TRABAJO FIN DE MÁSTER

Universitat Oberta de Catalunya

Presentación del Proyecto

Inclusión de los sistemas de información de una organización dentro del Esquema Nacional de seguridad (ENS) en virtud del Real Decreto 3/2010

Autor: Esteban Sánchez Sánchez

1

CONTENIDO GENERAL

Universitat Oberta de Catalunya

- ❑ **Fase 1. Esquema Nacional de Seguridad**
- ❑ **Fase 2. Entorno del proyecto**
- ❑ **Fase 3. Valoración y Categorización de los sistemas. Controles de seguridad**
- ❑ **Fase 4. Análisis de Riesgos**
- ❑ **Fase 5. Tratamiento y gestión de riesgos. Auditoría interna**
- ❑ **Fase 6. Plan de Mejora de la Seguridad**

2

CONTENIDO FASE 1

- **Fase 1. Esquema Nacional de Seguridad**
  - **1.1 Introducción y Conceptos**
  - **1.2 Relación del ENS con las normas la ISO 27001 e ISO 27002**

3

FASE 1. ESQUEMA NACIONAL DE SEGURIDAD

1.1 INTRODUCCIÓN Y CONCEPTOS

- Real Decreto 3/2010 del 8 de Enero

- 6 Principios básicos:

- Seguridad Integral
- Gestión de Riesgos
- Prevención reacción y recuperación
- Líneas de defensa
- Reevaluación Periódica
- Función diferenciada

4

FASE 1. ESQUEMA NACIONAL DE SEGURIDAD

1.1 INTRODUCCIÓN Y CONCEPTOS

- **15 Requisitos mínimos:**

- Organización e implantación del proceso de seguridad.
- Análisis y gestión de los riesgos.
- Gestión de personal.
- Profesionalidad.
- Autorización y control de los accesos.
- Protección de las instalaciones.
- Adquisición de productos.
- Seguridad por defecto.
- Integridad y actualización del sistema.
- Protección de la información almacenada y en tránsito.
- Prevención ante otros sistemas de información interconectados.
- Registro de actividad.
- Incidentes de seguridad.
- Continuidad de la actividad.
- Mejora continua del proceso de seguridad.

5

FASE 1. ESQUEMA NACIONAL DE SEGURIDAD

1.1 INTRODUCCIÓN Y CONCEPTOS

- **Las dimensiones de la seguridad y sus niveles (Anexo I):**
  - **Disponibilidad:** la información y los servicios deben estar accesibles según las necesidades de la organización.
  - **Autenticidad:** una entidad es quien dice ser.
  - **Integridad:** El activo no se ha alterado de forma no autorizada.
  - **Confidencialidad:** la información o servicio sólo debe estar disponible para los autorizados.
  - **Trazabilidad:** se controlan las actuaciones de una entidad y se le pueden imputar (también se le denomina "no repudio").
- **Niveles de las dimensiones de seguridad (Anexo I):**
  - **Nivel Bajo:** Se utilizará cuando las consecuencias de un incidente de seguridad supongan un perjuicio limitado sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.
  - **Nivel Medio:** Se utilizará cuando las consecuencias de un incidente de seguridad supongan un perjuicio grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.
  - **Nivel Alto:** Se utilizará cuando las consecuencias de un incidente de seguridad supongan un perjuicio muy grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados

6

FASE 1. ESQUEMA NACIONAL DE SEGURIDAD

1.1 INTRODUCCIÓN Y CONCEPTOS

- La categorización de los sistemas (Anexo I):

- **Categoría Alta:** Un sistema de información será de categoría Alta si alguna de sus dimensiones de seguridad alcanza el nivel Alto.
- **Categoría Media:** Un sistema de información será de categoría Media si alguna de sus dimensiones de seguridad alcanza el nivel Medio, y ninguna alcanza un nivel superior.
- **Categoría Básica:** Un sistema de información será de categoría básica si alguna de sus dimensiones de seguridad alcanza el nivel básico, y ninguna alcanza un nivel superior.

- La selección de las medidas de seguridad. (Anexo II):

- **Organizativas (4 medidas en total):** se refieren a la organización global de la seguridad.
- **Operacionales (31 medidas):** son para la protección de la operación del sistema (control de acceso, explotación, continuidad, etc.)
- **De protección (40 medidas):** se centran en proteger activos concretos (instalaciones, personal, equipos, comunicaciones, etc.)

7

FASE 1. ESQUEMA NACIONAL DE SEGURIDAD

1.2 RELACIÓN DEL ENS CON LAS NORMAS ISO 27001 E ISO 27002

	ISO 27001/27002	ENS
Ontología	Norma internacional de seguridad, sin rango legal.	Regulación legal de carácter estatal, perteneciente al ordenamiento jurídico español derivado de la Ley 11/2007.
Carácter	certificación voluntaria	cumplimiento obligatorio
Ámbito de aplicación	Para cualquier sistema de gestión de seguridad de la información.	Para los sistemas de información de las Administraciones públicas comprendidos en el ámbito de aplicación de la Ley 11/2007.
Modulación de las medidas	Según criterio del auditor	Regulado en función de los tipos de activos y los niveles de seguridad requeridos
Evidencia de cumplimiento o conformidad	Mediante certificación, expedida por un auditor autorizado, previa auditoría con resultado satisfactorio	Mediante declaración de conformidad legal, previa auditoría con resultado satisfactorio.

8

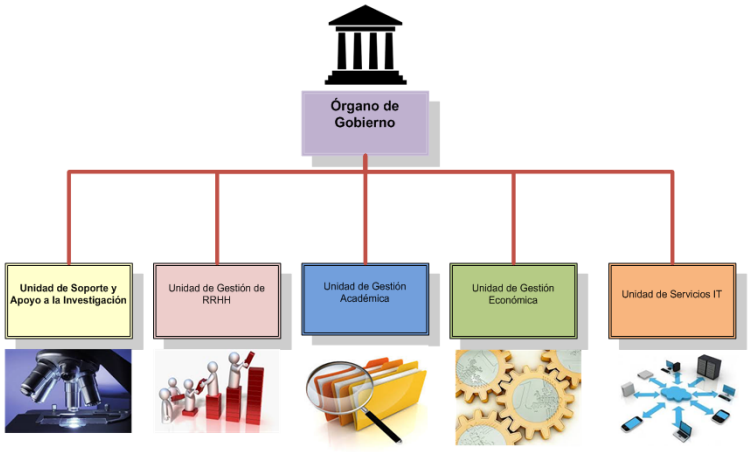
CONTENIDO FASE 2

- Fase 2. Entorno del proyecto
  - 2.1 Organigrama de la UPRG
  - 2.2 Arquitectura de TI general
  - 2.3 Sistema de Información

9

FASE 2. ENTORNO DEL PROYECTO

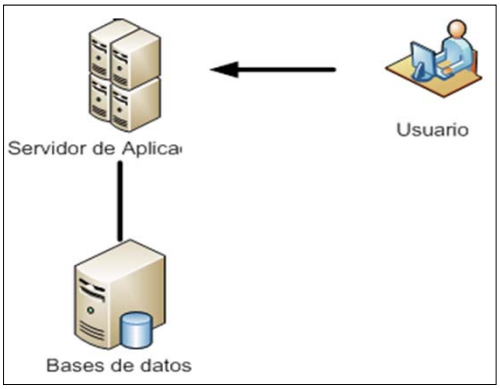
2.1 ORGANIGRAMA DE LA UPRG



10

FASE 2. ENTORNO DEL PROYECTO

2.2 ARQUITECTURA TI GENERAL



11

FASE 2. ENTORNO DEL PROYECTO

2.3 SISTEMAS DE INFORMACIÓN

Sistema	Servicio
Sistema ERP Institucional	ERP – Académico
Sistema ERP Institucional	ERP – Económico
Sistema ERP Institucional	ERP – RRHH
Sistema ERP Institucional	ERP – Investigación
Sistema AE	AE – Sede
Sistema AE	AE - Tablón Oficial
Sistema AE	AE – Registro telemático y tramitación

12

CONTENIDO FASE 3

- **Fase 3. Valoración y Categorización de los sistemas. Controles de seguridad**
  - **3.1 Valoración de información y servicios**
  - **3.2 Categorización de los sistemas**
  - **3.3 Selección de los controles de seguridad**

13

FASE 3. VALORACIÓN Y CATEGORIZACIÓN DE LOS SISTEMAS. CONTROLES DE SEGURIDAD

3.1 VALORACIÓN DE INFORMACIÓN Y SERVICIOS

Dimensión	Criterios Generales para valorar la información	Criterios Generales para valorar los Servicios
Confidencialidad	El nivel de seguridad requerido en el aspecto de confidencialidad se establecerá en función de las consecuencias que tendría su revelación a personas no autorizadas o que no necesitan conocer la información.	
Integridad	El nivel de seguridad requerido en el aspecto de integridad se establecerá en función de las consecuencias que tendría su modificación por alguien que no está autorizado a modificar la información	Los requisitos de integridad sobre un servicio derivan de la información que maneja. Esto incluye la posibilidad de que la información quede en un estado impropio porque el servicio no se complete adecuadamente.
Autenticidad	El nivel de seguridad requerido en el aspecto de autenticidad se establecerá en función de las consecuencias que tendría el hecho de que la información no fuera auténtica.	El nivel de seguridad requerido en el aspecto de autenticidad se establecerá en función de las consecuencias que tendría el hecho de que el servicio fuera usado por personas indebidamente autenticadas; o sea, por personas que no son quienes se cree que son
Trazabilidad	El nivel de seguridad requerido en el aspecto de trazabilidad se establecerá en función de las consecuencias que tendría el no poder rastrear a posteriori quién ha accedido a o modificado una cierta información.	El nivel de seguridad requerido en el aspecto de trazabilidad se establecerá en función de las consecuencias que tendría el no poder rastrear a posteriori quién ha accedido al servicio.
Disponibilidad	El nivel de seguridad requerido en el aspecto de disponibilidad se establecerá en función de las consecuencias que tendría el que una persona autorizada no pudiera acceder a la información cuando la necesita.	El nivel de seguridad requerido en el aspecto de disponibilidad se establecerá en función de las consecuencias que tendría el que una persona autorizada no pudiera usar al servicio cuando lo necesita.

14

FASE 3. VALORACIÓN Y CATEGORIZACIÓN DE LOS SISTEMAS. CONTROLES DE SEGURIDAD

Universitat Oberta de Catalunya

3.1 VALORACIÓN DE INFORMACIÓN Y SERVICIOS

- Ejemplo: Valoración de la información para Sistema ERP Institucional - Servicio de Gestión Académica

Información	Nivel	Motivo
Confidencialidad	Bajo	Información de uso interno para un grupo de Personal de Administración y Servicios (PAS). Sin autorización explícita. Contiene datos personales de nivel bajo.
Integridad	Medio	Daños importantes, aunque subsanables. El principal riesgo es la emisión de títulos auténticos con información falsa.
Autenticidad	Bajo	La falsedad en el origen o el destinatario causaría algún tipo de perjuicio.
Trazabilidad	Bajo	La ausencia de trazabilidad dificultaría la subsanación de errores.
Disponibilidad	Bajo	La disponibilidad común es de 1 a 5 días. Excepcionalmente, en periodos de matrícula y actas deberá ser de menos de 1 día.

15

FASE 3. VALORACIÓN Y CATEGORIZACIÓN DE LOS SISTEMAS. CONTROLES DE SEGURIDAD

Universitat Oberta de Catalunya

3.2 CATEGORIZACIÓN DE LOS SISTEMAS

Servicio	Confidencialidad	Integridad	Autenticidad	Trazabilidad	Disponibilidad	Nivel Global
ERP - Académico	Bajo	Medio	Medio	Bajo	Bajo	Medio
ERP - Económico	Bajo	Medio	Medio	Bajo	Bajo	Medio
ERP - RRHH	Medio	Bajo	Medio	Bajo	Bajo	Medio
ERP - Investigación	Bajo	Bajo	Medio	Sin valorar	Bajo	Medio
ERP - Portal	Bajo	Bajo	Medio	Bajo	Bajo	Medio
AE - Sede	Sin valorar	Medio	Medio	Bajo	Medio	Medio
AE - Tablón Oficial	Sin valorar	Medio	Medio	Bajo	Medio	Medio
AE - Registro Telemático + Tramitación	Medio	Medio	Medio	Medio	Bajo	Medio

Sistema	Confidencialidad	Integridad	Autenticidad	Trazabilidad	Disponibilidad	Nivel Global
Sistema ERP Institucional	Medio	Medio	Medio	Bajo	Bajo	Medio
Sistema AE	Medio	Medio	Medio	Medio	Medio	Medio

16

FASE 3. VALORACIÓN Y CATEGORIZACIÓN DE LOS SISTEMAS. CONTROLES DE SEGURIDAD

Universitat Oberta de Catalunya

3.3 SELECCIÓN DE LOS CONTROLES DE SEGURIDAD

Código	Descripción	Sistema ERP	Sistema AE
org.1	Política de seguridad	aplica	aplica
org.2	Normativa de seguridad	aplica	aplica
org.3	Procedimiento de seguridad	aplica	aplica
org.4	Proceso de autorización	aplica	aplica
op.pl.4	Dimensionamiento / Gestión de capacidades	n.a	aplica
op.pl.5	Componentes certificados	n.a	n.a
mp.if.9	Instalaciones alternativas	n.a	n.a
mp.per.1	Caracterización del puesto de trabajo	aplica	aplica
mp.per.2	Deberes y obligaciones	aplica	aplica
mp.per.3	Concienciación	aplica	aplica
mp.per.4	Formación	aplica	aplica
mp.per.9	Personal alternativo	n.a	n.a
mp.eq.2	Bloqueo de puesto de trabajo	aplica	aplica
mp.eq.3	Protección de equipos portátiles	aplica	aplica
mp.eq.9	Medios alternativos	n.a	aplica

17

CONTENIDO

Universitat Oberta de Catalunya

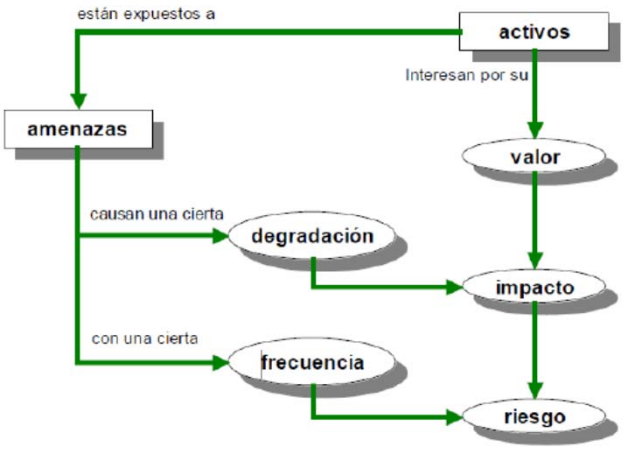
- Fase 4. Análisis de Riesgos
  - 4.1 Conceptos básicos
  - 4.2 Escenario
  - 4.3 Creación del Proyecto
  - 4.4 Modelado de activos. Clases de activos
  - 4.5 Modelo de activos. Dependencias
  - 4.6 Valoración de activos
  - 4.7 Identificación de amenazas
  - 4.8 Valoración de amenazas
  - 4.9 Impacto y riesgo potencial acumulado

18

FASE 4. ANÁLISIS DE RIESGOS

Universitat Oberta de Catalunya

4.1 CONCEPTOS BÁSICOS



19

FASE 4. ANÁLISIS DE RIESGOS

Universitat Oberta de Catalunya

4.1 CONCEPTOS BÁSICOS

Activo:

- **Valor propio:** el del elemento en sí mismo.
- **Valor acumulado:** el proporcional a los elementos que tiene encima
- **Valor nuclear:** El que tiene el elemento de más alto nivel (generalmente la información)

20

FASE 4. ANÁLISIS DE RIESGOS

Universitat Oberta de Catalunya

4.1 CONCEPTOS BÁSICOS

Amenazas:

- Eventos que pueden desencadenar un incidente en la organización produciendo daños materiales o pérdidas inmateriales
- Tipos de amenazas:
  - Naturales
  - Industriales
  - Errores no intencionados
  - Ataques intencionados

21

FASE 4. ANÁLISIS DE RIESGOS

Universitat Oberta de Catalunya

4.1 CONCEPTOS BÁSICOS

- Las amenazas varían de un activo a otro.
- Amenaza por cada activo y dimensión
- No todas las dimensiones afectadas por todas las amenazas

22

FASE 4. ANÁLISIS DE RIESGOS

4.1 CONCEPTOS BÁSICOS

Impacto:

- Medida del daño sobre un activo derivado de la materialización de una amenaza
- Impacto por cada amenaza, activo y dimensión
- 2 tipos de impacto: acumulado y repercutido

23

FASE 4. ANÁLISIS DE RIESGOS

4.1 CONCEPTOS BÁSICOS

Impacto Acumulado:

- Valor acumulado*degradación
- Se calcula sobre un activo teniendo en cuenta:
  - Su valor acumulado (el propio más el acumulado por los activos que dependen de él)
  - Las amenazas a las que está expuesto

24

FASE 4. ANÁLISIS DE RIESGOS

4.1 CONCEPTOS BÁSICOS

Impacto Repercutido:

- Valor propio*degradación
- Se calcula sobre un activo teniendo en cuenta:
  - Su valor propio
  - Las amenazas a las que están expuesto los activos de los que depende

25

FASE 4. ANÁLISIS DE RIESGOS

4.1 CONCEPTOS BÁSICOS

Riesgo:

- Medida del daño probable de un sistema. Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización
- Riesgo por activo amenaza y dimensión

26

FASE 4. ANÁLISIS DE RIESGOS

Universitat Oberta de Catalunya

4.1 CONCEPTOS BÁSICOS

Riesgo Acumulado:

- Impacto acumulado * frecuencia amenaza
- Se calcula sobre un activo teniendo en cuenta:
  - El impacto acumulado sobre un activo
  - La frecuencia de la amenaza

27

FASE 4. ANÁLISIS DE RIESGOS

Universitat Oberta de Catalunya

4.1 CONCEPTOS BÁSICOS

Riesgo Repercutido:

- Impacto repercutido * frecuencia amenaza
- Se calcula sobre un activo teniendo en cuenta:
  - El impacto repercutido sobre un activo
  - La frecuencia de la amenaza

28

FASE 4. ANÁLISIS DE RIESGOS

Universitat Oberta de Catalunya

4.1 CONCEPTOS BÁSICOS

Riesgo potencial:

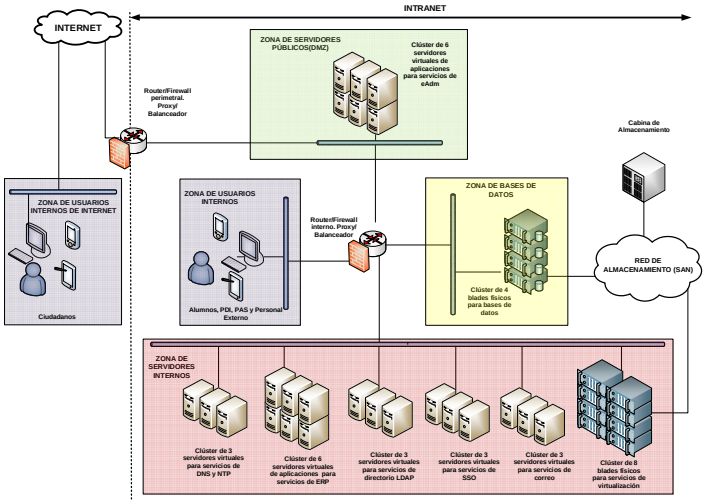
- Riesgo sin tener en cuenta la aplicación de ningún tipo de salvaguarda

29

FASE 4. ANÁLISIS DE RIESGOS

Universitat Oberta de Catalunya

4.2 ESCENARIO



30

FASE 4. ANÁLISIS DE RIESGOS

Universitat Oberta de Catalunya

4.3 CREACION DEL PROYECTO

- ¿Por donde empiezo?

- Información de partida en esta fase:

- Información y servicios que queremos proteger

- Identificación de los 2 sistemas que llevan esta información y servicios

- Incluir resto de activos (aplicaciones, hardware,etc..)

- Recopilar la información de activos y establecer las relaciones entre ellos de acuerdo a los 2 sistemas identificados

- Primera aproximación al modelo de relación entre activos que se acabará reflejando en Pilar

- Mucha voluntad

- Traducir los sistemas y el modelo de relaciones entre los activos de los sistemas al mundo de Pilar

31

FASE 4. ANÁLISIS DE RIESGOS

Universitat Oberta de Catalunya

4.3 CREACIÓN DEL PROYECTO

¿Cómo traslado los 2 sistemas a Pilar?

Se barajaron 3 opciones:

- **Opción 1**→ Un sólo proyecto y un mismo dominio de seguridad

- **Opción 2**→ Un solo proyecto y varios dominios de seguridad

- **Opción 3**→ Un proyecto y un dominio de seguridad por cada sistema

¿Cuál es la mejor opción?

32

FASE 4. ANÁLISIS DE RIESGOS

Universitat Oberta de Catalunya

4.3 CREACIÓN DEL PROYECTO

Opción 1 → Un sólo proyecto y un mismo dominio de seguridad

Ventajas:

- Todo en un único proyecto
- No es necesario replicar activos

Desventajas:

- Modelado complejo
- Pérdida de visión de los sistemas por separado

33

FASE 4. ANÁLISIS DE RIESGOS

Universitat Oberta de Catalunya

4.3 CREACION DEL PROYECTO

Opción 2 → Un solo proyecto y varios dominios de seguridad

Ventajas:

- Todo en un único proyecto
- Visión de los sistemas por separado (uno por dominio)

Desventajas:

- Necesidad de replicar activos entre dominios
- Pilar no termina de funcionar bien con varios dominios

34

FASE 4. ANÁLISIS DE RIESGOS

4.3 CREACIÓN DEL PROYECTO

Opción 3 → Un proyecto y un dominio de seguridad por cada sistema

Ventajas:

- Visión de los sistemas por separado (uno por dominio)

- Seguridad de que Pilar funcionará correctamente

Desventajas:

- Necesidad de replicar activos entre proyectos

35

FASE 4. ANÁLISIS DE RIESGOS

4.4 MODELADO DE ACTIVOS. CLASES DE ACTIVOS

¿Para que sirve tener el activo clasificado?

- Tenerlo clasificado e identificado en el modelo

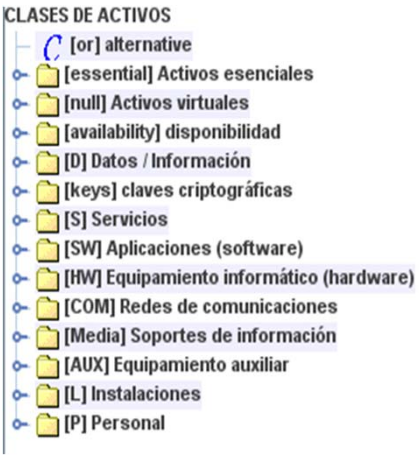
- Agruparlo junto con otros activos de la misma clase facilitando el modelado

¿Sirve para algo más?

- Una amenaza puede afectar a todos los activos a sólo a algunos en base a su clase

- La correspondencia activo -amenaza ya la sabe Pilar. Por tanto clasificarlos permite a Pilar seleccionar por nosotros las amenazas en la fase de identificación de amenazas

- Conclusión: una buena clasificación, no ir a la ligera. Aprovechar las subcategorias que ofrece Pilar



36

FASE 4. ANÁLISIS DE RIESGOS

4.4 MODELADO DE ACTIVOS. CLASES DE ACTIVOS

Capa	Descripción
[I] Capa de Información [Negocio]	Incluye los activos de tipo información. Estos activos
[S] Capa de Servicios [Negocio]	Incluye los activos de tipo servicio. Estos activos junto con los de tipo Información son los más importantes
[A] Aplicaciones	Aplicaciones que actúan de forma conjunta para proporcionar un servicio
[IT] Servicios IT	El objetivo de esta nueva capa es incluir los servicios que aunque no entran dentro del alcance del presente análisis son activos a tener en cuenta de cara a realizar el análisis de riesgo. Esto es así porque se trata de servicios horizontales que son usados por las aplicaciones que sí entran en el análisis y por lo tanto el buen funcionamiento de las aplicaciones depende de estos activos/servicios.

37

FASE 4. ANÁLISIS DE RIESGOS

4.4 MODELADO DE ACTIVOS. CLASES DE ACTIVOS

Capa	Descripción
[H] Hosts	Capa que estaría ubicada en el modelo tradicional entre Aplicaciones y Equipo informático. Incluye los servidores virtualizados considerado desde el punto de vista de un sistema operativo que permite la ejecución software de base (Servidores web, servidores de Aplicaciones,et ...) para las aplicaciones que se ejecutan en ellos. Siempre que sea posible se agruparan los servidores que formen un clúster en un solo activo.
[HW] Hardware	En esta capa se incluye todo lo que sea equipamiento físico tanto a nivel de máquina como a nivel de almacenamiento.
[NET] Redes y Comunicaciones	Incluye todod lo relacionado con las redes y los equipamientos de red
[UBI] Ubicaciones	En esta capa se incluyen los espacios físicos
[P] Personas	Incluye los proveedores, personal del servicio de informatica, Alumnos y PAS/PDI

38

FASE 4. ANÁLISIS DE RIESGOS

4.4 MODELADO DE ACTIVOS. CLASES DE ACTIVOS

Capa	Subcapas	Contenido
[HW] Hardware	[SERV] Servidores	Servidores hardware físicos . Para los servidores que están en clúster creamos un grupo que representa la agrupación de servidores físicos relacionando cada uno de los servidores físicos con este grupo. Esto se hace así para simplificar el modelado de la conexión con lo sistemas de almacenamiento así como con la capa superior de "Hosts". Así por ejemplo se creó el activo Cluster Virtualización. Este activo depende de una serie de blades que lo componen cada uno de los cuales está conectado a la cabina de almacenamiento. Para evitar tener que especificar que cada una de las conexiones de almacenamiento se especificó solamente para Clúster Virtualización.
	[ALM] Sistema de Almacenamiento	Equipos y redes de almacenamiento físico . Permite incluir lo elementos proprios red de almacenamiento SAN como es el caso de la cabina de almacenamiento
	[EQU] Equipos	Dispositivos físicos electrónicos usados por los usuarios ya sean equipos de escritorio o dispositivos móviles
	[SPINF] Soportes de Información	Soportes de información electrónicos
[NET] Redes y Comunicaciones	[NETTOP] Topología	Representa la zona a la que están conectados los activos. Una zona puede estar compuesta por uno o más VLANs
	[NETHW] Equipos de Red	Se incluyen aquí todos los equipos que realizan funciones sobre el tráfico de datos que incluyen el routeado, filtrado de tráfico, proxy y balanceo

39

FASE 4. ANÁLISIS DE RIESGOS

4.4 MODELADO DE ACTIVOS. DEPENDENCIAS

¿Para que sirven las dependencias?

- Construimos un modelo del sistema en base a las relaciones entre sus activos.

- No es un modelo detallado:

  - La herramienta de Pilar no permite modelado complejo

  - La forma de relacionar una activo con otros activos viene determinada por el tipo de activo

  - Tipos de activos diferentes tienen distintos tipos de relaciones (no simpre es "contenido en" o "depende de")

  - Independientemente de los tipos de relaciones ,nuestro objetivo final es hacer un modelo lo más posible y que cumpla con los requisitos para el análisis de riesgo

¿Cómo debe ser un modelo que sirva para el análisis de riesgos?

- El valor acumulado se debe repartir de forma adecuado entre todos los activos.
- Activos de capas inferiores acumulan valor de activos de capas superiores

40

FASE 4. ANÁLISIS DE RIESGOS

Universitat Oberta de Catalunya

4.5 MODELADO DE ACTIVOS. DEPENDENCIAS

Capa	Relaciones con otras capas
[I] Capa de Información [Negocio]	[S] Capa de Servicios [Negocio]. La información se accede a través de los servicios que permiten el acceso a la misma
[S] Capa de Servicios [Negocio]	[S] Capa de Servicios [Negocio]. Para el caso de servicios que son horizontales a otros.
	[IT] Servicios IT. El funcionamiento de las servicios depende de determinados servicios IT
	[A] Aplicaciones. Las aplicaciones incluyen la funcionalidad para proporcionar los servicios
[A] Aplicaciones	[A] Aplicaciones. Ocurre para aplicaciones que son horizontales a otras. En el modelado de ambos sistemas no se han identificado este tipo de dependencias por lo que no aparece en el diagrama sacado de Pilar
	[H] Hosts . Relación con los hosts que contiene el software base sobre el que se ejecutan las aplicaciones.
[IT] Servicios IT	[IT] Servicios IT. Para el caso de servicios que son horizontales a otros.
	[A] Aplicaciones. Las aplicaciones incluyen la funcionalidad para proporcionar los servicios
	[H] Hosts . Relación con los hosts que contiene el software base sobre el que se ejecutan las aplicaciones.

41

FASE 4. ANÁLISIS DE RIESGOS

Universitat Oberta de Catalunya

4.5 MODELADO DE ACTIVOS. DEPENDENCIAS

Capa	Relaciones con otras capas
[H] Hosts	[HW] Hardware. Máquinas hardware sobre las que corre el software base o sistema virtual.
	[NET] Redes y Comunicaciones. Esta relación permite modelar el hecho de que los servidores virtualizados pueden encontrarse en una zona de red diferente al del servidor físico que los contiene.
[HW] Hardware	[HW] Hardware. Para poder establecer relaciones entre el propio equipamiento hardware incluido los servidores y el equipamiento de las redes de almacenamiento SAN
	[NET] Redes y Comunicaciones. Para relacionar con la zona de Red IP en la que se encuentra la máquina hardware. En principio la capa Servidores tiene principalmente relaciones con la Red de almacenamiento SAN siendo las relaciones con la capa de Red IP más propias de la capa "hosts"
	[UBI] Ubicaciones. Al tratarse de activos físicos deben estar en una ubicación.
[NET] Redes y Comunicaciones	[NET] Redes y Comunicaciones. Para relacionar con la zona de Red IP en la que se encuentra un equipo de red
	[UBI] Ubicaciones. Al tratarse de activos físicos deben estar en una ubicación.
[UBI] Ubicaciones	[UBI] Ubicaciones. Es el caso de las salas de comunicaciones y de redes que están ubicada en la unidad de TI, el cual a su vez está ubicado en el campus
	[P] Personas . Las personas acceden a los espacios físicos
[P] Personas	

42

FASE 4. ANÁLISIS DE RIESGOS

4.5 MODELADO DE ACTIVOS. MODELO PARA CADA SISTEMA

Sistema	Capas	Activos
ERP	[I] Capa de Información [Negocio]	[I_ACADE] Información Académica
		[I_ECONO] Información Económica
		[I_RRHH] Información sobre Recursos Humanos
		[I_IDI] Información de Investigación, Desarrollo e Innovación
	[S] Capa de Servicios [Negocio]	[S_ACADE] Servicio ERP Académico
		[S_ECONO] Servicio ERP Económico
		[S_RRHH] Servicio ERP RRHH
		[S_IDI] Servicio ERP Investigación, Desarrollo e Innovación
	[A] Aplicaciones	[A_ACADE] Aplicación de Académico
		[A_CORREO] Aplicación de Correo
		[A_ECONO] Aplicación para Económico
		[A_RRHH] Aplicación de RRHH
		[A_IDI] Aplicación de IDI
	[H] Hosts	[H_SRVWEB] Cluster de 6 VMs para servicios de ERP

43

FASE 4. ANÁLISIS DE RIESGOS

4.5 MODELADO DE ACTIVOS. MODELO PARA CADA SISTEMA

Sistema	Capas	Activos
EADM	[I] Capa de Información [Negocio]	[I_PUBLICACION] Información de publicaciones
		[I_TRAMITACION] Información de Tramitación electrónica
	[S] Capa de Servicios [Negocio]	[S_TABLON] Servicio Tablón Oficial
		[S_TRAMITACION] Servicio de Tramitación Electrónica
		[S_SEDE] Servicio de Sede Electrónica
	[A] Aplicaciones	[A_TABLON] Aplicación Tablón Electrónico
		[A_TRAMITACION] Aplicación Tablón Electrónico
		[A_SEDE] Aplicación de Sede
	[IT] Servicios IT	[IT_PROXY_BALANCEADOR_EXT] Servicio de Proxy y Balanceo para acceso externo
		[IT_DNS_EXT] Servicio DNS consultas publicas
	[H] Hosts	[H_SRVWEB] Cluster de 6 VMs para servicios de AE

44

FASE 4. ANÁLISIS DE RIESGOS

Universitat Oberta de Catalunya

4.5 MODELADO DE ACTIVOS. MODELO PARA CADA SISTEMA

Sistema	Capas	Activos
COMUNES	[IT] Servicios IT	[IT_PROXY_BALANCEADOR_INT] Servicio de Proxy y Balanceo para acceso interno
		[IT_DNS_INT] Servicio DNS consultas internas
		[IT_NTP] Servicio NTP
		[IT_SGBD] Servicio de Bases de Datos
		[IT_DIRECTORIO] Servicio LDAP
		[IT_SSO] Servicio de Autenticación Centralizada y SSO
		[IT_CORREO] Servicio de Correo Electrónico
	[A] Aplicaciones	[A_CORREO] Aplicación de Correo
		[A_DNS] Aplicación de DNS
		[A_NTP] Aplicación de NTP
		[A_SGBD] Sistema de Gestión de Bases de Datos
		[A_DIRECTORIO] Aplicación de LDAP
		[A_SSO] Aplicación de SSO
	[H] Hosts	[H_DNS_NTP] Cluster de 3 VMs para DNS y NTP
		[H_SGBD] Cluster de 3 host físicos de BBDD
		[H_DIRECTORIO] Clúster de 3 VMs de directorio LDAP
		[H_SSO] Clusters de 3 VMs para servicios de SSO
		[H_CORREO] Clúster de 3 VMs de correo para PDI y PAS

45

FASE 4. ANÁLISIS DE RIESGOS

Universitat Oberta de Catalunya

4.5 MODELADO DE ACTIVOS. MODELO PARA CADA SISTEMA

Sistema	Capas	Activos
COMUNES	[HW] Hardware-[SERV] Servidores	[HW_VIRTUALIZACION] Cluster de blades físicos para Virtualización
		[HW_SGBD] Cluster de 3 hosts físicos para SGBD
	[HW] Hardware-[ALM] Sistema de Almacenamiento	[HW_CABINA] Cabina de Almacenamiento
		[HW_NETALM] Red de Almacenamiento
	[HW] Hardware-[EQU] Equipos	[EQU_FIJO] Equipo personal de escritorio de usuario
		[EQU_MOVIL] Equipo móvil de usuario
	[HW] Hardware-[SPINF] Soportes de información	[SPINF_EXTRAIBLES] Soportes extraibles de información
	[NET] Redes y Comunicaciones-[NETTOP] Topología	[NETTOP_WAN] Red Externa e Internet
		[NETTOP_WIFI] Red WIFI
		[NETTOP_DMZ] LAN - Zona Servidores públicos
		[NETTOP_USUARIOS] LAN - Zona equipos de usuarios
		[NETTOP_SRVINT] LAN - Zona Servidores internos
		[NETTOP_BBDD] LAN - Zona Servidores de Bases de Datos
		[NETTOP_GEST] LAN - Zona Gestión de Equipamiento

46

FASE 4. ANÁLISIS DE RIESGOS

4.5 MODELADO DE ACTIVOS. MODELO PARA CADA SISTEMA

Sistema	Capas	Activos
COMUNES	[NET] Redes y Comunicaciones-[NETHW] Equipos de Red	[NETHW_ROUTER_PERIMETRAL] Equipo conectado a la red externa con funciones de Router,Firewall,Proxy y Balanceador
		[NETHW_WAP] Puntos de acceso WIFI
		[NETHW_ROUTER_INTERNO] Equipo interno con funciones de Router,Firewall,Proxy y Balanceador
	[UBI] Ubicaciones	[UBI_IT] Unidad de IT
		[UBI_SERV] Sala de Servidores
		[UBI_COM] Sala de Comunicaciones
		[UBI_CAMPUS] Campus UPRG
	[P] Personas	[P_IT] Personal de IT
		[P_PASPDI] Personal PAS/PDI
		[P_ALU] Alumnos
		[P_PROV] Personal de Proveedores y Subcontratación

47

FASE 4. ANÁLISIS DE RIESGOS

4.6 VALORACIÓN DE ACTIVOS

¿Para que sirve la valoración?

- Nos dará una visión de la importancia de nuestro activo en términos de seguridad en base a la valoración de las 5 dimensiones de la seguridad (IDCAT).

- Se empleará el valor acumulado. Así un activo por sí mismo puede valer menos que la suma de los activos que tiene por encima.

¿Qué escala de valoración se empleo?

- Cualitativa:

Valor en PILAR	Valor en ENS
0	Sin Valorar
1	Bajo
4	Medio
5	Alto

- Se eligió de manera que encajase con los valores que se les dio a la información y a los servicios en la fase previa a Pilar

- La información y los servicios es lo más importante en cuanto a valor nuclear desde el punto de vista del ENS. Su valor se arrastra al resto seleccionando valor acumulado.

48

FASE 4. ANÁLISIS DE RIESGOS

Universitat Oberta de Catalunya

4.7 IDENTIFICACIÓN DE AMENAZAS

Clase de Amenaza	Origen	Descripción
[N] Desastres naturales	Natural (accidental)	Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.
[I] De origen industrial	Entorno (accidental), Humano (accidental o deliberado)	Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.
[E] Errores y fallos no intencionados	Humano (accidental)	Fallos no intencionales causados por las personas.
[A] Ataques intencionados	Humano (deliberado)	Fallos deliberados causados por las personas.

[código] descripción sucinta de lo que puede pasar	
Tipos de activos: • que se pueden ver afectados por este tipo de amenazas	**Dimensiones:** 1. de seguridad que se pueden ver afectadas por este tipo de amenaza, ordenadas de más a menos relevante
Descripción: complementaria o más detallada de la amenaza: lo que le puede ocurrir a activos del tipo indicado con las consecuencias indicadas	

49

FASE 4. ANÁLISIS DE RIESGOS

Universitat Oberta de Catalunya

4.7 IDENTIFICACIÓN DE AMENAZAS

Recordar a la hora de seleccionarlas que:

- Una amenaza puede afectar a uno o varios activos

- Se puede consultar el “ameno” manual con todas las amenazas una por una e ir seleccionado.

¿Cómo se seleccionaron?

- Dejar a Pilar que nos sugiera. Recordar que lo hace en base a como clasificamos los activos

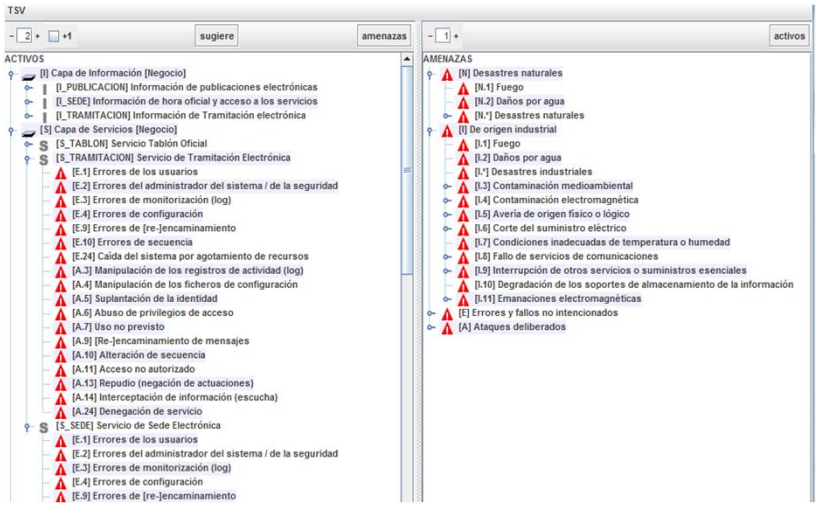
- En base al manual de información de Pilar eliminar las que no convencen o introducir otras nuevas

50

FASE 4. ANÁLISIS DE RIESGOS

Universitat Oberta de Catalunya

4.7 IDENTIFICACIÓN DE AMENAZAS



51

FASE 4. ANÁLISIS DE RIESGOS

Universitat Oberta de Catalunya

4.8 VALORACIÓN DE AMENAZAS

Frecuencia de ocurrencia	Degradación del valor del activo
100 --> muy frecuente–a diario	**5% -->** Degradación Baja
10 --> frecuente–mensualmente	**30% -->** Degradación Media
1 --> normal–una vez al año	**50% -->** Degradación Alta
1/10 --> poco frecuente – cada varios años	**80% -->** Degradación Muy Alta
1/100--> muy infrecuente–cada varias décadas	**100% -->** Completa

52

FASE 4. ANÁLISIS DE RIESGOS

4.8 VALORACIÓN DE AMENAZAS

Recordar a la hora de valorar que:

- Una amenaza puede afectar a una o varias dimensiones de un activo

- Podemos volver a consultar el "ameno" manual con todas las amenazas una por una e ir viendo a que dimensiones afecta.

¿Cómo se valoraron?

1.- Dejar a Pilar que nos sugiera. Recordar que lo hace en base a como describimos nuestro escenario en términos de vulnerabilidad

2.- Partiendo de las valoraciones de Pilar, adaptarlas a nuestra escala

53

FASE 4. ANÁLISIS DE RIESGOS

4.8 VALORACIÓN DE AMENAZAS

Problemas más importantes que surgen al valorar :

- Hay que valorar como si no hubiese salvaguardas (algo bastante complicado).

- Falta una base de datos que recoja de forma detallada todo el histórico de incidentes

-Además se puede pensar que hay amenazas que no se han producido nunca cuando en verdad lo que ha pasado es que:

- Las han parado las salvaguardas que tenemos

- No se han podido detectar que ocurran con los medios de los que se dispone

54

FASE 4. ANÁLISIS DE RIESGOS

Universitat Oberta de Catalunya

4.8 VALORACIÓN DE AMENAZAS

Método a seguir al valorar :

- Reuniones de donde sacar experiencia previa

- Cuando no se tiene experiencia previa de que haya sucedido , para el caso de la frecuencia la seleccionamos de acuerdo con lo probable que es que se produzca ese incidente aunque no haya pasado nunca.

- Cuando valoramos la degradación lo hacemos sin tener en cuenta ningún tipo de salvaguarda, por lo que cosas que ya han pasado provocarán una mayor degradación puesto que no está la salvaguarda que protegió en su momento

55

FASE 4. ANÁLISIS DE RIESGOS

Universitat Oberta de Catalunya

4.8 VALORACIÓN DE AMENAZAS

activo	frecuencia	[D]	[I]	[C]	[A]	[T]
ACTIVOS						
[I] Capa de Información [Negocio]						
[I_PUBLICACION] Información de publicaciones electrónicas		80%	100%		100%	50%
[E.1] Errores de los usuarios	10	10%	10%			
[E.2] Errores del administrador del sistema / de la seguridad	1	30%	10%			
[E.3] Errores de monitorización (log)	1					10%
[E.4] Errores de configuración	1	10%	10%		30%	10%
[E.18] Destrucción de la información	1	10%				
[A.3] Manipulación de los registros de actividad (log)	1					50%
[A.4] Manipulación de los ficheros de configuración	1	50%	10%		10%	30%
[A.5] Suplantación de la identidad	1		50%		100%	
[A.6] Abuso de privilegios de acceso	0,1		30%			
[A.15] Modificación de la información	0,1		100%			
[A.18] Destrucción de la información	0,1	80%				
[I_SEDE] Información de hora oficial y acceso a los servicios		80%	100%		100%	50%
[E.1] Errores de los usuarios	1	10%	10%			
[E.2] Errores del administrador del sistema / de la seguridad	1	30%	10%			
[E.3] Errores de monitorización (log)	1					10%
[E.4] Errores de configuración	1	10%	10%		30%	10%
[E.18] Destrucción de la información	0,1	10%				
[A.3] Manipulación de los registros de actividad (log)	0,1					50%
[A.4] Manipulación de los ficheros de configuración	1	50%	10%		10%	30%
[A.5] Suplantación de la identidad	1		50%		100%	
[A.6] Abuso de privilegios de acceso	0,1		30%			
[A.15] Modificación de la información	0,1		100%			
[A.18] Destrucción de la información	0,1	80%				
[I_TRAMITACION] Información de Tramitación electrónica		80%	100%	100%	100%	50%
[E.1] Errores de los usuarios	10	10%	10%	10%		

56

FASE 4. ANÁLISIS DE RIESGOS

Universitat Oberta de Catalunya

4.9 IMPACTO Y RIESGO POTENCIAL ACUMULADO

{9} - catástrofe
{8} - desastre
{7} - extremadamente crítico
{6} - muy crítico
{5} - crítico
{4} - muy alto
{3} - alto
{2} - medio
{1} - bajo
{0} - despreciable

57

FASE 4. ANÁLISIS DE RIESGOS

Universitat Oberta de Catalunya

4.9 IMPACTO Y RIESGO POTENCIAL ACUMULADO

activo	amenaza	dimensión	impacto
[I_PUBLICACION] Información de publi...	[A.15] Modificación de la información	[I]	[4]
[I_PUBLICACION] Información de publi...	[A.5] Suplantación de la identidad	[A]	[4]
[I_PUBLICACION] Información de publi...	[A.18] Destrucción de la información	[D]	[4]
[I_PUBLICACION] Información de publi...	[A.5] Suplantación de la identidad	[I]	[3]
[I_PUBLICACION] Información de publi...	[A.4] Manipulación de los ficheros de ...	[D]	[3]
[I_PUBLICACION] Información de publi...	[E.2] Errores del administrador del si...	[D]	[2]
[I_PUBLICACION] Información de publi...	[E.4] Errores de configuración	[A]	[2]
[I_PUBLICACION] Información de publi...	[A.6] Abuso de privilegios de acceso	[I]	[2]
[I_PUBLICACION] Información de publi...	[A.4] Manipulación de los ficheros de ...	[I]	[1]
[I_PUBLICACION] Información de publi...	[E.4] Errores de configuración	[D]	[1]
[I_PUBLICACION] Información de publi...	[E.1] Errores de los usuarios	[I]	[1]
[I_PUBLICACION] Información de publi...	[E.18] Destrucción de la información	[D]	[1]
[I_PUBLICACION] Información de publi...	[A.4] Manipulación de los ficheros de ...	[A]	[1]
[I_PUBLICACION] Información de publi...	[E.2] Errores del administrador del si...	[I]	[1]
[I_PUBLICACION] Información de publi...	[E.4] Errores de configuración	[I]	[1]
[I_PUBLICACION] Información de publi...	[E.1] Errores de los usuarios	[D]	[1]
[I_PUBLICACION] Información de publi...	[A.3] Manipulación de los registros d...	[T]	[0]
[I_PUBLICACION] Información de publi...	[A.4] Manipulación de los ficheros de ...	[T]	[0]
[I_PUBLICACION] Información de publi...	[E.4] Errores de configuración	[T]	[0]
[I_PUBLICACION] Información de publi...	[E.3] Errores de monitorización (log)	[T]	[0]
[I_SEDE] Información de hora oficial y ...	[A.5] Suplantación de la identidad	[A]	[4]
[I_SEDE] Información de hora oficial y ...	[A.15] Modificación de la información	[I]	[4]
[I_SEDE] Información de hora oficial y ...	[A.18] Destrucción de la información	[D]	[4]
[I_SEDE] Información de hora oficial y ...	[A.5] Suplantación de la identidad	[I]	[3]
[I_SEDE] Información de hora oficial y ...	[A.4] Manipulación de los ficheros de ...	[D]	[3]
[I_SEDE] Información de hora oficial y ...	[E.4] Errores de configuración	[A]	[2]
[I_SEDE] Información de hora oficial y ...	[A.6] Abuso de privilegios de acceso	[I]	[2]
[I_SEDE] Información de hora oficial y ...	[E.2] Errores del administrador del si...	[D]	[2]
[I_SEDE] Información de hora oficial y ...	[A.4] Manipulación de los ficheros de ...	[I]	[1]

58

FASE 4. ANÁLISIS DE RIESGOS

Universitat Oberta de Catalunya

4.9 IMPACTO Y RIESGO POTENCIAL ACUMULADO

activo	amenaza	dimensión	riesgo
[I_TRAMITACION] Información de Tra...	[A.5] Suplantación de la identidad	[A]	{4,2}
[ALM.HW_CABINA] Cabina de Almace...	[A.6] Abuso de privilegios de acceso	[D]	{4,2}
[S_TRAMITACION] Servicio de Tramita...	[A.5] Suplantación de la identidad	[A]	{4,2}
[ALM.HW_CABINA] Cabina de Almace...	[A.19] Revelación de información	[C]	{4,2}
[ALM.HW_NETALM] Red de Almacena...	[A.5] Suplantación de la identidad	[A]	{4,2}
[H_SSO] Clusters de 3 VMs para servi...	[A.4] Manipulación de los ficheros de ...	[D]	{4,2}
[ALM.HW_CABINA] Cabina de Almace...	[A.4] Manipulación de los ficheros de ...	[D]	{4,2}
[NETTOP.NETTOP_USUARIOS] LAN - Zo...	[A.24] Denegación de servicio	[D]	{4,2}
[I_TRAMITACION] Información de Tra...	[A.19] Revelación de información	[C]	{4,2}
[NETHW.NETHW_ROUTER_PERIMETRAL...	[A.5] Suplantación de la identidad	[A]	{4,2}
[H_SRVWEB] Cluster de 6 VMs para s...	[A.14] Interceptación de información (...	[T]	{4,2}
[ALM.HW_CABINA] Cabina de Almace...	[A.18] Destrucción de la información	[D]	{4,2}
[H_SSO] Clusters de 3 VMs para servi...	[A.4] Manipulación de los ficheros de ...	[C]	{4,2}
[H_SGBD] Cluster de 3 host físicos de...	[A.5] Suplantación de la identidad	[A]	{4,2}
[IT_CORREO] Servicio de Correo Elect...	[A.5] Suplantación de la identidad	[C]	{4,2}
[IT_CORREO] Servicio de Correo Elect...	[A.14] Interceptación de información (...	[C]	{4,2}
[H_SSO] Clusters de 3 VMs para servi...	[A.4] Manipulación de los ficheros de ...	[I]	{4,2}
[NETHW.NETHW_ROUTER_PERIMETRAL...	[A.24] Denegación de servicio	[D]	{4,2}
[IT_DIRECTORIO] Servicio LDAP	[A.5] Suplantación de la identidad	[A]	{4,2}
[H_DNS_NTP] Cluster de 3 VMs para D...	[A.22] Manipulación de programas	[T]	{4,2}
[ALM.HW_CABINA] Cabina de Almace...	[A.4] Manipulación de los ficheros de ...	[A]	{4,2}
[H_SSO] Clusters de 3 VMs para servi...	[A.5] Suplantación de la identidad	[A]	{4,2}
[H_SSO] Clusters de 3 VMs para servi...	[A.5] Suplantación de la identidad	[I]	{4,2}
[ALM.HW_CABINA] Cabina de Almace...	[A.15] Modificación de la información	[I]	{4,2}
[NETHW.NETHW_ROUTER_INTERNO] Eq...	[A.5] Suplantación de la identidad	[A]	{4,2}
[A_TRAMITACION] Aplicación Tablón E...	[A.5] Suplantación de la identidad	[A]	{4,2}
[H_SSO] Clusters de 3 VMs para servi...	[A.5] Suplantación de la identidad	[C]	{4,2}
[ALM.HW_CABINA] Cabina de Almace...	[A.4] Manipulación de los ficheros de ...	[I]	{4,2}
[ALM.HW_CABINA] Cabina de Almace...	[A.4] Manipulación de los ficheros de ...	[C]	{4,2}
[H_SSO] Clusters de 3 VMs para servi...	[A.4] Manipulación de los ficheros de ...	[T]	{4,2}
[H_DIRECTORIO] Clúster de 3 VMs de ...	[A.5] Suplantación de la identidad	[A]	{4,2}

59

CONTENIDO

Universitat Oberta de Catalunya

- Fase 5. Tratamiento y gestión de riesgos
  - 5.1 Conceptos básicos
  - 5.2 Identificación y valoración de salvaguardas. Auditoría interna
  - 5.3 Riesgo residual

60

FASE 5. TRATAMIENTO Y GESTIÓN DE RIESGOS

Universitat Oberta de Catalunya

5.1 CONCEPTOS BÁSICOS

Salvaguardas:

- Se aplican para mitigar o reducir el riesgo hasta unos niveles asumibles por la organización
- Salvaguardas se eligen de forma global
- La salvaguarda debe/puede producir reducción en la degradación de la amenaza para cada dimensión
- La salvaguarda debe/puede producir una reducción en la frecuencia para cada dimensión

61

FASE 5. TRATAMIENTO Y GESTIÓN DE RIESGOS

Universitat Oberta de Catalunya

5.1 CONCEPTOS BÁSICOS

Riesgo Residual:

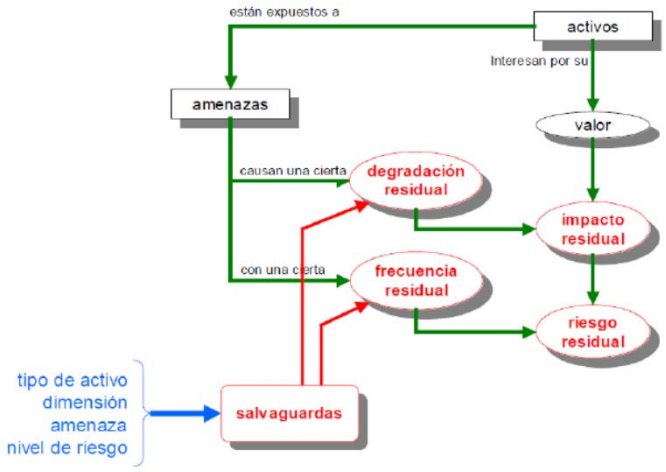
- Riesgo remanente en el sistema tras la implantación de las salvaguardas

62

FASE 5. TRATAMIENTO Y GESTIÓN DE RIESGOS

Universitat Oberta de Catalunya

5.1 CONCEPTOS BÁSICOS



63

FASE 5. TRATAMIENTO Y GESTIÓN DE RIESGOS

Universitat Oberta de Catalunya

5.2. IDENTIFICACIÓN Y VALORACIÓN DE SALVAGUARDAS. AUDITORIA INTERNA

- Informe de auditoría interna

  - Objetivos:

    – Identificar salvaguardas

      » Comprobar la existencia de los controles de seguridad requeridos por el RD 3/2010 en su Anexo II

    – Recopilar evidencias para justificar el nivel de valoración salvaguardas se aplican a nivel global para todo el sistema reduciendo y evitando el riesgo (gestionando el riesgo)

64

FASE 5. TRATAMIENTO Y GESTIÓN DE RIESGOS

Universitat Oberta de Catalunya

5.2. IDENTIFICACIÓN Y VALORACIÓN DE SALVAGUARDAS. AUDITORIA INTERNA

5.3 **Medidas de protección**

5.3.1 Locales, acondicionamiento y control de acceso [mp.if.1-3]

Sistemas a los que aplica	Sistema ERP, Sistema AE
Madurez evaluada	L1-L3

Valoración:

La organización cuenta con dos salas independientes para la infraestructura central del Sistema de Información: sala de servidores y nodo de comunicaciones.

Ambas salas cuentan con control de acceso y están configuradas como centros de proceso de datos, destinándose en exclusiva a la instalación de equipo de telecomunicaciones e informático, contando con el acondicionamiento adecuado.

Evidencias:

Se adjuntan fotografías del control de acceso automatizado, mediante tarjeta RF individual

Ilustración 5-28. Control de acceso a salas mediante tarjeta RF

65

FASE 5. TRATAMIENTO Y GESTIÓN DE RIESGOS

Universitat Oberta de Catalunya

5.2. IDENTIFICACIÓN Y VALORACIÓN DE SALVAGUARDAS. AUDITORIA INTERNA

- Las salvaguardas se aplican a nivel global para todo el sistema reduciendo y evitando el riesgo (gestionando el riesgo)

- Pilar contempla salvaguardas y grupos de salvaguardas

- Estas salvaguardas y grupos se pueden clasificar en función de diferentes criterios:

1 .- Aspecto que se protegerá

G: Aspecto de gestión.
T: Aspecto técnico → medidas más concretas que la de gestión
P: Aspecto de Personal.
F: Aspecto de Seguridad física (instalaciones)

66

FASE 5. TRATAMIENTO Y GESTIÓN DE RIESGOS

Universitat Oberta de Catalunya

5.2. IDENTIFICACIÓN Y VALORACIÓN DE SALVAGUARDAS. AUDITORIA INTERNA

2.- Estrategia que adopta la salvaguarda ante el incidente:

CR: Correctivas (gestión de incidentes)
IM: Minimizar impacto (desconexión de equipos)
RC: Recuperación del incidente (copias de seguridad)
DT: Detección (detectores de incendios)
MN: Monitorización (registros de actividad)
EL: Eliminación (Eliminar cuentas de usuarios que ya no emplean)
PR: Preventiva (autorización previa de usuarios)
DR: Disuasoria (vallas, guardias de seguridad)
AD: Administrativas (inventario de activos)
AW: Concienciación (cursos de concienciación)
std: basadas en normas
proc: basadas en procedimientos
cert: basadas en productos certificados (Firewalls)

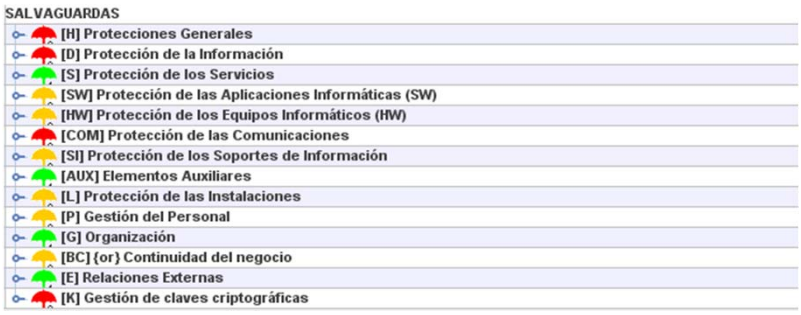
67

FASE 5. TRATAMIENTO Y GESTIÓN DE RIESGOS

Universitat Oberta de Catalunya

5.2. IDENTIFICACIÓN Y VALORACIÓN DE SALVAGUARDAS. AUDITORIA INTERNA

3 .- Clase de activo que protegerá (Grupo principal/raíz)



68

FASE 5. TRATAMIENTO Y GESTIÓN DE RIESGOS

5.2. IDENTIFICACIÓN Y VALORACIÓN DE SALVAGUARDAS. AUDITORIA INTERNA

4.- Importancia de la salvaguarda:

5.- Forma en la que se aplica:

{and}: Deberían aplicarse todas las salvaguardas.

{or}: Debería aplicarse al menos una de las salvaguardas

{xor}: Debería aplicarse sólo una de las salvaguardas (la que mejor aplique → la más recomendada).

69

FASE 5. TRATAMIENTO Y GESTIÓN DE RIESGOS

5.2. IDENTIFICACIÓN Y VALORACIÓN DE SALVAGUARDAS. AUDITORIA INTERNA

6.- Recomendación de su implantación:

1 (blanco) → no recomendable por que no aplica

2,3 (azul) → recomendable

4,5 (amarillo) → bastante recomendable

6,7 (rojo palido) → muy recomendable

8,9 (rojo) → necesaria

70

FASE 5. TRATAMIENTO Y GESTIÓN DE RIESGOS

5.2. IDENTIFICACIÓN Y VALORACIÓN DE SALVAGUARDAS. AUDITORIA INTERNA

- Consideración sobre su aplicación:

[Vacío]: Aplica la salvaguarda o no, según tenga configurado en las "Opciones".

n.a.: No aplica la salvaguarda y, por lo tanto, no se mostrará a la hora de evaluar las salvaguardas. Si se la pongo a un grupo afecta a todo lo que hay por debajo

…: Indica que se trata de un grupo de salvaguardas que contiene a alguna salvaguarda en "n.a.".

- Consideración sobre su estado:

On: Quiero usarla para el análisis
Off: Aunque aplique a mi sistema, en este análisis no la quiero considerar

71

FASE 5. TRATAMIENTO Y GESTIÓN DE RIESGOS

5.2. IDENTIFICACIÓN Y VALORACIÓN DE SALVAGUARDAS. AUDITORIA INTERNA

Consideraciones sobre su selección:

- Cantidad muy elevada de salvaguardas
- Me interesan sobre todo las que se aplican al ENS

¿Hay alguna forma de hacer una preselección?

- Usar perfil de seguridad del ENS → Subconjunto de salvaguardas que se ofrecen en Pilar y que son de aplicación al ENS

72

FASE 5. TRATAMIENTO Y GESTIÓN DE RIESGOS

5.2. IDENTIFICACIÓN Y VALORACIÓN DE SALVAGUARDAS. AUDITORIA INTERNA

Dentro del perfil ENS, Pilar distingue entre:

Apartado	Descripción
Controles	Se corresponden con los apartados principales que aparecen en la normativa del ENS. Sirven para agrupar preguntas y salvaguardas
Preguntas	Se corresponden con los comentarios y subapartados que aparecen en la norma del ENS. Sirven para evaluar el nivel de cumplimiento de la norma pero no tienen influencia sobre los valores del riesgo
Salvaguardas	Se corresponden con las que aparecen en el apartado T.2.1 y que Pilar ha seleccionado para dar cumplimiento a los controles y preguntas de la norma. Si tiene una influencia sobre los valores del riesgo

Para tener un análisis completo Pilar recomienda evaluar todas las salvaguardas y no sólo las que aparecen con la norma

73

FASE 5. TRATAMIENTO Y GESTIÓN DE RIESGOS

5.2. IDENTIFICACIÓN Y VALORACIÓN DE SALVAGUARDAS. AUDITORIA INTERNA

Consideración sobre aplicación de controles y preguntas:

Consideración	Valores
Aplicación de controles y preguntas	• **M:** Es obligatorio a cumplir según la norma. • **[Vacío]:** Es un control que no hay que cumplir según el nivel de la dimensión o se trata de un grupo de controles donde hay uno que no tiene que cumplirla. Ejemplo: [mp.if.9] Instalaciones alternativas • **Gris:** No tiene que cumplir según la norma porque no se han incluido categorías de activos que contempla esa norma Ejemplos: [mp.eq.3] Equipos portátiles • **n.a.:** Es obligatorio según la norma pero en nuestro caso se dan condiciones por las que no se va a cumplir à no influye sobre la gestión del riego

74

FASE 5. TRATAMIENTO Y GESTIÓN DE RIESGOS

Universitat Oberta de Catalunya

5.2. IDENTIFICACIÓN Y VALORACIÓN DE SALVAGUARDAS. AUDITORIA INTERNA

eficacia	nivel	significado	administrativo
0%	**L0**	inexistente	inexistente
10%	**L1**	inicial / ad hoc	iniciado
50%	**L2**	reproducible, pero intuitivo	parcialmente realizado
90%	**L3**	proceso definido	en funcionamiento
95%	**L4**	gestionado y medible	monitorizado
100%	**L5**	optimizado	mejora continua

75

FASE 5. TRATAMIENTO Y GESTIÓN DE RIESGOS

Universitat Oberta de Catalunya

5.2. IDENTIFICACIÓN Y VALORACIÓN DE SALVAGUARDAS. AUDITORIA INTERNA

Código	Descripción	Nivel de madurez	Sistema ERP	Sistema AE
org.1	Política de seguridad	L0-L3	aplica	aplica
org.2	Normativa de seguridad	L0-L1	aplica	aplica
org.3	Procedimiento de seguridad	L1	aplica	aplica
org.4	Proceso de autorización	L0-L2	aplica	aplica

76

FASE 5. TRATAMIENTO Y GESTIÓN DE RIESGOS

Universitat Oberta de Catalunya

5.2. IDENTIFICACIÓN Y VALORACIÓN DE SALVAGUARDAS. AUDITORIA INTERNA

Código	Descripción	Nivel de madurez	Sistema ERP	Sistema AE
op.pl.1	Análisis de riesgos	L3	+	+
op.pl.2	Arquitectura de seguridad	L0-L2	aplica	aplica
op.pl.3	Adquisición de nuevos componentes	L0-L2	aplica	aplica
op.pl.4	Dimensionamiento / Gestión de capacidades	L1-L2	n.a	aplica
op.pl.5	Componentes certificados	L0	n.a	n.a
op.acc.1	Identificación	L2	aplica	aplica
op.acc.2	Requisitos de acceso	L2	aplica	aplica
op.acc.3	Segregación de funciones y tareas	L2	aplica	aplica
op.acc.4	Proceso de gestión de derechos de acceso	L2	aplica	aplica
op.acc.5	Mecanismo de autenticación	L2	+	+
op.acc.6	Acceso local (local logon)	L0-L2	+	+
op.acc.7	Acceso remoto (remote login)	L0-L2	+	+

77

FASE 5. TRATAMIENTO Y GESTIÓN DE RIESGOS

Universitat Oberta de Catalunya

5.2. IDENTIFICACIÓN Y VALORACIÓN DE SALVAGUARDAS. AUDITORIA INTERNA

Código	Descripción	Nivel de madurez	Sistema ERP	Sistema AE
op.exp.1	Inventario de activos	L2	aplica	aplica
op.exp.2	Configuración de seguridad	L1	aplica	aplica
op.exp.3	Gestión de la configuración	L1-L2	aplica	aplica
op.exp.4	Mantenimiento	L1	aplica	aplica
op.exp.5	Gestión de cambios	L1-L2	aplica	aplica
op.exp.6	Protección frente a código dañino	L1-L2	aplica	aplica
op.exp.7	Gestión de incidencias	L1	aplica	aplica
op.exp.8	Registro de la actividad de los usuarios	L0-L1	n.a	n.a
op.exp.9	Registro de la gestión de incidencias	L1	aplica	aplica
op.exp.10	Protección de los registros de actividad	L0-L1	n.a	n.a
op.exp.11	Protección de claves criptográficas	L1-L2	aplica	aplica
op.ext.1	Contratación y SLAs	L3	aplica	aplica
op.ext.2	Gestión diaria	L0-L1	aplica	aplica
op.ext.9	Medios alternativos	L0	n.a	n.a
op.cont.1	Análisis de impacto	L1	n.a	n.a
op.cont.2	Plan de continuidad	L0	n.a	n.a
op.cont.3	Pruebas periódicas	L0	n.a	n.a
op.mon.1	Detección de intrusión	L2	aplica	aplica
op.mon.2	Sistema de métricas	L0-L3	n.a	n.a

78

FASE 5. TRATAMIENTO Y GESTIÓN DE RIESGOS

Universitat Oberta de Catalunya

5.2. IDENTIFICACIÓN Y VALORACIÓN DE SALVAGUARDAS. AUDITORIA INTERNA

Código	Descripción	Nivel de madurez	Sistema ERP	Sistema AE
mp.if.1	Áreas separadas y con control de acceso	L1-L3	aplica	aplica
mp.if.2	Identificación de las personas	L3	aplica	aplica
mp.if.3	Acondicionamiento de los locales	L3	aplica	aplica
mp.if.4	Energía eléctrica	L3	aplica	+
mp.if.5	Protección frente a incendios	L3	aplica	aplica
mp.if.6	Protección frente a inundaciones	L0-L2	n.a	aplica
mp.if.7	Registro de entrada y salida de equipamiento	L0	aplica	aplica
mp.if.9	Instalaciones alternativas	L0	n.a	n.a
mp.per.1	Caracterización del puesto de trabajo	L1-L2	aplica	aplica
mp.per.2	Deberes y obligaciones	L2	aplica	aplica
mp.per.3	Concienciación	L1	aplica	aplica
mp.per.4	Formación	L0-L2	aplica	aplica
mp.per.9	Personal alternativo	L0	n.a	n.a
mp.eq.1	Puesto de trabajo despejado	L1-L2	+	+
mp.eq.2	Bloqueo de puesto de trabajo	L1	aplica	aplica
mp.eq.3	Protección de equipos portátiles	L1	aplica	aplica
mp.eq.9	Medios alternativos	L0	n.a	aplica

79

FASE 5. TRATAMIENTO Y GESTIÓN DE RIESGOS

Universitat Oberta de Catalunya

5.2. IDENTIFICACIÓN Y VALORACIÓN DE SALVAGUARDAS. AUDITORIA INTERNA

Código	Descripción	Nivel de madurez	Sistema ERP	Sistema AE
mp.com.1	Perímetro seguro	L3	aplica	aplica
mp.com.2	Protección de la confidencialidad	L3	aplica	aplica
mp.com.3	Protección de la autenticidad y de la integridad	L3	+	+
mp.com.4	Segregación de redes	L3	n.a	n.a
mp.com.9	Medios alternativos	L3	n.a	n.a
mp.si.1	Etiquetado	L2	aplica	aplica
mp.si.2	Criptografía	L2	aplica	aplica
mp.si.3	Custodia	L2	aplica	aplica
mp.si.4	Transporte	L2	aplica	aplica
mp.si.5	Borrado y destrucción	L0	aplica	aplica
mp.sw.1	Desarrollo	L2-L3	aplica	aplica
mp.sw.2	Aceptación y puesta en servicio	L2	+	+

80

FASE 5. TRATAMIENTO Y GESTIÓN DE RIESGOS

Universitat Oberta de Catalunya

5.2. IDENTIFICACIÓN Y VALORACIÓN DE SALVAGUARDAS. AUDITORIA INTERNA

Código	Descripción	Nivel de madurez	Sistema ERP	Sistema AE
mp.info.1	Datos de carácter personal	L1-L2	aplica	aplica
mp.info.2	Calificación de la información	L1-L2	+	+
mp.info.3	Cifrado	L0	n.a	n.a
mp.info.4	Firma electrónica	L0-L2	+	+
mp.info.5	Sellos de tiempo	L0-L2	n.a	n.a
mp.info.6	Limpieza de documentos	L0	aplica	aplica
mp.info.9	Copias de seguridad (backup)	L2-L3	aplica	aplica
mp.s.1	Protección del correo electrónico	L2-L3	aplica	aplica
mp.s.2	Protección de servicios y aplicaciones web	L1-L2	+	+
mp.s.8	Protección frente a la denegación de servicio	L2	n.a	aplica
mp.s.9	Medios alternativos	L2	n.a	n.a

81

FASE 5. TRATAMIENTO Y GESTIÓN DE RIESGOS

Universitat Oberta de Catalunya

5.2. IDENTIFICACIÓN Y VALORACIÓN DE SALVAGUARDAS. AUDITORIA INTERNA

Sistema	Familia de Medidas	Valoración actual	
		Nivel de madurez	Porcentaje de cumplimiento
Sistema ERP	Medidas Organizativas	L0-L3	26%
	Medidas Operativas	L0-L3	37%
	Medidas Técnicas	L0-L3	48%
	Cumplimiento total	**L0-L3**	**37%**

Sistema	Familia de Medidas	Valoración actual	
		Nivel de madurez	Porcentaje de cumplimiento
Sistema AE	Medidas Organizativas	L0-L3	26%
	Medidas Operativas	L0-L3	37%
	Medidas Técnicas	L0-L3	47%
	Cumplimiento total	**L0-L3**	**37%**

82

FASE 5. TRATAMIENTO Y GESTIÓN DE RIESGOS

Universitat Oberta de Catalunya

5.3. RIESGO RESIDUAL

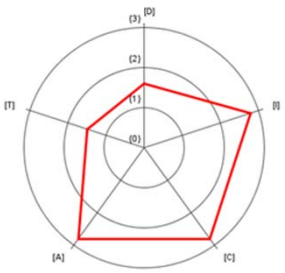


Ilustración 4-18. Riesgo acumulado. Sistema ERP

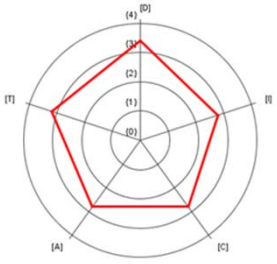


Ilustración 4-19. Riesgo acumulado. Sistema AE

CONTENIDO

Universitat Oberta de Catalunya

- Fase 6. Plan de mejora de la seguridad
  - 6.1 Alcance y Objetivos
  - 6.2 Plan de actuación
  - 6.3 Conclusiones

FASE 6. PLAN DE MEJORA DE LA SEGURIDAD

6.1. ALCANCE Y OBJETIVOS

- Información de partida en esta fase:

- Conclusiones del informe de auditoría
- Resultados del análisis de riesgos

- Fijar acciones a acometer en diferentes áreas:

- Gestión interna del sistema
- Gobierno corporativo de la seguridad
- Otras acciones concretas

- Identificar deficiencias no asumibles

85

FASE 6. PLAN DE MEJORA DE LA SEGURIDAD

6.2. PLAN DE ACTUACIÓN

Código	Bloque
B1	Gestión Interna de la seguridad
B2	Gestión Corporativa de la seguridad
B3	Acciones para madurez de medidas concretas

Plazos	Duración (a ejecutar antes de)
corto	6 meses
medio	1 año
largo	2 años

86

FASE 6. PLAN DE MEJORA DE LA SEGURIDAD

6.2. PLAN DE ACTUACIÓN

Código (Bloque.Prioridad)	Tarea	Descripción	Responsable	Recursos	plazos
B1.1	Mejora de procedimiento de Gestión del Cambio	La sección de TI deberá revisar y mejorar su procedimiento de Gestión del cambio (basado en ITIL) de tal forma que permita gestionar conjuntamente los aspectos que cubre hasta ahora, y que incluya al menos los siguientes aspectos: • Información de capacidad para dimensionamiento sistemático de los cambios que se quieran implementar. • Garantizar la actualización del actual Inventario de Activos (CMDB). • Definir un ciclo de cambio-entrega que garantice la ejecución de pruebas, previas a la puesta en explotación. • Gestionar actualizaciones de seguridad de los activos (al menos de los más críticos o de las actualizaciones más importantes) mediante este proceso. • Revisión del proceso y mejora según la experiencia hasta el momento.	• Gestor del Cambio	• 1 empleado de la sección de TI con rol de Gestor del Cambio • 1 empleado de la sección de TI con rol de Gestor de la Configuración	corto
B1.2	Gestión de incidentes de seguridad	La sección de TI deberá implantar un proceso y herramienta para la gestión de incidentes de seguridad, basado en la herramienta LUCIA, adaptada para el ENS por el CCN-CERT.	• Responsable de Seguridad	• 1 empleado de la sección de TI con rol de Responable de Seguridad • 1 empleado de la sección de TI a la órdenes del Responable de Seguridad	corto

87

FASE 6. PLAN DE MEJORA DE LA SEGURIDAD

6.2. PLAN DE ACTUACIÓN

Código (Bloque.Prioridad)	Tarea	Descripción	Responsable	Recursos	plazos
B1.3	Procedimientos de seguridad	Los responsables del Sistema deberán redactar los siguientes procedimientos por escrito y ponerlos en conocimiento del personal responsable y encargado de su ejecución: • Procedimiento de Gestión de Usuarios: altas, bajas, identificación, autenticación y control de acceso lógico los cambios que se quieran implementar. • Procedimiento de clasificación y tratamiento de la información clasificada del correo electrónico • Procedimiento de generación de copias de respaldo y de recuperación de la información	• Responable del Sistema de AE • Responable del Sistema de ERP	• 1 empleado de la sección de TI con rol de Responable del Sistema de AE • 1 empleado de la sección de TI con rol de Responable del Sistema de ERP	corto
B1.4	Protección de aplicativos web	Los responsables del Sistema deberán mejorar la protección de aplicativos web, implementando de forma sistematizada varias capas de seguridad: filtrado en cabecera de red (cortafuegos) y técnicas de filtrado a nivel de aplicación y/o servidor	• Responable del Sistema de AE • Responable del Sistema de ERP	• 1 empleado de la sección de TI con rol de Responable del Sistema de AE • 1 empleado de la sección de TI con rol de Responable del Sistema de ERP • 1 empleado de la sección de TI encargado de la gestión de la seguridad en red	corto

88

FASE 6. PLAN DE MEJORA DE LA SEGURIDAD

Universitat Oberta de Catalunya

6.2. PLAN DE ACTUACIÓN

Código (Bloque.Prioridad)	Tarea	Descripción	Responsable	Recursos	plazos
B1.5	Arquitectura de seguridad	El responsable de seguridad deberá redactar un Documento de Arquitectura de seguridad, según lo especificado en el ENS.	• Responsable de Seguridad	• 1 empleado de la sección de TI con rol de Responable de Seguridad • 1 empleado de la sección de TI con rol de Responable del Sistema de AE • 1 empleado de la sección de TI con rol de Responable del Sistema de ERP • 1 empleado de la sección de TI a la órdenes del Responable de Seguridad	corto
B1.6	Gestión de claves privadas	Los responsables del Sistema deberán definir un procedimiento para la gestión de claves privadas de servidores y sello de órgano (solicitudes CSR y gestión de certificados: generación, custodia en explotación, etc).	• Responable del Sistema de AE • Responable del Sistema de ERP	• 1 empleado de la sección de TI con rol de Responable del Sistema de AE • 1 empleado de la sección de TI con rol de Responable del Sistema de ERP • 1 empleado de la sección de TI encargado de la gestión de la infraestructura PKI	corto

89

FASE 6. PLAN DE MEJORA DE LA SEGURIDAD

Universitat Oberta de Catalunya

6.2. PLAN DE ACTUACIÓN

Código (Bloque.Prioridad)	Tarea	Descripción	Responsable	Recursos	plazos
B2.1	Difundir política de seguridad	El Equipo de Gobierno, los Responsables del Sistema y el Responsable de Seguridad deberán revisar y actualizar la Política de la UPRG y darle máxima difusión dentro de la Universidad.	• Equipo de Gobierno	• 1 Componente del equipo de Gobierno (Vicerector de nuevas tecnologías o similar) • 1 empleado de la sección de TI con rol de Responable del Sistema de AE • 1 empleado de la sección de TI con rol de Responable del Sistema de ERP • 1 empleado de la sección de TI con rol de Responable de Seguridad	corto
B2.2	Normativas de seguridad	El Equipo de Gobierno, los Responsables del Sistema y el Responsable de Seguridad deberán redactar al menos las siguientes normativas de seguridad y darle máxima difusión dentro de la Universidad. • Deberes y obligaciones del personal en materia de seguridad y las consecuencias su incumplimiento • Uso correcto de equipos, servicios e instalaciones y lo que se considera un uso indebido. • Política de contraseñas de la UPRG	• Equipo de Gobierno	• 1 Componente del equipo de Gobierno (Vicerector de nuevas tecnologías o similar) • 1 empleado de la sección de TI con rol de Responable del Sistema de AE • 1 empleado de la sección de TI con rol de Responable del Sistema de ERP • 1 empleado de la sección de TI con rol de Responable de Seguridad	corto

90

FASE 6. PLAN DE MEJORA DE LA SEGURIDAD

Universitat Oberta de Catalunya

6.2. PLAN DE ACTUACIÓN

Código (Bloque.Prioridad)	Tarea	Descripción	Responsable	Recursos	plazos
B2.3	Política de calificación de la información	l Equipo de Gobierno deberá aprobar una Política de calificación de la información y lo que se puede o no se puede hacer con ella, partiendo de la base de lo que ya hay establecido para el ENS y el cumplimiento de la LOPD. La política debe cubrir aspectos tales como: • Calificación de la información, según su grado de confidencialidad. • Condiciones en el tratamiento de cada tipo de información, según su calificación. • Requisitos para la transmisión de la información. • Restricciones sobre la difusión y almacenamiento.	• Equipo de Gobierno	• 1 Componente del equipo de Gobierno (Vicerector de nuevas tecnologías o similar) • 1 empleado Responable de la Información y Servicios de ERP • 1 empleado Responable de la información y Servicios de AE • 1 empleado de la sección de TI con rol de Responable del Sistema de AE • 1 empleado de la sección de TI con rol de Responable del Sistema de ERP • 1 empleado de la sección de TI con rol de Responable de Seguridad	medio
B2.4	Política de firma y de sellado de tiempo	El Equipo de Gobierno deberá aprobar una Política de Firma y sellado de tiempo que explicite los motivos por los que la información debe, o no, ser firmada digitalmente y los mecanismos usados para ello en cada caso.	• Equipo de Gobierno	• 1 Componente del equipo de Gobierno (Vicerector de nuevas tecnologías o similar) • 1 empleado Responable de la Información y Servicios de ERP • 1 empleado Responable de la información y Servicios de AE • 1 empleado de la sección de TI con rol de Responable del Sistema de AE • 1 empleado de la sección de TI con rol de Responable del Sistema de ERP • 1 empleado de la sección de TI con rol de Responable de Seguridad	medio

91

FASE 6. PLAN DE MEJORA DE LA SEGURIDAD

Universitat Oberta de Catalunya

6.2. PLAN DE ACTUACIÓN

Código (Bloque.Prioridad)	Tarea	Descripción	Responsable	Recursos	plazos
B2.5	Control de calidad de las contraseñas	El responsable del Sistema correspondiente, a instancias del Equipo de Gobierno, deberá implementar mecanismos de control de calidad de las contraseñas que garanticen, al menos, una longitud y complejidad mínimas y un tiempo de vida limitado.	• Equipo de Gobierno	• 1 Componente del equipo de Gobierno (Vicerector de nuevas tecnologías o similar) • 1 empleado de la sección de TI con rol de Responable del Sistema de AE • 1 empleado de la sección de TI con rol de Responable del Sistema de ERP • 1 empleado de la sección de TI con rol de Responable de Seguridad	corto
B2.6	Plan de concicenciación en seguridad TI	El equipo de Gobierno, con el apoyo de los Responsables del Sistema y del Responsable de Seguridad, deberá aprobar y ejecutar un plan de concienciación en Seguridad TI para todo el personal de la organización; este plan incluirá la organización de pequeños talleres y jornadas a lo largo del año, centradas en actividades eminentemente prácticas, así como el envío periódico de píldoras informativas.	• Equipo de Gobierno	• 1 Componente del equipo de Gobierno (Vicerector de nuevas tecnologías o similar) • 1 empleado de la sección de TI con rol de Responable del Sistema de AE • 1 empleado de la sección de TI con rol de Responable del Sistema de ERP • 1 empleado de la sección de TI con rol de Responable de Seguridad	largo

92

FASE 6. PLAN DE MEJORA DE LA SEGURIDAD

Universitat Oberta de Catalunya

6.2. PLAN DE ACTUACIÓN

Código (Bloque.Prioridad)	Tarea	Descripción	Responsable	Recursos	plazos
B2.7	Plan de formación	Tal y como establece el RD 3/2010 de 8 de enero de 2010, el Equipo de Gobierno deberá aprobar un Plan de formación que explícitamente cubra los requisitos en materia de seguridad de la información deseables para el personal de la Unidad de Informática; además deberá dotarlo con los recursos necesarios, ya sea incorporándolo al plan de formación del PAS de la UPRG o reservando una partida económica en el presupuesto anual.	• Equipo de Gobierno	• 1 Componente del equipo de Gobierno (Vicerector de nuevas tecnologías o similar) • 1 empleado de la sección de TI con rol de Responable de Seguridad	largo
B2.8	Protección en los equipos de usuario	Los responsables del Sistema y el Responsable de Seguridad, con la aprobación del Equipo de Gobierno, deberán definir e implementar la homogenización de medidas de protección en los equipos de usuario y en los equipos portátiles, definiendo, según el tipo de equipo, puesto de trabajo e información tratada aspectos de la configuración de seguridad tales como: antivirus, política de actualización de escritorio, cortafuegos personal, bloqueo, encriptación, etc.	• Equipo de Gobierno	• 1 Componente del equipo de Gobierno (Vicerector de nuevas tecnologías o similar) • 1 empleado de la sección de TI con rol de Responable del Sistema de AE • 1 empleado de la sección de TI con rol de Responable del Sistema de ERP • 1 empleado de la sección de TI con rol de Responable de Seguridad • 4 empleados de la sección de TI encargados de dar soporte al usuario	medio

93

FASE 6. PLAN DE MEJORA DE LA SEGURIDAD

Universitat Oberta de Catalunya

6.2. PLAN DE ACTUACIÓN

Código (Bloque.Prioridad)	Tarea	Descripción	Responsable	Recursos	plazos
B3.1	Acceso remoto	Incluirlo en Normativa de seguridad y definir procedimiento de acceso.	• Responsable de Seguridad	• 1 empleado de la sección de TI con rol de Responable de Seguridad • 1 empleado de la sección de TI a la órdenes del Responable de Seguridad	corto
B3.2	Acondicionamiento del CPD	Mejorar el acondicionamiento del CPD: retirar el material que no debe estar allí como cajas y, fundamentalmente, informar al Área de Infraestructuras sobre el riesgo de las tuberías en el techo (inundación) para solucionar este riesgo.	• Responsable de Seguridad	• 1 empleado de la sección de TI con rol de Responable de Seguridad • 1 empleado de la sección de TI a la órdenes del Responable de Seguridad	medio
B3.3	Correo electrónico	Uso obligatorio de protocolos sobre SSL/TLS en el interior de la organización.	• Responsable de Seguridad	• 1 empleado de la sección de TI con rol de Responable de Seguridad • 1 empleado de la sección de TI a la órdenes del Responable de Seguridad	medio

94

FASE 6. PLAN DE MEJORA DE LA SEGURIDAD

Universitat Oberta de Catalunya

6.2. PLAN DE ACTUACIÓN

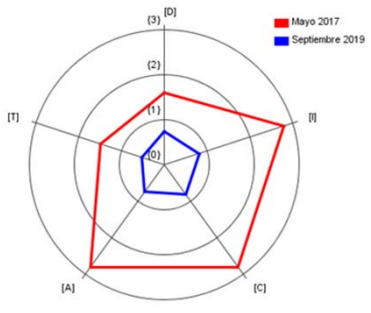
Código (Bloque.Prioridad)	Tarea	Descripción	Responsable	Recursos	plazos
B3.4	Pruebas de recuperación	Ejecución de una prueba de recuperación completa de un servicio al menos, una vez cada dos años.	• Responsable de Seguridad	• 1 empleado Responable de la Información y Servicios de ERP • 1 empleado Responable de la información y Servicios de AE • 1 empleado de la sección de TI con rol de Responable del Sistema de AE • 1 empleado de la sección de TI con rol de Responable del Sistema de ERP • 1 empleado de la sección de TI con rol de Responable de Seguridad • 1 empleado de la sección de TI encargado de la Gestión de copias de seguridad y recuperaciones	largo
B3.5	Ataques de DoS	Para eviitar ataques de DoS activar filtros en firewall de cabecera y también sobre la plataforma de monitorización.	• Responsable de Seguridad	• 1 empleado de la sección de TI con rol de Responable de Seguridad • 1 empleado de la sección de TI encargado de la Gestión de la seguridad en red	corto
B3.6	Destrucción de soportes	Evaluar soluciones para el desarrollo de un procedimiento de destrucción de soportes utilizados en la Unidad de Informática y ofrecer un servicio de destrucción de soportes al usuario del sistema de información.	• Responsable de Seguridad	• 1 empleado de la sección de TI con rol de Responable de Seguridad • 1 empleado de la sección de TI encargado del soporte al usuario	medio

95

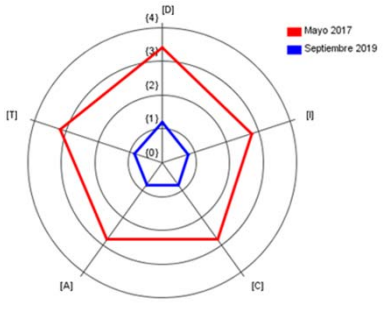
FASE 6. PLAN DE MEJORA DE LA SEGURIDAD

Universitat Oberta de Catalunya

6.3 CONCLUSIONES



Mejora en Riesgo acumulado. Sistema ERP



Mejora en Riesgo acumulado. Sistema AE

96

FASE 6. PLAN DE MEJORA DE LA SEGURIDAD

Universitat Oberta de Catalunya

6.3 CONCLUSIONES

Sistema	Familia de Medidas	Mayo 2017		Septiembre 2019	
		Nivel de madurez	Porcentaje de cumplimiento	Nivel de madurez	Porcentaje de cumplimiento
Sistema ERP	Medidas Organizativas	L0-L3	26%	L3	90%
	Medidas Operativas	L0-L3	37%	L2-L3	90%
	Medidas Técnicas	L0-L3	48%	L1-L3	88%
	Cumplimiento total	**L0-L3**	**37%**	**L1-L3**	**89%**

Sistema ERP: Mejora Nivel de madurez de grupos de medidas y grado de cumplimiento del ENS

Sistema	Familia de Medidas	Mayo 2017		Septiembre 2019	
		Nivel de madurez	Porcentaje de cumplimiento	Nivel de madurez	Porcentaje de cumplimiento
Sistema AE	Medidas Organizativas	L0-L3	26%	L3	90%
	Medidas Operativas	L0-L3	37%	L1-L3	70%
	Medidas Técnicas	L0-L3	47%	L1-L3	87%
	Cumplimiento total	**L0-L3**	**37%**	**L1-L3**	**82%**

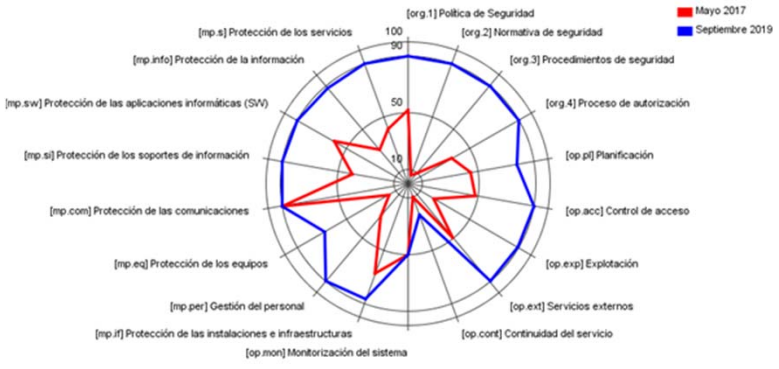
Sistema AE: Mejora Nivel de madurez de grupos de medidas y grado de cumplimiento del ENS

97

FASE 6. PLAN DE MEJORA DE LA SEGURIDAD

Universitat Oberta de Catalunya

6.3 CONCLUSIONES



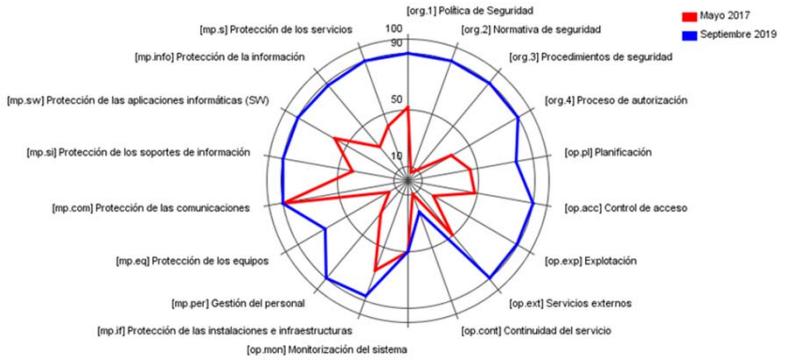
Mejora en grado de cumplimiento del ENS de las medidas para sistema ERP

98

FASE 6. PLAN DE MEJORA DE LA SEGURIDAD

Universitat Oberta de Catalunya

6.3 CONCLUSIONES



Mejora en grado de cumplimiento del ENS de las medidas para sistema AE

99