TRABAJO FIN DE MÁSTER

Universitat Oberta de Catalunya

Resumen Ejecutivo

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

- ❑ 1. Valoración de Servicios
- ❑ 2. Sistema identificados
- ❑ 3. Catalogación de sistemas ENS
- ❑ 4. Aplicabilidad de medidas
- ❑ 5. Resumen ejecutivo del Análisis de Riesgos
- ❑ 7. Cumplimiento del ENS
- ❑ 6. Plan de Mejora de la Seguridad

2

CONTENIDO 1

- 1. Valoración de Servicios
  - 1.1 Valoración de servicios por dimensiones y global

3

1. VALORACIÓN DE SERVICIOS

1.1 VALORACIÓN DE SERVICIOS POR DIMENSIONES Y GLOBAL

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

4

CONTENIDO 2

- 2. Sistemas identificados
  - 2.1 Sistemas identificados y servicios asociados

5

2. SISTEMAS IDENTIFICADOS

2.1 SISTEMAS IDENTIFICADOS Y SERVICIOS ASOCIADOS

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

6

CONTENIDO 3

- 3. Catalogación de sistemas ENS
  - 3.1 Catalogación de sistemas por dimensiones y Global

7

3. CATALOGACIÓN DE SISTEMAS ENS

3.1 CATALOGACIÓN DE SISTEMAS POR DIMENSIONES Y GLOBAL

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

8

CONTENIDO 4

- 4. Aplicabilidad de medidas
  - 4.1 Medidas organizativas
  - 4.2 Medidas operativas
  - 4.3 Medidas de protección

9

4. APLICABILIDAD DE MEDIDAS

4.1 MEDIDAS ORGANIZATIVAS

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

10

4. APLICABILIDAD DE MEDIDAS

Universitat Oberta de Catalunya

4.2 MEDIDAS OPERATIVAS

Código	Descripción	Sistema ERP	Sistema AE
op.pl.1	Análisis de riesgos	+	+
op.pl.2	Arquitectura de seguridad	aplica	aplica
op.pl.3	Adquisición de nuevos componentes	aplica	aplica
op.pl.4	Dimensionamiento / Gestión de capacidades	n.a	aplica
op.pl.5	Componentes certificados	n.a	n.a
op.acc.1	Identificación	aplica	aplica
op.acc.2	Requisitos de acceso	aplica	aplica
op.acc.3	Segregación de funciones y tareas	aplica	aplica
op.acc.4	Proceso de gestión de derechos de acceso	aplica	aplica
op.acc.5	Mecanismo de autenticación	+	+
op.acc.6	Acceso local (local logon)	+	+
op.acc.7	Acceso remoto (remote login)	+	+
op.exp.1	Inventario de activos	aplica	aplica
op.exp.2	Configuración de seguridad	aplica	aplica
op.exp.3	Gestión de la configuración	aplica	aplica
op.exp.4	Mantenimiento	aplica	aplica
op.exp.5	Gestión de cambios	aplica	aplica
op.exp.6	Protección frente a código dañino	aplica	aplica
op.exp.7	Gestión de incidencias	aplica	aplica
op.exp.8	Registro de la actividad de los usuarios	n.a	n.a
op.exp.9	Registro de la gestión de incidencias	aplica	aplica
op.exp.10	Protección de los registros de actividad	n.a	n.a
op.exp.11	Protección de claves criptográficas	aplica	aplica
op.ext.1	Contratación y SLAs	aplica	aplica
op.ext.2	Gestión diaria	aplica	aplica
op.ext.9	Medios alternativos	n.a	n.a
op.cont.1	Análisis de impacto	n.a	n.a
op.cont.2	Plan de continuidad	n.a	n.a
op.cont.3	Pruebas periódicas	n.a	n.a
op.mon.1	Detección de intrusión	n.a	n.a
op.mon.2	Sistema de métricas	n.a	n.a

11

4. APLICABILIDAD DE MEDIDAS

Universitat Oberta de Catalunya

4.3 MEDIDAS DE PROTECCIÓN

Código	Descripción	Sistema ERP	Sistema AE
mp.if.1	Áreas separadas y con control de acceso	aplica	aplica
mp.if.2	Identificación de las personas	aplica	aplica
mp.if.3	Acondicionamiento de los locales	aplica	aplica
mp.if.4	Energía eléctrica	aplica	+
mp.if.5	Protección frente a incendios	aplica	aplica
mp.if.6	Protección frente a inundaciones	n.a	aplica
mp.if.7	Registro de entrada y salida de equipamiento	aplica	aplica
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.1	Puesto de trabajo despejado	+	+
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
mp.com.1	Perímetro seguro	aplica	aplica
mp.com.2	Protección de la confidencialidad	aplica	aplica
mp.com.3	Protección de la autenticidad y de la integridad	+	+
mp.com.4	Segregación de redes	n.a	n.a
mp.com.9	Medios alternativos	n.a	n.a
mp.si.1	Etiquetado	aplica	aplica
mp.si.2	Criptografía	aplica	aplica
mp.si.3	Custodia	aplica	aplica
mp.si.4	Transporte	aplica	aplica
mp.si.5	Borrado y destrucción	aplica	aplica
mp.sw.1	Desarrollo	aplica	aplica
mp.sw.2	Aceptación y puesta en servicio	+	+
mp.info.1	Datos de carácter personal	aplica	aplica
mp.info.2	Calificación de la información	+	+
mp.info.3	Cifrado	n.a	n.a
mp.info.4	Firma electrónica	+	+
mp.info.5	Sellos de tiempo	n.a	n.a
mp.info.6	Limpieza de documentos	aplica	aplica
mp.info.9	Copias de seguridad (backup)	aplica	aplica
mp.s.1	Protección del correo electrónico	aplica	aplica
mp.s.2	Protección de servicios y aplicaciones web	+	+
mp.s.8	Protección frente a la denegación de servicio	n.a	aplica
mp.s.9	Medios alternativos	n.a	n.a

12

CONTENIDO 5

- 5. Resumen ejecutivo del Análisis de Riesgos
  - 5.1 Contexto
  - 5.2 Situación actual

13

5. RESUMEN EJECUTIVO DEL ANÁLISIS DE RIESGOS

5.1 CONTEXTO

- Medidas de seguridad: aplicación puntual de salvaguardas (no orgánica)
- Requisitos de seguridad medios-bajos
- Dimensiones prioritarias: integridad, autenticidad y confidencialidad.
- Dimensión secundaria: disponibilidad
- Dimensión terciaria: trazabilidad.

14

5. RESUMEN EJECUTIVO DEL ANÁLISIS DE RIESGOS

Universitat Oberta de Catalunya

5.2 SITUACIÓN ACTUAL

- **Estado:**
  - Baja madurez y baja homogeneidad en las salvaguardas existentes.
- **Consecuencias:**
  - Valores de riesgo alto en las dimensiones dominantes de cada sistema, debido a la falta de homogeneidad y a la inmadurez de las salvaguardas.

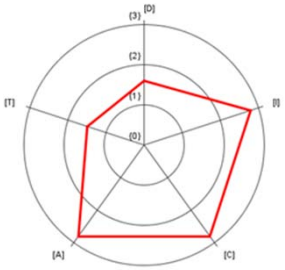


Ilustración 4-18. Riesgo acumulado. Sistema ERP

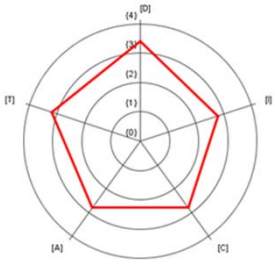


Ilustración 4-19. Riesgo acumulado. Sistema AE

15

CONTENIDO 6

Universitat Oberta de Catalunya

- 6. Cumplimiento del ENS
  - 6.1 Estado actual de cumplimiento del ENS

16

6. CUMPLIMIENTO DEL ENS

6.1 ESTADO ACTUAL DE CUMPLIMIENTO DEL ENS

- **Aportación del ENS a la gestión del riesgo**
  - Madurez en las salvaguardas
  - Homogeneidad en las salvaguardas
- **Consecuencias de la implantación del ENS**
  - Reducción razonable del riesgo a valores medios y medios-bajos.

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%**

Tabla 4-15. Sistema ERP: Nivel de madurez de grupos de medidas y grado de cumplimiento del ENS

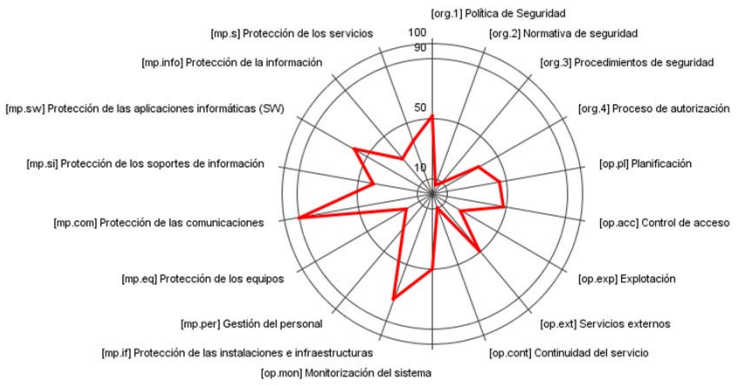
Sistema	Familia de Medidas	Valoración actual	
		Nivel de madurez	Porcentaje de cumplimiento
Sistema AE	Medidas Organizativas	L0-L3	26%
	Medidas Operativas	L0-L3	37%
	Medidas Técnicas	L0-L3	47%
	Cumplimiento total	**L0-L3**	**37%**

Tabla 4-16. Sistema AE: Nivel de madurez de grupos de medidas y grado de cumplimiento del ENS

17

6. CUMPLIMIENTO DEL ENS

6.1 ESTADO ACTUAL DE CUMPLIMIENTO DEL ENS



18

CONTENIDO 7

- 7. Plan de mejora de la Seguridad
  - 7.1 Objetivo y alcance
  - 7.2 Actuaciones para Gestión Interna de la Seguridad
  - 7.3 Actuaciones para Gestión Corporativa de la Seguridad
  - 7.4 Acciones para madurez de medidas concretas
  - 7.5 Conclusiones

19

7. PLAN DE MEJORA DE LA SEGURIDAD

7.1 OBJETIVO Y ALCANCE

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

20

7. PLAN DE MEJORA DE LA SEGURIDAD

7.2 ACTUACIONES PARA GESTIÓN INTERNA DE LA SEGURIDAD

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

21

7. PLAN DE MEJORA DE LA SEGURIDAD

7.2 ACTUACIONES PARA GESTIÓN INTERNA DE LA SEGURIDAD

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

22

7. PLAN DE MEJORA DE LA SEGURIDAD

7.2 ACTUACIONES PARA GESTIÓN INTERNA DE LAS EGURIDAD

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

23

7. PLAN DE MEJORA DE LA SEGURIDAD

7.3 ACTUACIONES PARA GESTIÓN CORPORATIVA DE LA SEGURIDAD

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

24

7. PLAN DE MEJORA DE LA SEGURIDAD

7.3 ACTUACIONES PARA GESTIÓN CORPORATIVA DE LA SEGURIDAD

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

25

7. PLAN DE MEJORA DE LA SEGURIDAD

7.3 ACTUACIONES PARA GESTIÓN CORPORATIVA DE LA SEGURIDAD

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

26

7. PLAN DE MEJORA DE LA SEGURIDAD

7.3 ACTUACIONES PARA GESTIÓN CORPORATIVA DE LA SEGURIDAD

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 Responsable 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 Responsable del Sistema de AE • 1 empleado de la sección de TI con rol de Responsable del Sistema de ERP • 1 empleado de la sección de TI con rol de Responsable de Seguridad • 4 empleados de la sección de TI encargados de dar soporte al usuario	medio

27

7. PLAN DE MEJORA DE LA SEGURIDAD

7.4 ACCIONES PARA MADUREZ DE MEDIDAS CONCRETAS

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 Responsable de Seguridad • 1 empleado de la sección de TI a la órdenes del Responsable 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 Responsable de Seguridad • 1 empleado de la sección de TI a la órdenes del Responsable 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 Responsable de Seguridad • 1 empleado de la sección de TI a la órdenes del Responsable de Seguridad	medio

28

6. PLAN DE MEJORA DE LA SEGURIDAD

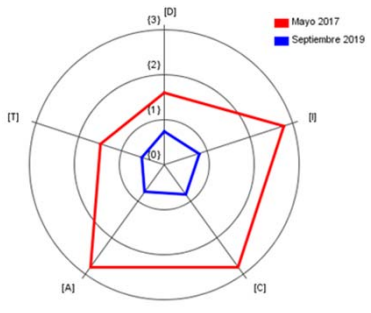
7.4 ACCIONES PARA MADUREZ DE MEDIDAS CONCRETAS

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

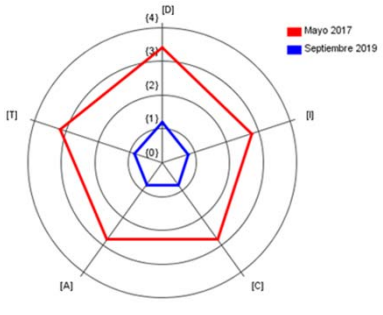
29

7. PLAN DE MEJORA DE LA SEGURIDAD

7.5 CONCLUSIONES



Mejora en Riesgo acumulado. Sistema ERP



Mejora en Riesgo acumulado. Sistema AE

30

7. PLAN DE MEJORA DE LA SEGURIDAD

Universitat Oberta de Catalunya

7.5 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%**

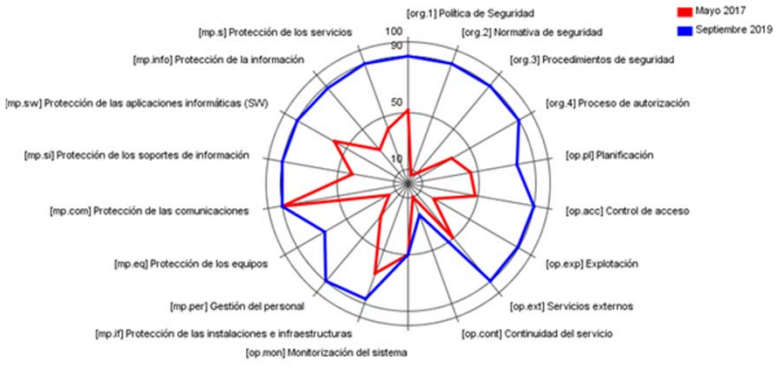
Sistema AE: Mejora Nivel de madurez de grupos de medidas y grado de cumplimiento del ENS

31

7. PLAN DE MEJORA DE LA SEGURIDAD

Universitat Oberta de Catalunya

7.5 CONCLUSIONES

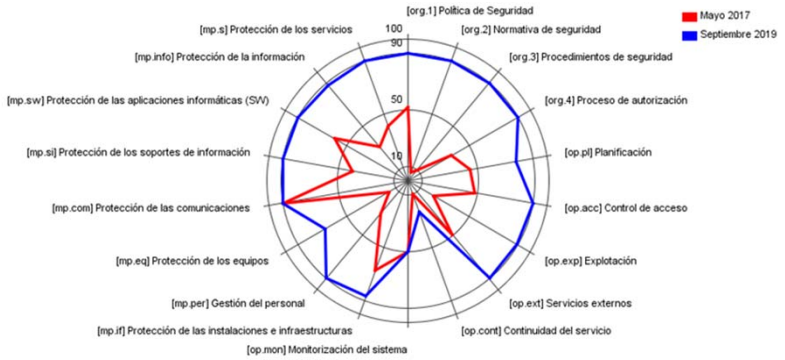


Mejora en grado de cumplimiento del ENS de las medidas para sistema ERP

32

7. PLAN DE MEJORA DE LA SEGURIDAD

7.5 CONCLUSIONES



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

33