Caída del sistema por agotamiento de recursos | 150 | Implantación de solución en alta disponibilidad para aquellos servicios críticos. |
| Bajas no cursadas | 250 | Se desarrolla procedimiento IT-005 Rev.0 Instrucción Técnica de Bajas de usuarios del sistema. |

| Amenaza: Ataques intencionados | Riesgo | Salvaguarda |
|---|---|---|
| Difusión de software dañino: virus, troyanos. | 150 | Implantación de consola central de Antivirus para el control de la actualización de antivirus en los equipos cliente. |
| Denegación de servicio | 200 | Implantación de solución en alta disponibilidad para aquellos servicios críticos y políticas Anti DoS. |
| Sustracción de credenciales | 250 | Incorporación de cifrado de conexiones en los accesos a servicios con requerimiento de credenciales e integración de AD en la red para logon de sesión. |
| Robo de equipos | 150 | Incorporación de sistemas de videovigilancia en puntos estratégicos. |

*Figura nº 28: Tablas de Riesgo no aceptable*

La Dirección, en coordinación con el Comité de Seguridad de la Información estima que el perjuicio para la Universidad de no mitigar el riesgo de los activos de nivel Medio, Bajo y muy bajo es muy inferior al coste económico que supondría para la Universidad mitigar esos riesgos.

Por lo tanto la Dirección expone que:

**Asume el riesgo definido tras la aplicación de las salvaguardas correspondientes, es decir asume el riesgo de nivel Medio, Bajo y Muy bajo, con valores de riesgo inferiores a 150.**

Además, la Dirección **es consciente del riesgo residual existente en los niveles Alto y Muy alto tras la aplicación de las salvaguardas correspondientes, y es consciente de que el objetivo final de este riesgo es reducirlo a niveles de riesgo aceptable.**

# 11. Propuestas de proyectos

Conocido el nivel de riesgo actual de la Universidad, y con la conformidad de Dirección, se plantean una serie de proyectos alineados con el Plan Director de Seguridad de la Información que permitan mejorar en general el estado de la seguridad, mitigando el riesgo, así como aportando valor añadido en la gestión de procesos y optimización de recursos.

Se adjunta documento anexo **anexo_proyectos.pdf,** con el desarrollo de todos los proyectos planteados.

# 12. Auditoría de cumplimiento

Es necesario en un determinado momento, evaluar la madurez de la seguridad de la Universidad en los diferentes dominios de la norma ISO/IEC 27002:2013.
Se adjunta documento anexo **anexo_nivel_cumplimiento.pdf,** donde se detalla con exactitud la evaluación de cumplimiento.

# 13. Referencias


- International Standards Organization, ISO/IEC 27001:2013
- International Standards Organization, ISO/IEC 27002:2013
- Estevan de Quesada, R. UOC. Auditoría de certificación ISO 27001, PID_00143002
- Cruz Allende D., Garre Gui, S. UOC. Sistema de Gestión de Seguridad de la Información, PID_00177808
- http://colaboracion.uv.mx/rept/files/pdp/2014-161/03-SGSI-GE-OT-001.PDF
- https://seguridadinformaticaufps.wikispaces.com/file/view/Establecimiento+SGSI+-+1150017-1150013.pdf
- http://www.smalltalking.net/papers/boi/ch03.html
- http://openaccess.uoc.edu/webapps/o2/bitstream/10609/19887/13/rduitamaTFM0113Anexo1_Plan%20Director%20Seguridad%20%28TFM%29.pdf

- http://www.pmg-ssi.com/2014/05/analisis-de-la-nueva-version-iso-270012013-i-parte-i/
- http://isc2capitulocolombia.org/portal/images/documents/ISO_27001-2013_ISC2_Colombia_Chapter.pdf
- http://blog.firma-e.com/iso-270012013-analisis-detallado-de-la-nueva-version-parte-1-de-4/
- http://datateca.unad.edu.co/contenidos/233004/47797859-ISO-27002-Espanol.pdf
- https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/
- http://www.incoder.gov.co/documentos/A%C3%91O_2014/Gestion_Incoder/Politicas/Agosto_15/PoliticadeSeguridaddelaInformacion.pdf
- http://www.iso27000.es/download/doc_sgsi_all.pdf
- https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/swf/video_07.swf
- https://www.incibe.es/blogs/post/Seguridad/SecurityBlog/Article_and_comments/analisis_riesgos_pasos_sencillo
- http://es.wikipedia.org
- Cruz Allende D.,UOC. Análisis de Riesgos, PID_00177810.
- https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/822-Procedimientos_de_Seguridad_en_el_ENS/822-Procedimientos_de_seguridad-ANEXOI-081112.pdf


# 14. Glosario de términos

**Activo:** información imprescindible para el correcto funcionamiento de las empresas.

**Auditoría:** examen crítico y sistemático que realiza una persona o grupo de personas independientes del sistema auditado.

**Cluster:** Conjunto de computadoras que se comportan como una única.

**Core:** Sistema central de una red.

**CMM:** Modelo de Capacidad y Madurez.

**CPD:** Centro de Proceso de Datos donde se alojan activos de las organizaciones.

**Diagrama de Gantt:** Herramienta gráfica cuyo objetivo es exponer el tiempo de dedicación previsto para diferentes tareas o actividades a lo largo del tiempo.

**DSI:** Departamento de Sistemas de Información.

**Firewall:** Elemento diseñado para bloquear el acceso no autorizado.

**Indicador:** Instrumentos de medición, basados en hechos y datos, que permiten evaluar la calidad de los procesos, productos y servicios.

**ISO 27001:2013:** Norma certificable para la gestión de un sistema de gestión de la seguridad de la información.

**ISO 27002:2013:** Código de buenas prácticas referenciado en la norma ISO 27001:2013.

**LOPD:** Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal.

**Magerit:** Metodología para el análisis y gestión del riesgo de los sistemas de información desarrollada y promovida por la administración pública.

**Métrica:** Medida numérica directa, que representa un conjunto de datos de negocios en la relación a una o más dimensiones.

**MTA:** Mail Transfer Agent, servicio para la retransmisión de correos entre servidores.

**PDCA:** Plan-Do-Check-Act, base de trabajo y desarrollo del Sistema de Gestión de la Seguridad de la Información.

**PILAR**: Herramienta para la gestión del análisis de riesgos basada en Magerit.

**Riesgo:** Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización

**Riesgo aceptable:** Riesgo conocido y asumido por la Dirección de la Organziación.

**Riesgo residual:** Riesgo asumido por la Dirección de la Organización tras la aplicación de salvaguardas.

**Router:** Dispositivo que proporciona conectividad a nivel de red.

**Salvaguarda:** Control o medida para la mitigación o reducción del riesgo.

**SGSI:** Sistema de gestión de la seguridad.