2017

ANEXO I

Informe de auditoría interna

Autor: Esteban Sánchez Sánchez

06/06/2017

Índice de Contenido:

Índice de Tablas:

Índice de Imágenes:

1 Tipo, Objetivo y Alcance de la Auditoría

1.1 Objetivos y tipología

Se trata de una auditoría interna que tiene como principal interesado a la Universidad pública de Rocagorda (en adelante UPRG). Dicha auditoría tiene como objetivo comprobar la existencia de los controles de seguridad requeridos por el RD 3/2010 en su Anexo II así como valorar su nivel de madurez de tal forma que sirva para estimar el nivel de riesgo residual de los sistemas auditados. El conocimiento del riesgo residual permitirá a los responsables correspondientes decidir qué riesgos asumen y cuáles otros deciden eliminar o reducir en base a un plan para el tratamiento del riesgo el cual se concrete en una serie de proyectos a desarrollar en diferentes fases

Finalmente el objetivo último de esta auditoría es sustentar la confianza que merece el sistema auditado en materia de seguridad; es decir, calibrar su capacidad para garantizar la integridad, disponibilidad, autenticidad, confidencialidad y trazabilidad de los servicios prestados y la información tratada, almacenada o transmitida.

1.2 Alcance

Los sistemas evaluados son los siguientes:

Sistema	Nivel Global	Entidad Responsable
Sistema ERP Institucional	Medio	UPRG
Sistema AE	Medio	UPRG

Tabla 1-1. Sistemas evaluados

Dichos sistemas representan los siguientes servicios especificados a continuación.

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 + Tramitación

Tabla 1-2. Servicios asociados a los Sistemas

Se quiere puntualizar, no obstante, que el sistema de información de la UPRG contiene otros servicios IT, gestionados por la Unidad de TI o no, que no se encuentran incluidos en el alcance del ENS de la entidad.

Así mismo no ha sido evaluada la interconexión de la UPRG con otras organizaciones más allá del uso de las medidas de seguridad exigibles por el ENS para cualquier tipo de acceso remoto.

1.3 **Equipo auditor**

La auditoría ha sido llevada a cabo por un único auditor externo que actuará como auditor jefe y que ha sido designado por la UPRG. Dicho auditor cumple los requisitos recomendables para llevar a cabo dicha auditoría los cuales se citan a continuación:

- Experiencia verificable y evidenciada de al menos 4 años en auditoría de tecnologías de la información;

- Conocimientos de seguridad y gestión de riesgos de seguridad; conocimiento de los requisitos del RD 3/2010

- Conocimientos de otra legislación aplicable relativa a la protección de datos de carácter personal, y al acceso electrónico de los ciudadanos a los Servicios Públicos

- No haber participado o detentado responsabilidades previas a la auditoría, al menos en los dos últimos años, en el sistema de información auditado.

2 Metodología y Legislación

2.1 Metodología

Para la ejecución del presente proceso de auditoría han sido seguidas las indicaciones al respecto recogidas por el RD 3/2010 por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, así como la información adicional recogida en la guía CCN-STIC 802 titulada “Esquema Nacional de Seguridad: Guía de Auditoría”

2.1.1 Planificación y programa de auditoría

Para la realización del proceso de auditoría se ha realizado una planificación preliminar que, fundamentalmente, ha consistido en establecer los requisitos de información y documentación necesarios e imprescindibles. Concretamente:

- Establecer y desarrollar el programa de auditoría.
- Concretar los conocimientos necesarios del equipo de auditoría.
- Definir la agenda de revisiones, reuniones y entrevistas.
- Definir las revisiones y pruebas a realizar.
- Adjudicar las tareas a los componentes del equipo de auditores y expertos.

Adicionalmente para el desarrollo del programa de auditoría se han tenido en cuenta las siguientes premisas:

- Los criterios organizativos del órgano responsable del sistema auditado y la descripción de las funciones del personal afectados por este sistema.
- Los elementos de la seguridad que pueden auditarse mediante la revisión de documentación, observación, y/ o entrevistas.
- La selección de medidas de seguridad a verificar en cuanto a su cumplimiento tal y como han sido aprobadas.
- Las revisiones que deben realizarse mediante la ejecución de pruebas técnicas.
- Las pruebas podrán realizarse en base a muestras y la elección de una muestra significativa.
- Las evidencias que se espera obtener en cada prueba y cuáles son ineludibles para documentar la realización de la prueba.

2.1.2 Informe final

Una vez confirmados los hechos y deficiencias resultado de las revisiones y pruebas de auditoría, se ha desarrollado el presente informe final que será presentado a los Responsables del Sistema y al Responsable de Seguridad. Este informe se redacta siguiendo las indicaciones de la guía CCN-STIC 802 titulada “Esquema Nacional de Seguridad: Guía de Auditoría”.

2.2 Legislación

Para la ejecución de la presente auditoría se ha tenido en cuenta la legislación que afecta al sistema de información objeto de la misma a fecha de la auditoría, que es:

- Ley Orgánica de Universidades (6/2001) y Ley Orgánica de modificación de la L.O.U. (4/2007).
- Ley 39/2015, de 1 de Octubre, del Procedimiento Administrativo Común
- Ley 40/2015, de 1 de Octubre, del régimen jurídico del sector público.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Ley 34/2002, de 11 de julio de Servicios de la Sociedad de la Información.

3 Resumen ejecutivo

3.1 Valoración del estado actual del sistema

Según la evaluación llevada a cabo en el apartado 5 del presente informe, se emite la siguiente valoración del sistema de información a fecha de Mayo de 2017:

Familia de Medidas	Nivel de madurez actual
Medidas Organizativas	L0-L3
Medidas Operativas	L0-L3
Medidas Técnicas	L0-L3
Cumplimiento total	**L0-L3**

Tabla 3-1. Nivel de madurez actual de las salvaguardas

3.2.- Aspectos fundamentales del informe

El sistema evaluado presenta una madurez media en la gestión de la seguridad de la información, detectándose un esfuerzo significativo en el desarrollo de los principios básicos exigibles por parte del Esquema Nacional de Seguridad como el desarrollo de una política de seguridad, así como la existencia de gran parte de las medidas de protección técnicas a nivel de red.

Sin embargo, el sistema presenta deficiencias muy significativas en dos grandes áreas:

1. Deficiencias muy significativas en las medidas de seguridad exigibles en la explotación diaria del sistema por parte de la unidad de TI debido en parte a la falta de la existencia de una normativa de seguridad a nivel de toda la organización.

2. Deficiencias muy significativas en las medidas asociadas a protección de los recursos informáticos del personal de la Organización y aquellas derivadas de la importancia de la concienciación y formación en materia de seguridad de la información.

3.1.1 Seguridad en la explotación del sistema de información

Estas medidas atañen fundamentalmente a la unidad de TI y están estrechamente relacionadas con la capacidad de la misma para atender las necesidades de seguridad de la información que el trabajo diario requiere: configuración y mantenimiento de sistemas seguros, seguimiento de vulnerabilidades, actualización y aplicación de parches de seguridad, homogeneidad en la gestión de la seguridad, aplicación proactiva de la seguridad, etc.

Estas medidas, en contra de otro tipo de medidas que tienen una naturaleza muy técnica, están principalmente ligadas a la disponibilidad de personal para atender esta gestión.

3.1.2 Medidas de protección del personal y sus recursos informáticos

Estas medidas atañen a la organización en su conjunto, y trascienden con mucho, el alcance de la Unidad de TI como garante de la seguridad de los sistemas de información. Las medidas de

protección de la información gestionada por el personal y sus recursos informáticos, están íntimamente relacionadas con dos aspectos:

1. La capacidad de la organización de involucrarse globalmente en la gestión de la seguridad de la información

2. La existencia de acciones de formación y concienciación sobre el personal.

Únicamente la existencia de ambos aspectos permitirá desplegar medidas de seguridad sobre los recursos informáticos del personal (equipos, soportes, portátiles, teléfonos, etc.); así como prevenir que el personal sea víctima de ataques informáticos sobre la información que gestiona (virus, troyanos, robos de información, etc.).

4 Entrevistas, Documentación y Evidencias

4.1 Entrevistas

Durante el proceso de auditoría las siguientes entrevistas han sido realizadas:

Persona	Duración	Fecha	Objetivo
Técnico de TI responsable jefe de la sección de sistemas	3 horas	28/04/2017	Revisión Medidas Seguridad y Marco Operacional
Técnico de TI responsable jefe de la sección de soporte al usuario final	1 hora	02/05/2017	Revisión Medidas Seguridad y Marco Operacional
Técnico de TI responsable jefe de la sección de Redes	1 hora	02/05/2017	Revisión Medidas Seguridad y Marco Operacional
Técnico de TI responsable jefe de la sección de desarrollo de aplicaciones	1 hora	02/05/2017	Revisión Medidas Seguridad y Marco Operacional
Responsable de seguridad TI	1 hora	03/05/2017	Revisión Medidas Seguridad y Marco Organizativo y Operacional
Jefe la Unidad de TI	1 hora	03/05/2017	Revisión Medidas Seguridad y Marco Organizativo y Operacional
PAS	4 horas	04/05/2017	7 entrevistas a personal PAS no técnico.
PDI	2 horas	05/05/2017	3 entrevistas a personal PDI no técnico.

Tabla 4-1. Personal entrevistado en la auditoría

4.2 Documentación revisada

Durante el proceso de auditoría la siguiente documentación ha sido revisada:

- Política de seguridad
- Acta de Consejo de Gobierno de aprobación de la política de seguridad
- Normativa de seguridad

- Acta de Consejo de Gobierno Comisión de Nuevas Tecnologías de aprobación de las normativas
- Procedimientos y guías de configuración existentes en la unidad de TI
- Documentación relativa a la arquitectura de seguridad: áreas, sistemas, redes,...
- Pliego de adquisición de un componente y pliego de adquisición de un servicio.
- Organigrama / RPT de la organización
- Normativa de contratación de personal
- Deberes y obligaciones del personal
- Acuerdos de confidencialidad.
- Material de formaciones en seguridad.
- Material de acciones de concienciación.
- Documentación de desarrollo seguro y checklists de desarrollo.
- Informes de análisis de vulnerabilidades de aplicativos.
- Referencia a documentos LOPD

4.3 **Recopilación de Evidencias**

Durante la auditoría se han llevado a cabo se han llevado a cabo las pruebas para verificar el cumplimiento de los controles requeridos en el Anexo II del ENS en base a la categoría de cada uno de los sistemas. El resultado de las mismas se ha recopilado en forma de evidencias. La documentación de las entrevistas y la información de los usuarios PAS/PDI de la organización que han sido evaluados en este proceso de auditoría no serán adjunta al presente informe más que de forma desnaturalizada en las tablas y estadísticas que se muestran en la sección sexta.

5 Resultados del proceso de auditoría

5.1 Marco Organizativo

5.1.1 Política de seguridad [org.1]

Sistemas a los que aplica	Sistema ERP, Sistema AE
Madurez evaluada	L0-L3

Tabla 5-1. Política de seguridad. Nivel de madurez

Valoración:

La organización cuenta con una política de seguridad disponible en su sede electrónica. Esta política de seguridad ha sido aprobada por un órgano superior competente según lo dispuesto en el RD3/2010: el Consejo de Gobierno de la UPRG.

Así mismo la política de seguridad precisa los objetivos, la misión de la entidad, el alcance de la misma, el marco legal en el que se desarrolla, además de los roles y la estructura y funciones del comité de seguridad. También se ha detectado que carece de una referencia al documento de seguridad requerido por la LOPD al carecer de dicho documento.

En general, la política de seguridad toma como referencia la publicada en la guía CCN-STIC-805 titulada “Política de Seguridad de la Información”

Evidencias:

La política de seguridad es accesible en https://esede.uprg.es/normas. A continuación se muestra una captura de pantalla del índice de dicha política:

Ilustración 5-1. Política de seguridad de la organización

Recomendaciones:

No existe ninguna acción correctiva a implementar sobre esta medida. No obstante, se recomienda dar la máxima difusión a la política de seguridad en la organización; así como mantenerla actualizada a lo largo del tiempo.

5.1.2 Normativa de seguridad [org.2]

Sistemas a los que aplica	Sistema ERP, Sistema AE
Madurez evaluada	L0-L1

Tabla 5-2. Normativa de seguridad. Nivel de madurez

Valoración:

La organización n o cuenta con una normativa en materia de seguridad relativa a aspectos tan básicos como los relacionados con la seguridad en el uso de los recursos TI de la organización en donde se recoja se recoja el uso correcto de equipo, servicios e instalaciones; así como lo que se considera un mal uso y la responsabilidad de los usuarios.

Evidencias:

No existe ningún tipo de normativa de seguridad de TI accesible en la sede ni en ningún otra ubicación física

Recomendaciones:

Se sugiere al menos desarrollar las siguientes normativas:

- 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

Una vez elaboradas se deberá dar la máxima difusión a estas normativas para favorecer la concienciación del personal en la adopción de las recomendaciones que en ella se hacen: calidad de contraseñas, protección de los equipos, actualización, sistema antivirus, etc.

5.1.3 Procedimientos de seguridad [org.3]

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

Tabla 5-3. Procedimientos de seguridad. Nivel de madurez

Valoración:

La organización no cuenta con documentos que describan los procedimientos de seguridad internos que describen como realizar tareas habituales en el sistema de información que indiquen:

- Cómo llevar a cabo las tareas habituales
- Quién debe hacer cada tarea
- Cómo identificar comportamientos anómalos
- Cómo reportar comportamiento anómalos

Evidencias:

Los empleados TI entrevistados no han sido capaces de aportar documentación que ilustre los procedimientos técnicos aludiendo que cada trabajador sabe lo que tiene que hacer y que lo aprende con el día a día del puesto.

Recomendaciones:

La guía CCN-STIC 822 titulada “Procedimientos de Seguridad” proporciona una serie de anexos que describen procedimientos técnicos y que sirven como plantilla para que un organismo pueda elaborar los suyos propios. Se recomienda seguir dichos anexos para elaborar los siguientes procedimientos técnicos contemplados en dicha guía:

- Procedimiento de Gestión de Usuarios: altas, bajas, identificación, autenticación y control de acceso lógico

- 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

5.1.4 Proceso de autorización [org.4]

Sistemas a los que aplica	Sistema ERP, Sistema AE
Madurez evaluada	L0-L2

Tabla 5-4. Proceso de autorización. Nivel de madurez

Valoración:

Existe un proceso de autorizaciones ad-hoc que cubre los siguientes aspectos:

- La utilización de instalaciones, habituales y alternativas.

- La entrada de equipos en producción

- La entrada de aplicaciones en producción

- Establecimiento de enlaces de comunicaciones con otros sistemas

- Utilización de soportes de información

No obstante no existen documentos formales que recojan dichos procesos de autorización. Además este proceso de autorización es parcial y únicamente afecta a la infraestructura centralizada (servidores, comunicaciones, aplicativos, servicios,...) no afectado por ejemplo a la utilización de equipos móviles o de otro tipo de recursos TI no centralizados.

Evidencias:

No se han encontrado documentos formales que describan dicho procedimiento. LE personal TI entrevistado da fé de que existe dicho proceso pero al parecer varía en función de la persona responsable del recursos que se autoriza.

Recomendaciones:

Establecer un documento formal y aplicable a todo el conjunto de la organización y particularmente al uso de dispositivos móviles.

5.2 Marco Operacional

5.2.1 Análisis de riesgos [op.pl.1]

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

Tabla 5-5. Análisis de Riesgos. Nivel de madurez

Valoración:

Se ha llevado a cabo un análisis de riesgos cualitativo en ambos sistemas empleando un lenguaje semiformal y usando una catálogo básico de amenazas y una semántica definida tal y como le corresponde a un sistema de categoría media.

Evidencias:

El análisis de riesgos está formado por 2 ficheros correspondientes a proyectos de PILAR para cada uno de los 2 sistemas:

- PILAR41.ENS.AE.mgr
- PILAR51.ENS.ERP.mgr

En dichos ficheros se puede verificar el análisis de riesgos desarrollado y cómo satisface las exigencias marcadas por el ENS. Además existen 2 informes obtenidos a partir de la herramienta PILAR que plasman en un documento dicho análisis de riesgos. Estos documentos son:

- Análisis de Riesgos AE.docx
- Análisis de Riesgos ERP.docx

Recomendaciones:

No existen acciones correctivas a implementar sobre la medida. La única recomendación es continuar actualizando el análisis de riesgos y utilizando su información para gestionar los riesgos de la organización, mediante la atención a las áreas críticas de riesgo y a las vulnerabilidades.

5.2.2 Arquitectura de seguridad [op.pl.2]

Sistemas a los que aplica	Sistema ERP, Sistema AE
Madurez evaluada	L0-L2

Tabla 5-6. Arquitectura de Seguridad. Nivel de madurez

Valoración:

No existe una documentación que refleje la arquitectura de seguridad según el espíritu presentado por el ENS, donde se recojan las áreas, los puntos de acceso, los sistemas, los equipos, las redes,

la conectividad con el exterior, las líneas de defensa, los cortafuegos, las tecnologías, la identificación de usuarios, los controles técnicos, etc.

Lo más similar a esta arquitectura de seguridad es la información contenida en el análisis de riesgos y los esquemas de red de los que dispone la organización. No obstante, sólo se satisfacen parcialmente las exigencias de la medida.

Evidencias:

A continuación se recoge una captura de pantalla donde se puede ver a alto nivel las diferentes zonas y su interconexión contenida en el análisis de riesgos

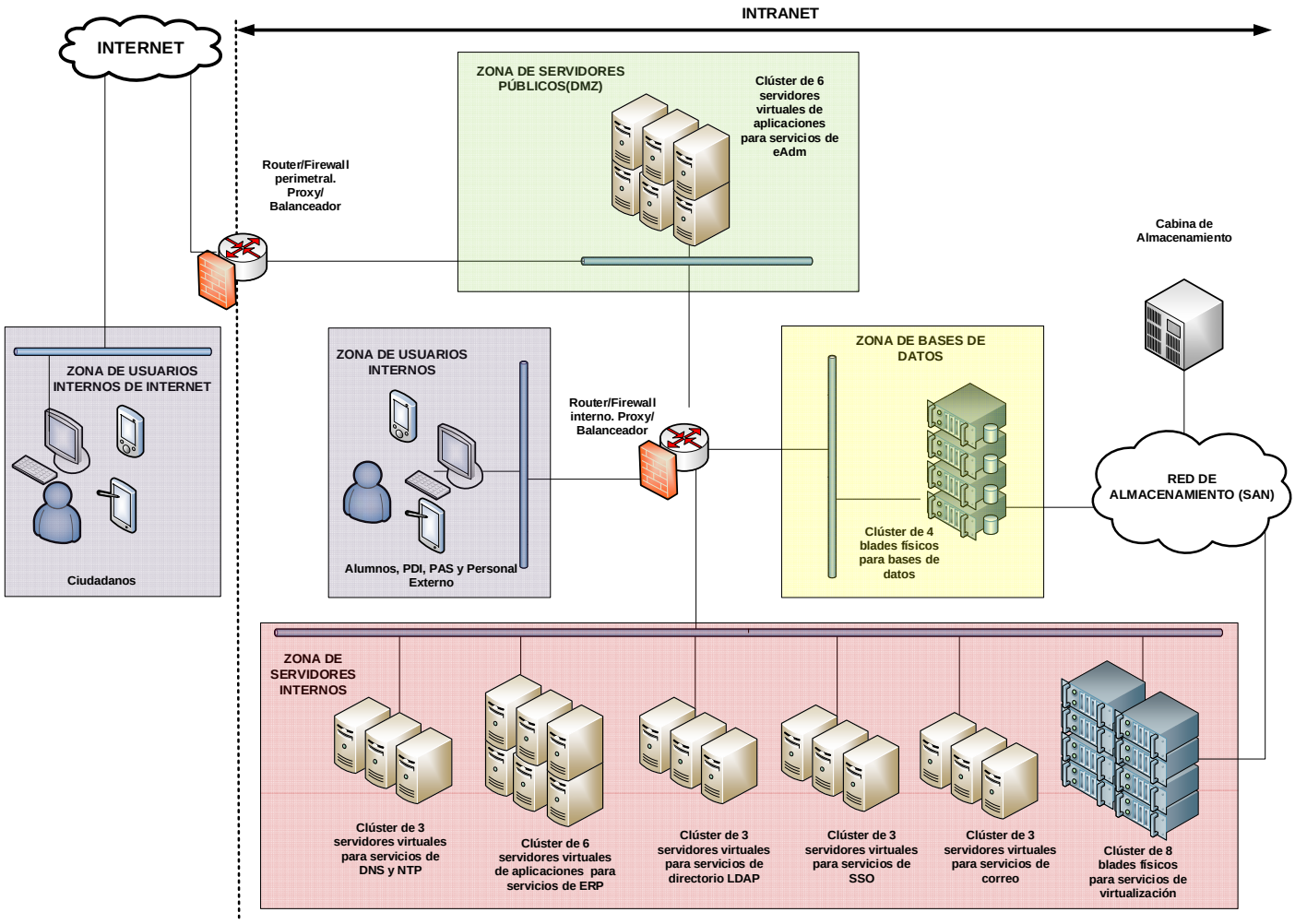

Ilustración 5-2. Arquitectura lógica de red

Recomendaciones:

Se recomienda alinear la información existente con las exigencias del ENS y completar aquellos aspectos que sean necesarios.

5.2.3 Adquisición de nuevos componentes [op.pl.3]

Sistemas a los que aplica	Sistema ERP, Sistema AE
Madurez evaluada	L0-L2

Tabla 5-7. Adquisición de nuevos componentes. Nivel de madurez

Valoración:

La adquisición de nuevos componentes no es un proceso que haya sido definido bajo la perspectiva del ENS para la organización.

En este sentido la organización no cuenta con una lista de requisitos de seguridad que debe satisfacer cada uno de los elementos hardware o software del sistema de información.

No obstante, tras revisar los pliegos de adquisición de los últimos servicios y productos, si bien es cierto que en general no se especifican requisitos de seguridad en ellos; en algún caso puntual, principalmente ligado a la compra de material hardware, estos requisitos sí han sido identificados.

Evidencias:

A continuación se recogen las especificaciones de seguridad para la adquisición de puntos de acceso inalámbricos:

1. Posibilidad de IEEE 802.11i, Wi-Fi Protected Access 2 (WPA2) o WPA.
2. Cifrado seguro AES (Norma de codificación avanzada) y TKIP (Protocolo de integridad de clave temporal).
3. Funciones de control de acceso de cliente para punto de acceso:
   - Autenticación IEEE 802.1X mediante EAP-TLS, EAP-TTLS y PEAP.
   - RADIUS AAA con EAP-MD5, PAP, CHAP y MS-CHAPv2
   - Cliente RADIUS

Ilustración 5-3. Especificaciones para puntos de acceso inalámbricos

Recomendaciones:

Se recomienda extender la acción puntual de identificar requisitos de seguridad a todo proceso de adquisición de material o servicios, como parte del proceso de gestión de cambios y autorización de los mismos.

En caso de que una nueva adquisición no tenga requisitos de seguridad aplicables, se recomienda que se especifique que es así.

5.2.4 Dimensionamiento y gestión de capacidades [op.pl.4]

Sistemas a los que aplica	Sistema AE
Madurez evaluada	L1-L2

Tabla 5-8. Dimensionamiento y gestión de capacidades. Nivel de madurez

Valoración:

El dimensionamiento y la gestión de la capacidad del sistema de información es un proceso que informalmente forma parte del proceso de aprobación de cambios de la organización.

El cambio es evaluado y valorado e implícitamente se valoran las necesidades de procesamiento, las necesidades de almacenamiento, las necesidades de comunicación, el impacto del cambio sobre el sistema de información, etc.

Adicionalmente, los sistemas son monitorizados en tiempo real mediante un software de monitorización.

Evidencias:

A continuación se adjunta captura de pantalla del detalle uno de los activos monitorizados, en el cual se puede ver cómo se obtiene información de disco, memoria, CPU o red.

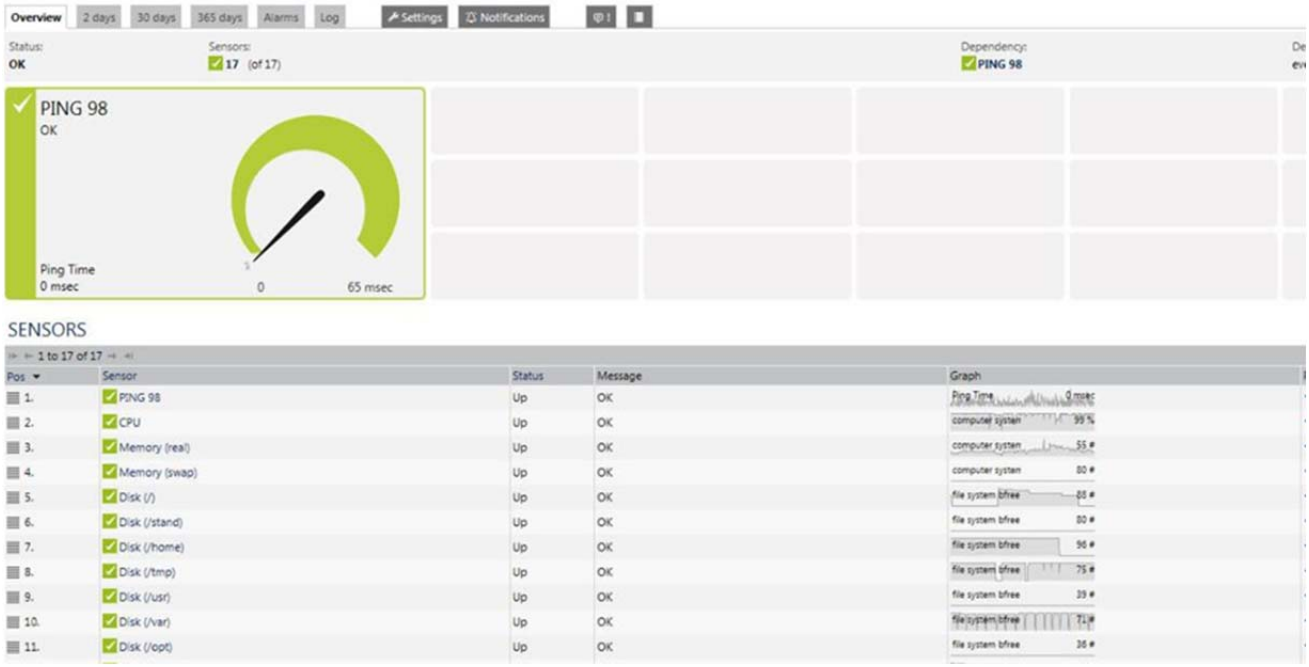

Ilustración 5-4. Monitorización de dispositivo vía software

Recomendaciones:

Se recomienda utilizar la información de capacidad del sistema de información como parte de la entrada del proceso de gestión de cambios, de tal forma que exista un dimensionamiento sistemático de todo cambio a implementar, en función de la información contenida en el sistema de monitorización.

5.2.5 Componentes certificados [op.pl.5]

Sistemas a los que aplica	No Aplica
Madurez evaluada	L0

Tabla 5-9. Componentes certificados. Nivel de madurez

No existen componentes certificados. Esta medida únicamente es aplicable de forma obligatoria a sistemas de nivel alto. La organización no cuenta con ningún sistema de nivel alto.

5.2.6 Control de acceso y acceso local [op.acc.1-6]

Sistemas a los que aplica	Sistema ERP, Sistema AE
Madurez evaluada	L0-L2

Tabla 5-10. Control de acceso y acceso local. Nivel de madurez

Valoración:

Los usuarios de la organización se encuentran correctamente identificados y poseen un identificador singular, mantenido por un sistema centralizado, que permite correspondencia, asignación de derechos, identificación de los derechos asignados y que es inhabilitado cuando el usuario abandona la organización.

Así mismo el sistema cuenta con un mecanismo de control de acceso global (CAS) que controla el acceso a los aplicativos y servicios desplegados en el mismo. Adicionalmente, cada aplicación cuenta con la posibilidad de otorgar privilegios y permisos delegados a los usuarios concretos de las mismas. La asignación de privilegios y permisos delegados a los usuarios de los aplicativos recae en el administrador funcional de cada una de las aplicaciones. Este administrador limita los privilegios de acceso de cada usuario a los necesarios para la ejecución de sus tareas.

En la gestión del sistema de información existe una segregación mínima entre la operación del sistema, repartida entre las unidades funcionales responsables de los aplicativos y servicios; y el desarrollo y mantenimiento del mismo, tarea de los empleados de TI. No obstante, no existe evidencia de la existencia de un rol definido de auditoría y supervisión.

El control de acceso usa, principalmente, un mecanismo de autenticación basado en contraseñas y puntualmente en certificados digitales. A este respecto existe una política de calidad de contraseñas, sin embargo, no se fuerza a los usuarios a su cumplimiento, ni a medidas de calidad como la renovación periódica de contraseñas.

Adicionalmente, la entrega de los identificadores al PAS/PDI, no garantiza el secreto de la contraseña por parte del usuario al que le ha sido entregada. No forzándose el cambio del identificador generado en el primer acceso del usuario al sistema. No se ha encontrado evidencia de la existencia de un esquema general que describa el mecanismo de control de acceso en su totalidad.

Evidencias:

A continuación se recogen imágenes del directorio LDAP de la organización:

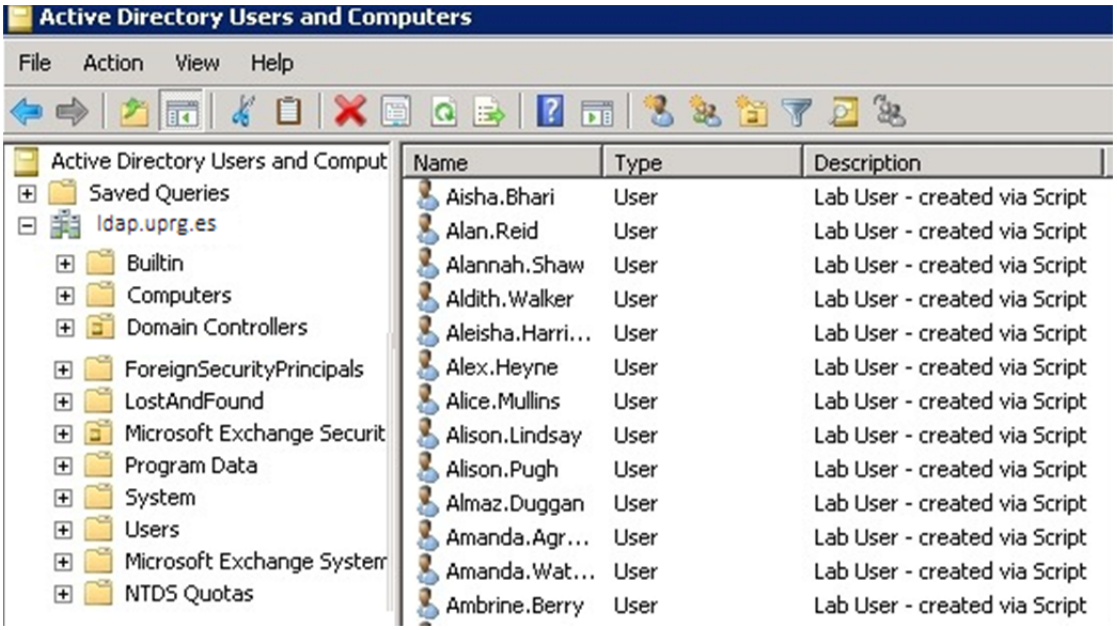

Ilustración 5-5. Usuarios de Active Directory

A partir de la información contenida en el directorio, el acceso es gestionado mediante un servicio CAS, al cual redirigen los procesos de autenticación de los aplicativos, el cual se comunica con el directorio de la organización, permitiendo la autenticación de usuarios y la asignación de derechos de acceso en función de los diferentes objectclass almacenados y de los grupos a los que pertenezca.

Ilustración 5-6. Servicio de control de acceso centralizado a los servicios

Paralelamente, los diferentes aplicativos correspondientes a cada servicio ENS (Administración Electrónica / ERP / ...) cuentan con mecanismos de delegación de privilegios. A continuación se puede ver como el software que implementa los servicios de ERP implementa un conjunto de

perfiles de acceso y cómo cada uno de los usuarios reciben diferentes privilegios de acceso al sistema de información, determinando a qué trámites tienen acceso y a qué trámites no tienen acceso.

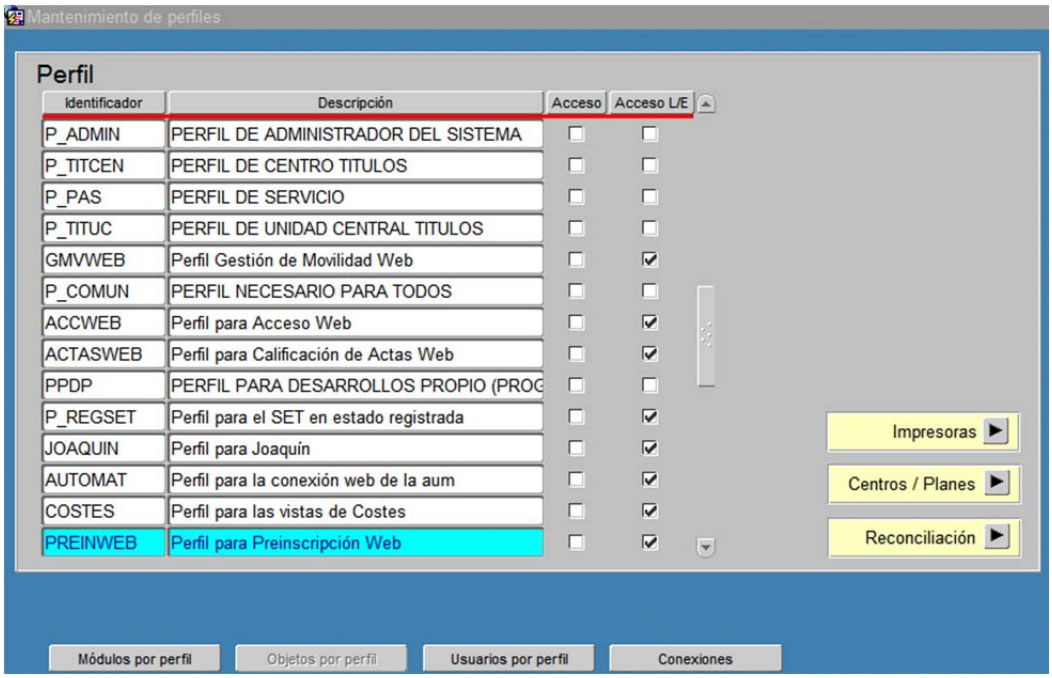

Ilustración 5-7. Perfiles de acceso en el software del sistema ERP

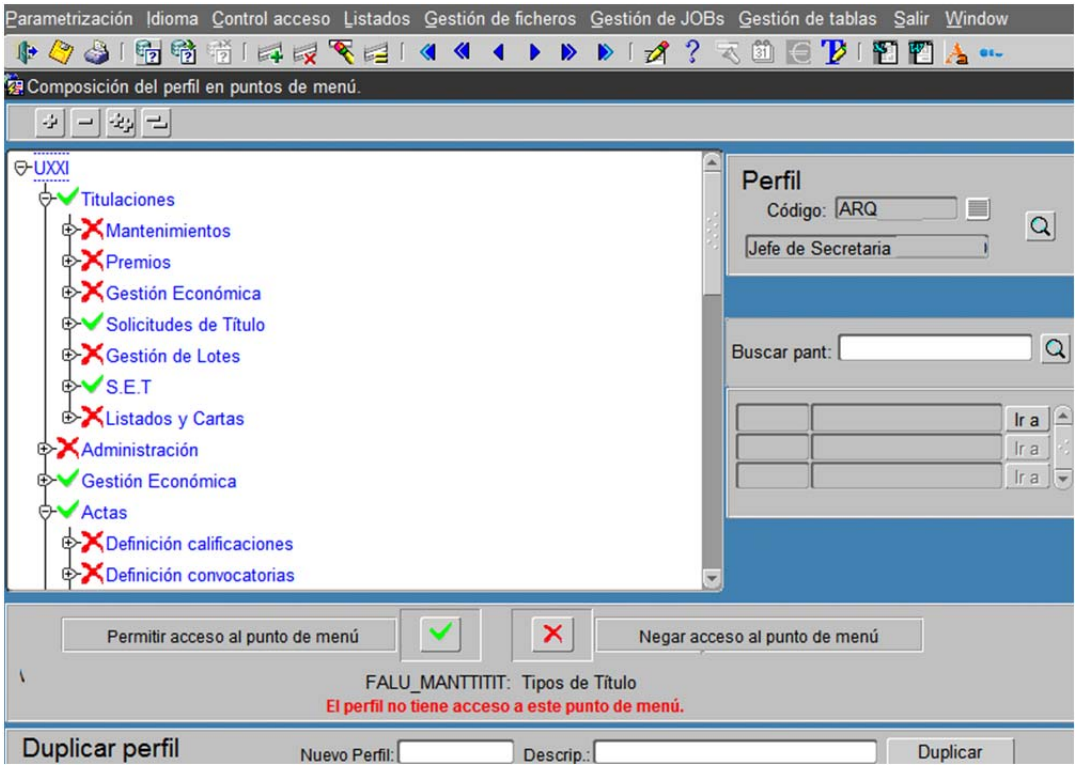

Ilustración 5-8. Acceso a trámites en función del perfil de acceso en el software del sistema ERP

De la misma forma, el aplicativo que sustenta el proceso de Administración Electrónica incluye diferentes grupos y delegaciones de privilegios tal y como se puede apreciar en las siguientes imágenes:

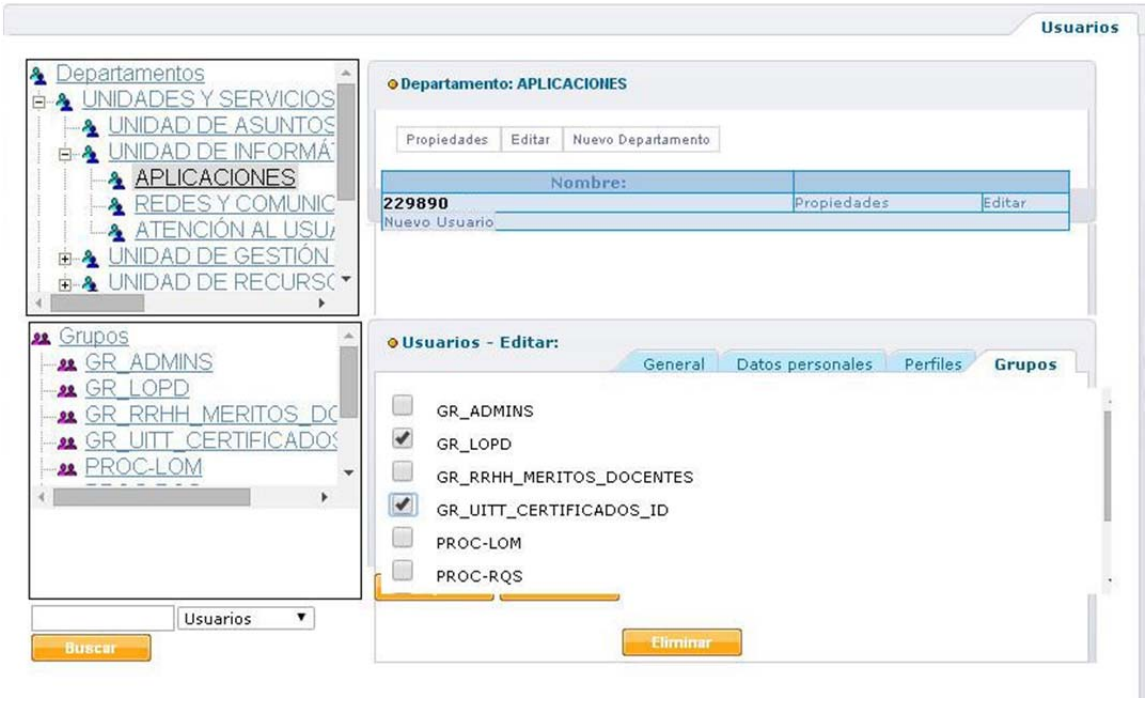

Ilustración 5-9. Grupos de usuarios en el software del sistema AE

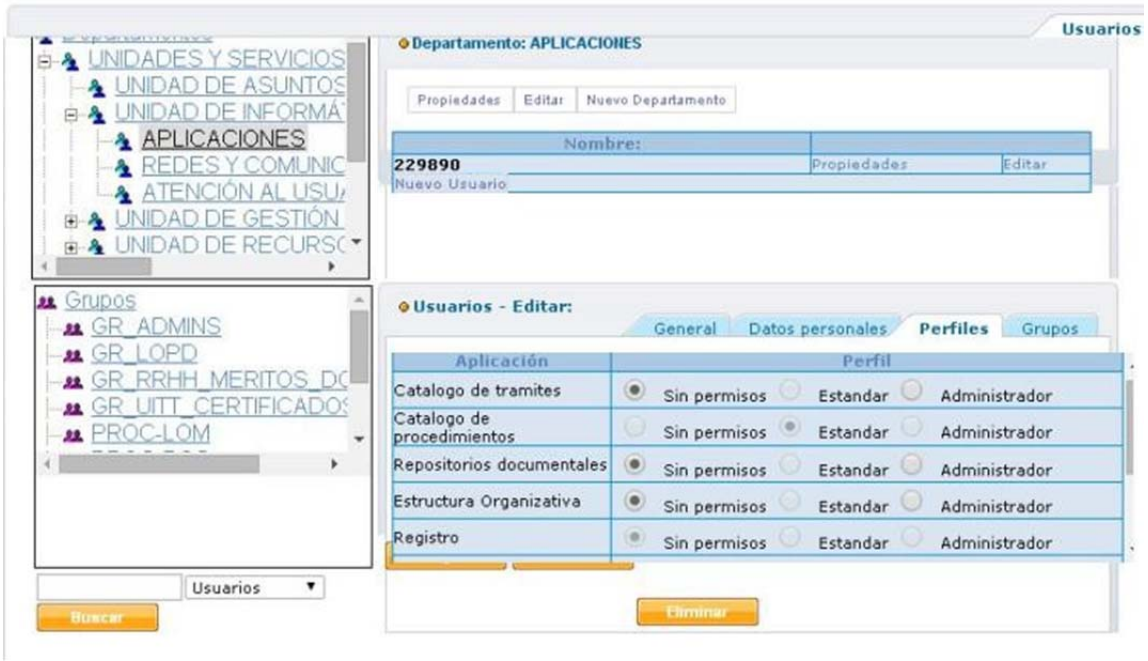

Ilustración 5-10. Perfiles de acceso en el software del sistema AE

Por contra, como se ha comentado, la política de contraseñas, aunque existe para la organización, no fuerza la existencia de unos criterios mínimos de calidad, dejando que sea el usuario el que decida qué criterios aplicar. Tampoco se establecen mecanismos de control de los ataques por

fuerza bruta ni se fuerza la expiración de contraseñas para que sea cambiada periódicamente por el usuario:

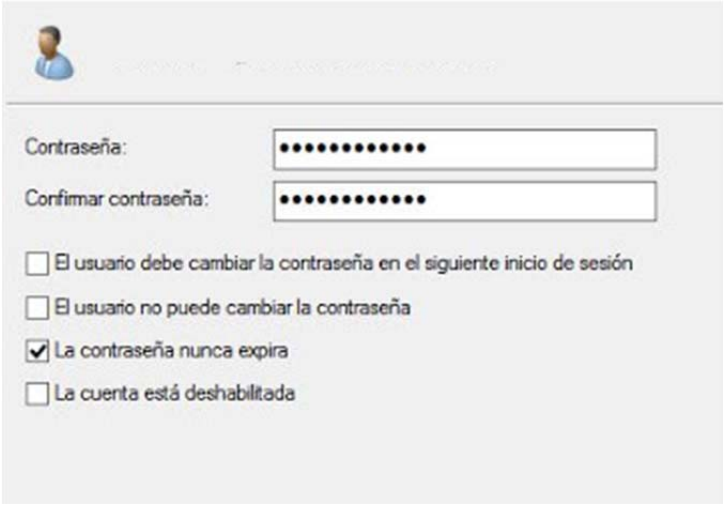

Ilustración 5-11. Política de contraseñas

A continuación, y para finalizar, se recoge la entrega de identificadores, la cual no garantiza el secreto del mismo, debido a que este es conocido por el técnico que lo entrega y no se fuerza el cambio tras el primer acceso.

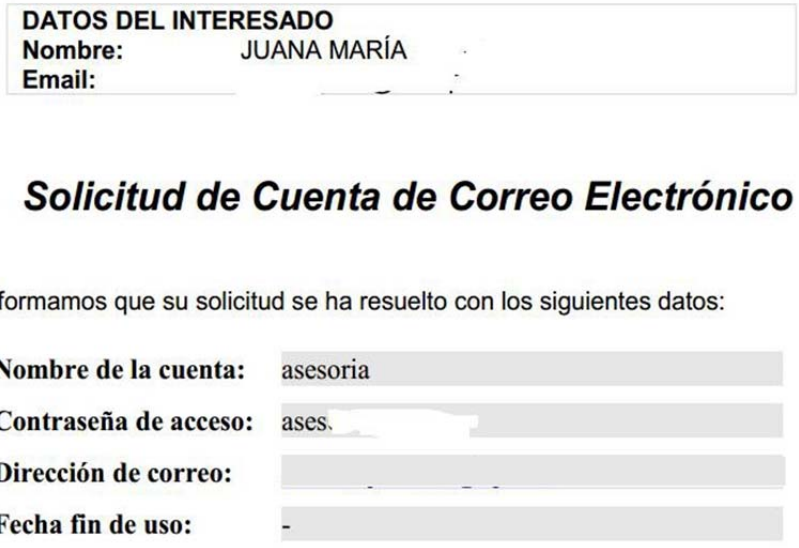

Ilustración 5-12. Documento de alta de identificador de correo para usuario

Recomendaciones:

Las recomendaciones para el proceso de autenticación se dividen en tres:

1. Implementar mecanismos de control de calidad de las contraseñas que garanticen, al menos, una longitud y complejidad mínimas.

2. Garantizar el secreto en la entrega de identificadores a los usuarios PAS/PDI.

3. Documentar el esquema de autenticación al completo, los mecanismos que participan, el proceso de alta, baja, entrega de identificadores, gestión de credenciales, ...

5.2.7 Acceso remoto [op.acc.7]

Sistemas a los que aplica	Sistema ERP, Sistema AE
Madurez evaluada	L0-L2

Tabla 5-11. Acceso remoto. Nivel de madurez

Valoración:

No existe en la organización una política de acceso remoto que explícitamente defina qué mecanismos de seguridad son aplicados a este tipo de acceso y de qué manera pueden ser accedidos los sistemas.

No obstante, implícitamente, existe una política de filtrado de red que limita la conexión a los sistemas de la organización desde el exterior y un servicio de acceso VPN, con diferentes perfiles de privilegio, que establece túneles seguros desde el exterior para los diferentes servicios que deben ser accedidos, incluyendo servicios remotos de terminal.

Evidencias:

A continuación se muestra una captura de pantalla del servicio VPN y los túneles que desde él se pueden establecer, tanto hacia servicios HTTP/HTTPS que tienen acceso filtrado desde el exterior, como hacia servicios de Escritorio Remoto o de Terminal SSH.

Ilustración 5-13. Túneles ofrecidos por el servicio VPN

Recomendaciones:

La recomendación sobre esta medida de seguridad es la creación de una política de acceso remoto que defina explícitamente lo que hasta ahora se hace de manera implícita, especificando qué servicios deben ser accedidos de esta manera, quiénes pueden acceder, qué no está permitido, etc.

5.2.8 Inventario de activos [op.exp.1]

Sistemas a los que aplica	Sistema ERP, Sistema AE
Madurez evaluada	L2

Tabla 5-12. Inventario de activos. Nivel de madurez

Valoración:

La organización dispone de un inventario del sistema de información, donde se especifica la naturaleza de cada elemento y su responsable. Existen así mismo evidencias de su actualización, a lo largo del tiempo y mantiene registro de los elementos que cursan baja en el sistema.

No obstante, el procedimiento de actualización no forma parte del ciclo del cambio del sistema de información y no se han encontrado referencias a la actualización de este inventario.

Evidencias:

List - Otro Hardware

Add card Otro Hardware

Sección	Grupo	Nombre	Tipo	Modelo	Ubica...	Fabric...	P/N	S/N	Num_Factura	Fecha_Factura	Fecha_Baja
Redes	Cámar...	Alarma1 - Ala...	Alarma								
Redes	Cámar...	Alarma2 - Ala...	Alarma								
Redes	Cámar...	Alarma3 - Ala...	Alarma								
Siste...		alteon	Balanceador	Alteon 2208	RACK...	Radw...		SSCPB803G6	1405000704	18/08/2005	01/07/2012
Siste...	Blade...	c7000	Chasis	Chasis Blade...	RACK...	HP	412152-B21	GB88393T93	3494103	11/10/2008	
Siste...	Blade...	C7000mm1	Gestión Blades	Onboard Ad...	RACK...	HP	412142-B21	O988MP0018			
Siste...	Blade...	C7000mm2	Gestión Blades	Onboard Ad...	RACK...	HP	412142-B21	O988MP3738			
Redes	Cámar...	Cámara 1 PB ...	Cámara		Murall...						
Redes	Cámar...	Cámara 2 PB ...	Cámara		Murall...						
Redes	Cámar...	Cámara 3 Ala...	Cámara		Murall...						
Redes	Cámar...	Cámara 4 Ala...	Cámara		Murall...						
Redes	Cámar...	Cámara 5 Ala...	Cámara		Murall...						
Redes	Cámar...	Cámara 7 I+D+I	Cámara		I+D+I						
Redes	Cámar...	Cámara 8 Al...	Cámara		I+D+I						
Redes	Cámar...	Cámara 9 SI -...	Cámara		I+D+I						
Redes		Controladora ...	Controladora	Colubris MSM...	CIM-C...	HP		SG9313P06F	3010977	11/12/2009	

Ilustración 5-14. CMDB de la organización

Recomendaciones:

Integrar el inventario de activos como parte de las tareas de la gestión del cambio, de tal forma que la gestión del inventario sea parte del proceso definido de gestión del cambio.

5.2.9 Configuración de seguridad [op.exp.2]

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

Tabla 5-13. Configuración de seguridad. Nivel de madurez

Valoración:

La organización no dispone de un procedimiento de fortificación y bastionado de los sistemas y elementos que componen el sistema de información.

En este sentido, la configuración de la seguridad en los sistemas no forma parte de un procedimiento estandarizado que gestione la configuración, sino que está vinculada a acciones puntuales, derivadas de pruebas o chequeos de la seguridad.

Evidencias:

Algunos sistemas cuentan con políticas de filtrado local en el host, mientras que otros sistemas carecen de ellas. A continuación se muestran las reglas del firewall local para un servidor web de cada uno de los sistemas:

```
Servidor web de sistema ERP:

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Ilustración 5-15. Reglas firewall local servidor web de sistema ERP

```
Servidor web de sistema EA:

Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTABLISHED
ACCEPT     all  --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh state NEW
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http state NEW
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:https state NEW
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:4443 state NEW
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http-alt state NEW
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:8444 state NEW
REJECT     all  --  anywhere             anywhere             reject-with icmp-port-unreachable

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Ilustración 5-16. Reglas firewall local servidor web de sistema AE

De la misma forma no se ha encontrado homogeneidad en los procesos de sistema en ejecución. Por ejemplo algunos de los procesos encontrados han sido:

```
Servidor Web de Sistema ERP

root      3558     1          0 05:00 ?  00:03:38 /usr/bin/perl /usr/bin/pandora_agent /etc/pandora
root      3706     1          0 05:00 ?  00:03:24 sendmail: accepting connections
```

Ilustración 5-17. Procesos servidor web de sistema AE

```
Servidor Web de sistema EA

root       678     1          0 06:00 ?  00:00:00 /usr/sbin/bluetoothd
whoopsie  1166     1          0 06:00 ?  00:00:00 whoopsie
```

Ilustración 5-18. Procesos servidor web de sistema AE

Recomendaciones:

Desarrollar un procedimiento de fortificación de sistemas y servicios, que defina procesos que deben ejecutarse, procesos que no deben ejecutarse, políticas de filtrado de los hosts, eliminación de usuarios por defecto, etc.

Generar hojas de revisión de la configuración por sistema y verificar que en cada despliegue, el procedimiento de fortificación es aplicado.

5.2.10 Gestión de la configuración de seguridad [op.exp.3]

Sistemas a los que aplica	Sistema ERP, Sistema AE
Madurez evaluada	L1-L2

Tabla 5-14. Gestión de la configuración de seguridad. Nivel de madurez

Valoración:

La organización cuenta con un proceso de gestión del cambio que parcialmente satisface algunas de las exigencias de la gestión de la configuración de seguridad en el sistema.

En este sentido, se requiere la aprobación y documentación de las necesidades del cambio. Sin embargo, el proceso no garantiza la ejecución de pruebas de seguridad bajo la nueva configuración.

Evidencias:

Se adjunta captura de pantalla del proceso de solicitud de cambios, en el cual se puede ver cómo el proceso cubre algunas de las exigencias de la gestión de la configuración.

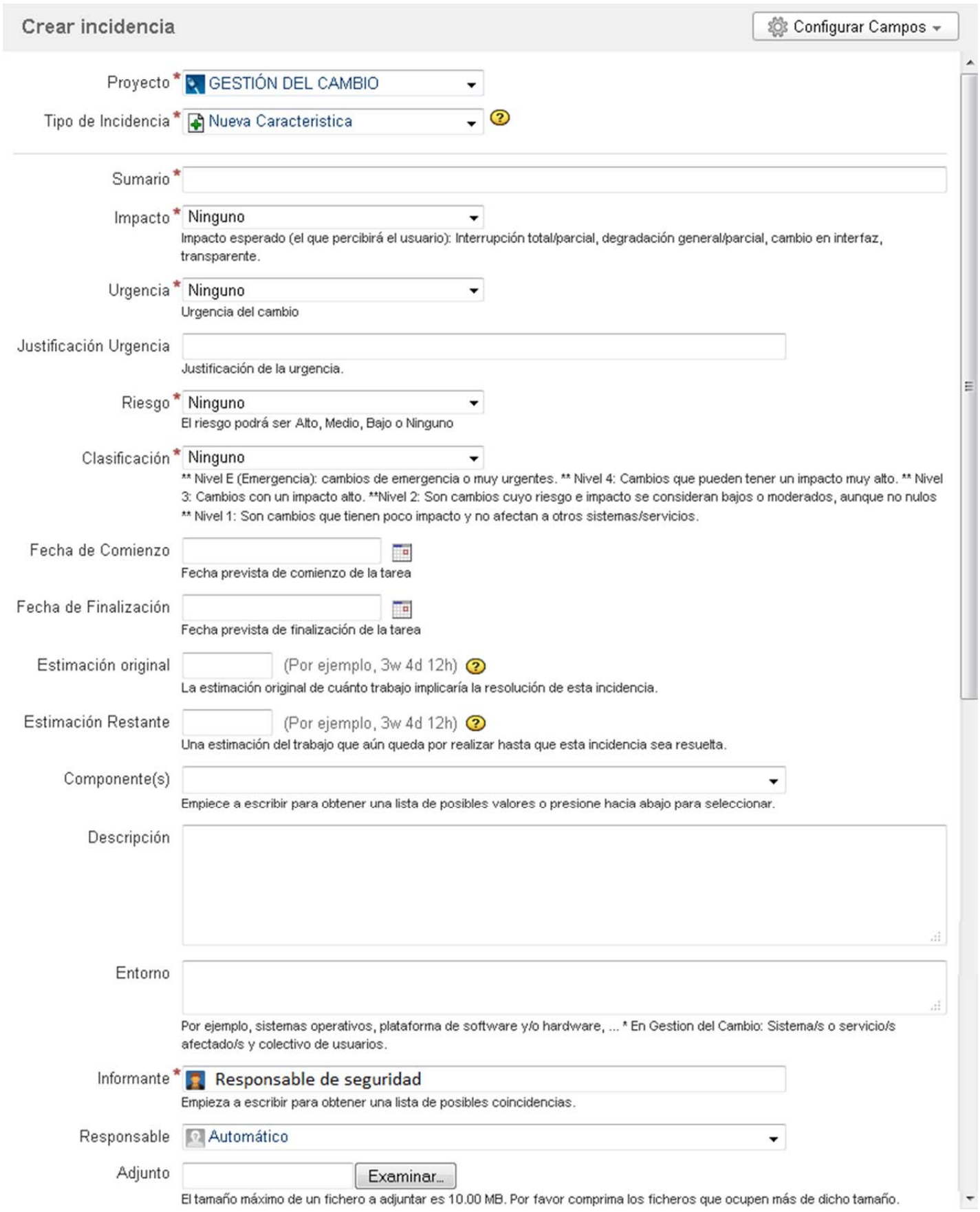

Ilustración 5-19. Formulario de solicitud de cambios

Recomendaciones:

Definir un ciclo de cambio-entrega que garantice la ejecución de pruebas y la verificación de la seguridad del nuevo entorno, así como la implementación de un plan de vuelta-atrás en caso de incidentes con la nueva configuración.

5.2.11 Mantenimiento [op.exp.4]

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

Tabla 5-15. Mantenimiento. Nivel de madurez

Valoración:

La organización no cuenta con un proceso de mantenimiento de la seguridad en el sistema de información. En este sentido no hay evidencia de que se realice un seguimiento de defectos y vulnerabilidades sobre el sistema de información, ni que estas estén siendo gestionadas de forma activa en el sistema de información.

Evidencias:

En el proceso de revisión de sistemas realizado sobre los sistemas de base de datos (nodo del clúster del servicio centralizado de bases de datos) y de uno de los servidores del sistema ERP (nodo del clúster de servidores de aplicaciones web del sistema ERP) y de uno de los servidores del sistema AE (nodo del clúster de servidores de aplicaciones web del sistema AE) no se ha encontrado evidencia de que los sistemas hayan sido actualizados en los últimos meses.

Se adjunta ejemplo de la ejecución del comando apt-get update sobre uno de los servidores del sistema AE, donde se muestra la existencia de 179 paquetes por actualizar, entre ellos algunos tan significativos como el propio núcleo del sistema, el servicio apache, el servicio ssh o los paquetes de php.

```
apt-get dist-upgrade
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Calculando la actualización... Listo
Se instalarán los siguientes paquetes NUEVOS:
  linux-headers-3.2.0-72  linux-headers-3.2.0-72-generic  linux-image-3.2.0-72-generic
Se actualizarán los siguientes paquetes:
  apache2 apache2-mpm-prefork apache2-utils apache2.2-bin apache2.2-common apparmor apport apt
apt-transport-https apt-utils base-files bash bsdutils curl dbus dbus-x11
  dh-apparmor dmidecode dpkg dpkg-dev file fonts-opensymbol gnupg gpgv grub-common grub-pc grub-
pc-bin grub2-common icedtea-6-jre-cacao icedtea-6-jre-jamvm ifupdown iproute
[..]
  python-problem-report python-uno qdbus rsyslog subversion tcpdump tzdata tzdata-java udev uno-
libs3 update-manager-core update-notifier-common ure util-linux uuid-runtime
  wget wpasupplicant
179 actualizados, 3 se instalarán, 0 para eliminar y 0 no actualizados.
```

Ilustración 5-20. Software desactualizado en servidor web del sistema AE

Recomendaciones:

Realizar un seguimiento proactivo de las recomendaciones y actualizaciones de los fabricantes, así como de sus boletines de seguridad. Gestionar estas actualizaciones dentro del proceso de gestión del cambio.

5.2.12 Gestión de cambios [op.exp.5]

Sistemas a los que aplica	Sistema ERP, Sistema AE
Madurez evaluada	L1-L2

Tabla 5-16. Gestión de cambios. Nivel de madurez

Valoración:

La organización cuenta con un proceso de gestión de cambios operativo, que valora y controla de forma continua los cambios a implementar en el sistema de información. Así mismo, la aprobación de los cambios incluye valoración del impacto sobre los servicios asociados, riesgo del cambio, etc.

No obstante, el proceso de gestión de cambios no garantiza un despliegue del cambio siguiendo criterios de buenas prácticas, ni garantizando una fase de preproducción del mismo.

Evidencias:

Se adjunta el diagrama del proceso de gestión de cambios de la organización:

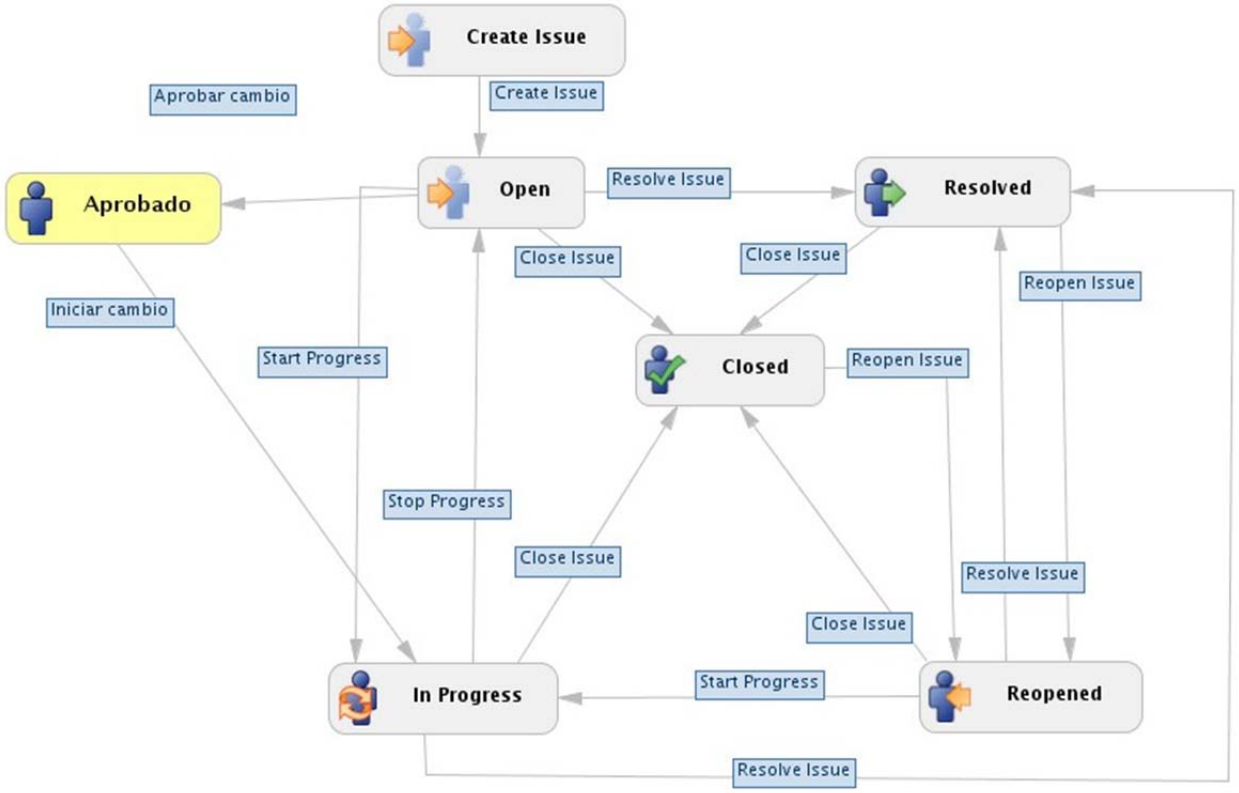

Ilustración 5-21. Diagrama del proceso de gestión de cambios

Recomendaciones:

La recomendación es ampliar el proceso de gestión de cambios incluyendo el ciclo completo de planificación, diseño, implementación, evaluación y despliegue del cambio.

También hay que añadir a la planificación del cambio los requisitos de seguridad desde el comienzo. Evaluar los requisitos implementados en la fase de evaluación (pruebas) de cada cambio.

5.2.13 Protección frente a código dañino [op.exp.6]

Sistemas a los que aplica	Sistema ERP, Sistema AE
Madurez evaluada	L1-L2

Tabla 5-17. Protección frente a código dañino. Nivel de madurez

Valoración:

La organización dispone de un servicio antivirus centralizado, con soporte por parte del fabricante, que le permite prevenir y reaccionar ante código dañino (virus, gusanos, troyanos, ...).

Este servicio de antivirus se encuentra actualizado y operativo, tiene la capacidad de emitir alertas ante situaciones de riesgo, incluye información estadística del estado de todos los clientes conectados al mismo, etc.

Sin embargo, el servicio no es universal para toda la organización y únicamente es usado de forma sistemática en los equipos del personal de administración y servicios, siendo optativa su utilización en el equipo del personal docente investigador.

Evidencias:

Se adjunta captura de pantalla del sistema antivirus utilizado como mecanismo de protección frente a código dañino en la organización.

Antivirus	Current Version	Upgraded	Not Upgraded	Upgrade Rate
Smart Scan Agent Pattern	11.315.00	326	5	98%
Virus Pattern	11.317.00	0	0	0%
IntelliTrap Pattern	0.211.00	326	5	98%
IntelliTrap Exception Pattern	1.139.00	326	5	98%
Virus Scan Engine (32-bit)	9.800.1009	273	5	98%
Virus Scan Engine (64-bit)	9.800.1009	53	0	100%
Anti-spyware	**Current Version**	**Upgraded**	**Not Upgraded**	**Upgrade Rate**
Spyware Pattern	15.69	326	5	98%
Spyware Active-monitoring Pattern	1.569.00	0	0	0%
Spyware Scan Engine (32-bit)	6.2.3030	278	0	100%
Spyware Scan Engine (64-bit)	6.2.3030	53	0	100%
Damage Cleanup Services	**Current Version**	**Upgraded**	**Not Upgraded**	**Upgrade Rate**
Virus Cleanup Template	1422	331	0	100%
Virus Cleanup Engine (32-bit)	7.1.1044	278	0	100%
Virus Cleanup Engine (64-bit)	7.1.1044	53	0	100%
Behavior Monitoring Components	**Current Version**	**Upgraded**	**Not Upgraded**	**Upgrade Rate**
Behavior Monitoring Detection Pattern (32-bit)	1.413.00	277	1	99%
Behavior Monitoring Driver (32-bit)	2.95.1170	278	0	100%
Behavior Monitoring Core Service (32-bit)	2.95.1170	278	0	100%
Behavior Monitoring Detection Pattern (64-bit)	1.413.64	53	0	100%
Behavior Monitoring Driver (64-bit)	2.95.1170	53	0	100%
Behavior Monitoring Core Service (64-bit)	2.95.1170	53	0	100%
Behavior Monitoring Configuration Pattern	1.234.00	331	0	100%
Policy Enforcement Pattern	1.215.00	331	0	100%
Digital Signature Pattern	1.416.00	331	0	100%
Program	**Current Version**	**Upgraded**	**Not Upgraded**	**Upgrade Rate**
OfficeScan Client (32-bit)	10.6.3205	278	0	100%
OfficeScan Client (64-bit)	10.6.3205	53	0	100%
Cisco Trust Agent	2.1.103	0	0	0%

Ilustración 5-22. Sistema antivirus de protección frente a código dañino

Recomendaciónes:

Incluir en la normativa de seguridad el requisito de instalar el cliente de antivirus en todos los ordenadores y dispositivos móviles electrónicos de la organización para todos los miembros de la misma

5.2.14 Gestión de incidencias de seguridad y su registro [op.exp.7/9]

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

Tabla 5-18. Gestión de incidencias de seguridad y su registro. Nivel de madurez

Valoración:

No existe un proceso de gestión de incidencias de seguridad en la organización, ni información sobre los mismos. Tampoco parece existir capacidad operativa para afrontar la investigación de incidentes de seguridad, por limitaciones de personal y por falta de formación del personal.

No existe un sistema como tal para el registro de incidentes relacionados con la seguridad de los sistemas.

Recomendaciónes:

Implementar un proceso de gestión de incidentes de seguridad que permita el reporte y la investigación de esta tipología de incidente, permitiendo el esclarecimiento de los hechos acontecidos y el desarrollo de medidas preventivas.

5.2.15 Registros de actividad de los usuarios y protección de los mismos [op.exp.8/10]

Sistemas a los que aplica	No Aplica
Madurez evaluada	L0-L1

Tabla 5-19. Registros de actividad de los usuarios y protección de los mismos. Nivel de madurez

El registro de la actividad de los usuarios se hace aleatoriamente en algunas de las aplicaciones y puntualmente se configuran algunos de ellos pero siempre de forma extraoficial y no coordinada. Estas medidas son únicamente aplicables a sistemas de nivel alto. La organización no cuenta con ningún sistema de nivel alto.

5.2.16 Claves criptográficas [op.exp.11]

Sistemas a los que aplica	Sistema ERP, Sistema AE
Madurez evaluada	L1-L2

Tabla 5-20. Claves criptográficas. Nivel de madurez

Valoración:

La organización no genera claves criptográficas para identificación personal de usuarios, siendo de aplicación la utilización de las claves criptográficas contenidas en el DNI electrónico, o la utilización de certificados digitales emitidos por entidades de certificación reconocidas. Sobre estas últimas no existe una normativa / recomendación de protección de las mismas de cara a los usuarios.

Por última la organización utiliza entidades de confianza para la generación de certificados digitales para los servicios de red que lo requieren en el sistema de información. No existe un procedimiento detallado que describa los pasos a aplicar en cada circunstancia: generación de los ficheros CSR / KEY del certificado, proceso de firma del certificado por parte de una entidad de confianza, procedimiento de custodia de las claves privadas, etc.

Evidencias:

Como muestra de las insuficiencias en la gestión de claves criptográficas en el servicio de información, se muestran las claves activas en el sistema de tramitación electrónica en el cual se puede observar cómo los permisos del certificado permiten la lectura del mismo por parte de cualquier usuario del sistema.

```
-rw-r--r-- 1 root root 1631 jul 15 07:43 srvwebeadm1.uprg.es2016.pem
-rw-r--r-- 1 root root 1704 jul 15 07:43 srvwebeadm1.uprg.es2016.key
```

Ilustración 5-23. Certificados para servidor web del sistema de AE

Recomendaciones:

Se recomienda crear un procedimiento de gestión de claves privadas, solicitudes de firma de certificados y certificados, que incluya el proceso de generación, la custodia en explotación y la retirada de explotación.

Este procedimiento deberá ser aplicado a la gestión de las claves existentes, así como a las que se generen en un futuro. De especial relevancia es la seguridad de las claves en uso, garantizando que los privilegios de acceso al mismo son los correctos. En el caso de sistemas operativos actuales, no se debe permitir el acceso en modo lectura a la clave del certificado para cualquier usuario, limitando la lectura al grupo ssl-cert en aquellos sistemas que se implemente y si no, exclusivamente, al usuario administrador root.

5.2.17 Contratación y acuerdos de nivel de servicio [op.ext.1]

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

Tabla 5-21. Contratación y acuerdos de nivel de servicio. Nivel de madurez

Valoración:

La organización mantiene acuerdos de servicio con sus proveedores y estos acuerdos detallan las características de los servicios, los términos del nivel de servicio prestado, así como las responsabilidades de las partes. En este sentido se han evaluado los acuerdos que la organización mantiene con sus principales proveedores de servicio.

Evidencias:

Se adjuntan los puntos generales del acuerdo de nivel de servicio que la organización mantiene con su principal proveedor de servicio.

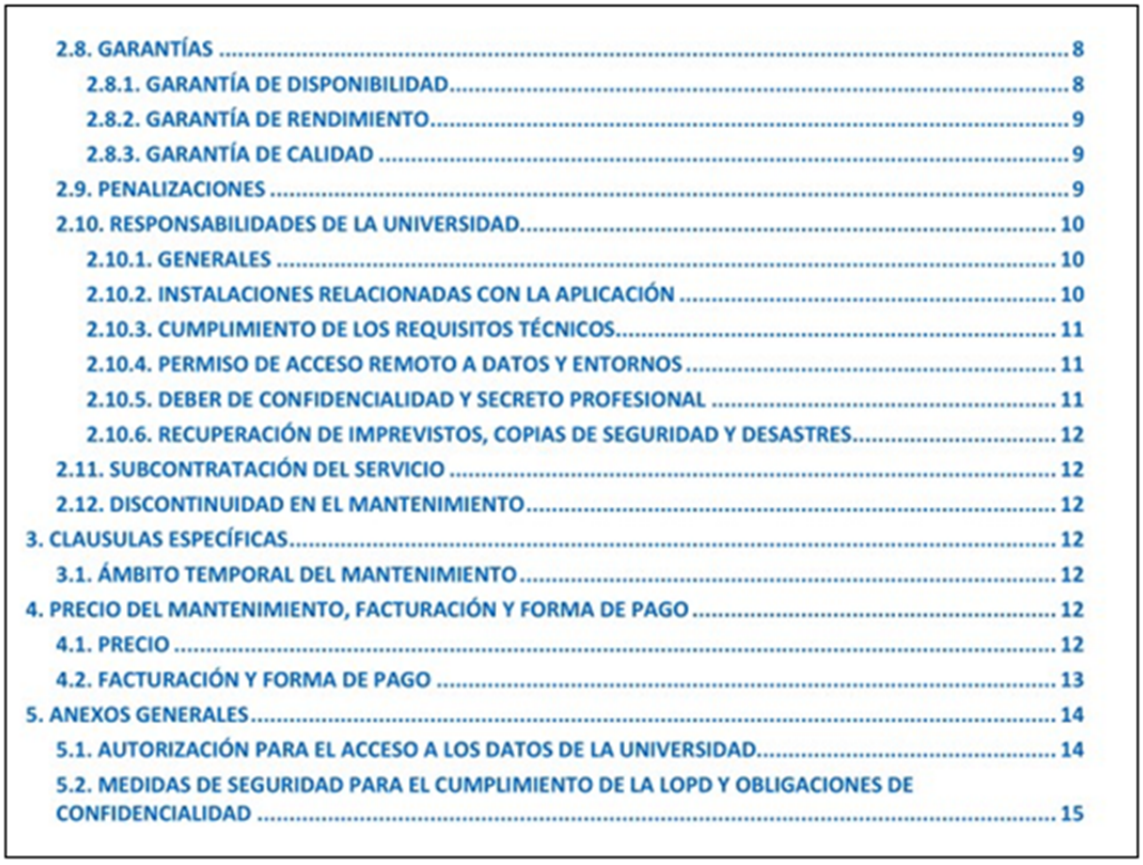

Ilustración 5-24. Puntos del acuerdo de nivel de servicio con principal proveedor de servicios

Recomendaciones:

No existen actividades correctivas en esta medida.

5.2.18 Gestión diaria [op.ext.2]

Sistemas a los que aplica	Sistema ERP, Sistema AE
Madurez evaluada	L0-L1

Tabla 5-22. Gestión diaria. Nivel de madurez

Valoración:

Existen unos mecanismos mínimos para el control diario de la actividad realizada por los proveedores de servicio, mediante el uso de sistemas de gestión de tickets y gestión de la operativa de proyectos.

No obstante, esta gestión está más enfocada al control del desempeño y al desarrollo de las funciones especificadas en el contrato, que a la posible gestión de la seguridad en las actuaciones. En este sentido no existe un mecanismo uniforme de coordinación con los proveedores para afrontar posibles incidentes de seguridad o desastres que pudiesen darse en la prestación de sus servicios.

Recomendaciones:

Incluir la gestión de la seguridad en los acuerdos de nivel de servicio con los proveedores, definiendo mecanismos para gestionar incidentes de seguridad o desastres que pudiesen acontecer, así como para garantizar que la seguridad se mantiene en los sistemas gestionados por terceros.

5.2.19 Medios alternativos [op.ext.9]

Sistemas a los que aplica	No Aplica
Madurez evaluada	L0

Tabla 5-23. Externalización: Medios alternativos. Nivel de madurez

No existen contratados medios alternativos en la externalización. Estas medidas son únicamente es aplicable de forma obligatoria a sistemas de nivel alto. La organización no cuenta con ningún sistema de nivel alto.

5.2.20 Análisis de impacto [op.cont.1]

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

Tabla 5-24. Análisis de impacto. Nivel de madurez

Valoración:

No existe un proceso de gestión que ejecute análisis de impacto sobre la continuidad de los servicios, ni los mantenga en el tiempo. Sólo como parte del análisis de riesgos se valora la disponibilidad de los servicios.

Los requisitos de disponibilidad de cada servicio están identificados de forma general, pero no se evalúan los elementos que son críticos para la prestación de dicho servicio, ni se entra a valorar la idoneidad de los mismos respecto a su misión.

Evidencias:

Se adjunta la valoración de disponibilidad del servicio de “Gestión Académica”

Servicio de Gestión Académica	Nivel	Motivo
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.

Tabla 5-25. Valoración de disponibilidad del servicio de Gestión Académica

Recomendaciones:

Implementar un proceso de análisis de impacto, asociado al proceso de gestión de cambios y análisis de riesgos.

5.2.21 Plan de continuidad [op.cont.2]

Sistemas a los que aplica	No Aplica
Madurez evaluada	L0

Tabla 5-26. Plan de continuidad. Nivel de madurez

No existe un plan de continuidad. Esta medida únicamente es aplicable de forma obligatoria a sistemas de nivel alto. La organización no cuenta con ningún sistema de nivel alto.

5.2.22 Pruebas periódicas [op.cont.3]

Sistemas a los que aplica	No Aplica
Madurez evaluada	L0

Tabla 5-27. Pruebas periódicas. Nivel de madurez

No se realizan pruebas periódicas de restauración de los servicios. Esta medida únicamente es aplicable de forma obligatoria a sistemas de nivel alto. La organización no cuenta con ningún sistema de nivel alto.

5.2.23 Detección de intrusión [op.mon.1]

Sistemas a los que aplica	Sistema ERP, Sistema AE
Madurez evaluada	L2

Tabla 5-28. Detección de intrusión. Nivel de madurez

Valoración:

Existe un sistema de detección de intrusiones (IDS) permite alertar en caso de detectar posibles patrones de ataque. Esta funcionalidad se encuentra implementada en el firewall perimetral aunque no existe evidencia de que esta funcionalidad esté siendo actualmente aprovechada.

Evidencias:

Captura del sistema de firewall perimetral, el cual incluye mecanismos IDS

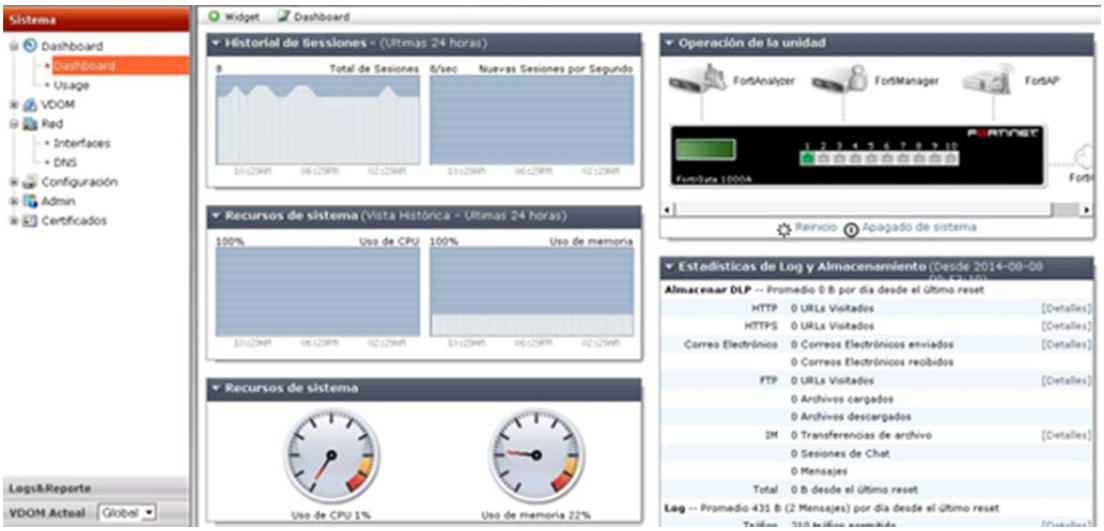

Ilustración 5-25. Menú de gestión de firewall perimetral

Recomendaciones:

Definir un método de actuación en base a la detección de intrusiones usando el sistema IDS del firewall.

5.2.24 Sistema de Métricas [op.mon.2]

Sistemas a los que aplica	No Aplica
Madurez evaluada	L0-L3

Tabla 5-29. Gestión de cambios. Nivel de madurez

Valoración:

La organización tiene definido un sistema de métricas e indicadores a nivel técnico en los servidores que permite mandar alertas en caso de que se sobrepasen unos valores preestablecidos en cuanto a uso de memoria, uso de CPU, carga de red , etc… No obstante las métricas e indicadores contemplados en esta medida se refieren a los aspectos de:

- Grado de implantación de las medidas de seguridad. La organización emplea un modelo de tipo CMM para evaluar el grado de madurez de las medidas establecido por Magerit

- Eficacia y eficiencia de las medidas. Se carece de métricas e indicadores para valorar la eficacia de una medida en relación a su coste

- Impacto de los incidentes de seguridad. Para clasificar el impacto de los incidentes de seguridad se sigue el modelo del grado de degradación del activo sugerido por la Guía del CCN titulada “CCN-STIC 803. Esquema Nacional de Seguridad Valoración de los sistemas”.

Esta medida únicamente es aplicable de forma obligatoria a sistemas de nivel alto. La organización no cuenta con ningún sistema de nivel alto.

Evidencias:

Indicadores definidos para determinar el grado de implantación de las medidas de seguridad:

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

Tabla 5-30.Escala de niveles de madurez de Salvaguardas en PILAR

Indicadores en relación al grado de degradación del valor del activo:

Degradación del valor del activo
5% --> Degradación Baja
30% --> Degradación Media
50% --> Degradación Alta
80% --> Degradación Muy Alta
100% --> Completa

Ilustración 5-26. Degradación del valor del activo

Recomendaciones:

Definir métricas que permitan evaluar la relación entre el coste de implantar una medida de seguridad y su eficacia.

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 5-27. Control de acceso a salas mediante tarjeta RF

En el interior de las salas los equipos se presentan distribuidos en rack y etiquetados.

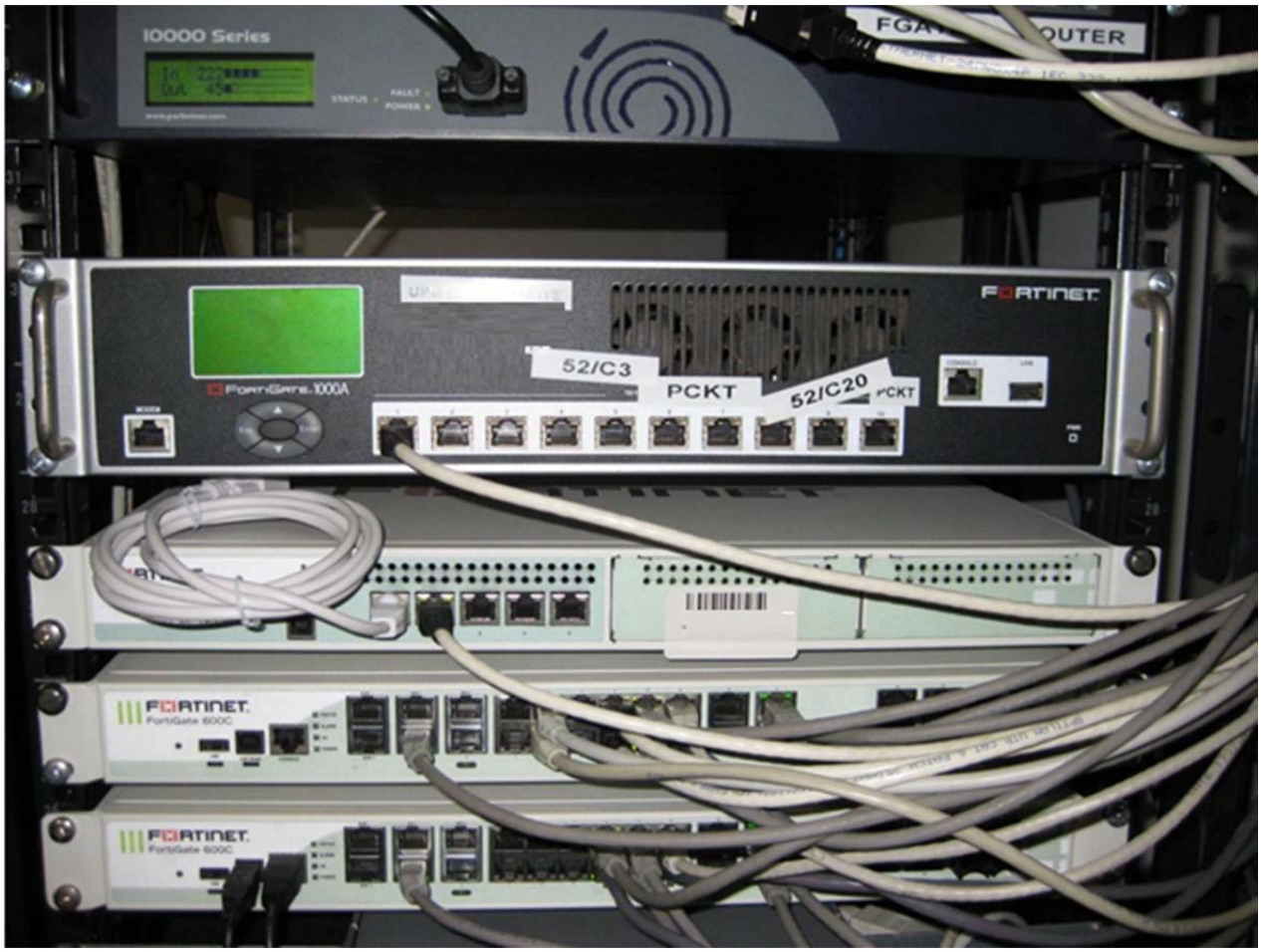

Ilustración 5-28.Detalle rack de sala de comunicaciones

Así mismo las salas cuentan con sistema de refrigeración dedicado, adicional al del edificio, para mantener las adecuadas condiciones de temperatura y humedad.

Ilustración 5-29. Medida de temperatura en sala de servidores

Como aspecto a corregir se encuentra la existencia de material, incluyendo embalajes de cartón, en el interior de las salas de equipos.

Ilustración 5-30. Detalle de embalajes de cartón en sala de comunicaciones

Recomendaciones:

Se recomienda reubicar el material ajeno a las salas del CPD, especialmente los embalajes de cartón, debido a su potencial inflamable.

5.3.2 Energía eléctrica [mp.if.4]

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

Tabla 5-31. Energía eléctrica. Nivel de madurez

Valoración:

La organización cuenta con una acometida eléctrica dimensionada para las salas del centro de proceso de datos, dicha acometida se respalda además con un sistema de alimentación ininterrumpido que garantiza el correcto apagado del sistema en caso de fallo eléctrico.

Evidencias:

Se adjunta captura de la entrada del suministro eléctrico a una de las salas del centro de proceso de datos.

Ilustración 5-31. Detalle de suministro eléctrico en CPD

Recomendaciones:

No existen acciones correctivas; las medidas instaladas se consideran suficientes para el nivel del sistema.

5.3.3 Protección frente a incendios [mp.if.5]

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

Tabla 5-32. Protección frente a incendios. Nivel de madurez

Valoración:

La organización cuenta con medidas contraincendios en ambas salas. En la sala de servidores existen mecanismos de detección de incendios, así como mecanismos de extinción manuales. En la sala de comunicaciones existen mecanismos automáticos de detección y extinción de incendios con un sistema autónomo mediante Heptafluoropropano (HFC-227ea). Así mismo, las salas cuentan con luces de emergencia.

Evidencias:

Se adjuntan imágenes de las sondas de detección de humo y los extintores de la sala de servidores:.

Ilustración 5-32. Detector de humo en sala de servidores

Ilustración 5-33. Extintor en sala de servidores

En el caso de la sala de comunicaciones se adjunta imagen del sistema autónomo de extinción HFC-227ea.

Ilustración 5-35. Sistema de extinción sala de comunicaciones

Ilustración 5-34. Detalle sistema de extinción

Finalmente, se adjunta captura de las luces de emergencia de las salas.

Ilustración 5-36. Luz de emergencia en salas

Recomendaciones:

El actual mecanismo de extinción es adecuado para el nivel del sistema de información. No obstante, como recomendación adicional, se sugiere extender el mecanismo automatizado de extinción a ambas salas.

5.3.4 Protección frente a inundaciones [mp.if.6]

Sistemas a los que aplica	Sistema AE
Madurez evaluada	L0-L2

Tabla 5-33. Protección frente a inundaciones. Nivel de madurez

Valoración:

La organización no cuenta con adecuados mecanismos de protección frente a las inundaciones. El diseño de las actuales salas incluye desagües y tuberías sobre los techos de ambas.

Adicionalmente, únicamente la sala de servidores cuenta con un suelo sobre- elevado, que permitiría una mayor protección en caso de inundación.

Evidencias:

Se adjunta captura de tuberías de desagüe que cruzan sobre las salas.

Ilustración 5-37. Detalle tuberías de desagüe

También se adjunta imagen del suelo sobre-elevado, medida de protección bastante eficaz ante inundaciones y que está presente en la sala de servidores, pero no en la sala de los nodos de comunicación.

Ilustración 5-38. Detalle suelo sobre-elevado en sala de servidores

Recomendaciones:

Se recomienda la instalación de suelo sobre-elevado en la sala del nodo de comunicaciones.

5.3.5 Registro E/S de equipamiento [mp.if.7]

Sistemas a los que aplica	Sistema ERP, Sistema AE
Madurez evaluada	L0

Tabla 5-34. Registro de E/S de equipamiento. Nivel de madurez

Valoración:

No existe un registro de salida de equipamiento de las salas de servidores o del nodo de comunicaciones.

Recomendaciones:

Se recomienda implantar un registro de E/S o, en su defecto, declarar la medida como no asumible, especificar los motivos por los que se rechaza su aplicación y detallar que contramedidas se aplican, si existen.

5.3.6 Instalaciones alternativas [op.if.9]

Sistemas a los que aplica	No Aplica
Madurez evaluada	L0

Tabla 5-35. Instalaciones alternativas. Nivel de madurez

No existen instalaciones físicas alternativas. Esta medida únicamente es aplicable de forma obligatoria a sistemas de nivel alto. La organización no cuenta con ningún sistema de nivel alto.

5.3.7 Caracterización, deberes y obligaciones [mp.per.1-2]

Sistemas a los que aplica	Sistema ERP, Sistema AE
Madurez evaluada	L1-L2

Tabla 5-36. Caracterización, deberes y obligaciones. Nivel de madurez

Valoración:

La organización no cuenta con una caracterización explícita de los puestos de trabajo, ni existen unos acuerdos individualizados de confidencialidad con los miembros de la misma, como sería exigible según el nivel del sistema.

Tampoco existe una normativa general que defina los requisitos de confidencialidad globales de la organización. Únicamente para trabajadores incluidos en el estatuto básico del Empleado Público, en su capítulo VI, artículo 52 se recoge el código de conducta de estos, haciendo referencia al principio de confidencialidad que debe regir su función.

Evidencias:

En entrevista personal a 10 trabajadores de la organización, 7 de ellos Personal de Administración y Servicios, y 3 de ellos Personal docente investigador, se evidencia que el 50% de los entrevistados admite que formalmente desconoce los requisitos de confidencialidad de su puesto.

	Los conoce formalmente	No los conoce formalmente
Requisitos Confidencialidad - PAS	4	3
Requisitos Confidencialidad - PDI	1	2

Tabla 5-37. Conocimiento por los empleados de los requisitos de confidencialidad de su puesto.

Recomendaciones:

Sería muy recomendable que, al menos, exista una norma que regule los requisitos de confidencialidad de los distintos perfiles que forman la organización y que esta sea difundida y conocida.

5.3.8 Concienciación [mp.per.3]

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

Tabla 5-38. Concienciación. Nivel de madurez

Valoración:

No existe un plan de concienciación del personal sistematizado en la organización. Únicamente existen acciones puntuales por parte de la Unidad de TI, pero tampoco están integradas en un conjunto de actuaciones sistemáticas y planificadas.

Evidencias:

En entrevista personal a 10 trabajadores de la organización, 7 de ellos Personal de Administración y Servicios, y 3 de ellos Personal docente investigador, se evidencia que ninguno de los entrevistados presenta una concienciación alta en materia de seguridad de la información.

Las cuestiones han girado en torno a la utilización de cifrado para proteger su información, la longitud de sus contraseñas, la periodicidad con la que se cambian, el conocimiento de la normativa de seguridad de la entidad, el conocimiento de la política de seguridad, el conocimiento del ENS, el conocimiento y uso de certificados digitales, etc.

	Conocimiento Alto	Conocimiento Medio	Conocimiento Bajo
Concienciación - PAS	0	5	2
Concienciación - PDI	0	2	1

Tabla 5-39. Nivel de concienciación de los usuarios en materia de seguridad de la información

Recomendaciones:

Se recomienda la organización de un plan de concienciación para todo el personal de la organización. La concienciación debería mezclar la concienciación telemática mediante el envío de píldoras informativas (twitter, correo electrónico, ...), con la organización de pequeños talleres y jornadas a lo largo del año, centradas en actividades eminentemente prácticas: cifrado de dispositivos móviles, medidas de protección en ficheros almacenados en dropbox y similares, contraseñas usables, etc.

5.3.9 Formación [mp.per.4]

Sistemas a los que aplica	Sistema ERP, Sistema AE
Madurez evaluada	L0-L2

Tabla 5-40. Formación. Nivel de madurez

Valoración:

No existe un plan de formación en materia de seguridad de la información del personal de la Unidad de TI. Únicamente existen acciones puntuales por parte del personal de TI, en función de necesidades concretas.

Evidencias:

Cursos impartidos en por el personal de TI desde el año 2014:

- Esquema Nacional de Seguridad y Gestión de Riesgos (Nov-2014, 25 horas)
- Desarrollo de Aplicaciones con SPRING (Nov-2014, 25 horas)
- Firma Electrónica (Mar-2015, 30 horas)
- Desarrollo de Aplicaciones (Abr-2015, 10 horas)
- Administración de sistemas Linux (May-2016, 25 horas)

De estos cursos, únicamente en el curso "Esquema Nacional de Seguridad y Gestión de Riesgos" y en "Desarrollo de Aplicaciones - iSUITE" existe contenido específico en materia de seguridad de la información.

Recomendaciones:

Implantar un plan de formación que explícitamente cubra los requisitos en materia de seguridad de la información deseables por el personal de TI.

5.3.10 Personal alternativo [op.per.9]

Sistemas a los que aplica	No Aplica
Madurez evaluada	L0

Tabla 5-41. Personal alternativo. Nivel de madurez

No existe personal alternativo. Esta medida únicamente es aplicable de forma obligatoria a sistemas de nivel alto. La organización no cuenta con ningún sistema de nivel alto.

5.3.11 Puesto de trabajo despejado [mp.eq.1]

Sistemas a los que aplica	Sistema ERP, Sistema AE
Madurez evaluada	L1-L2

Tabla 5-42. Puesto de trabajo despejado. Nivel d emadurez

La gran mayoría de empleados no llevan a cabo un control sobre el tipo de documentos que se encuentran en su puesto en función al tipo de información que contienen. Además en muchos casos dichos documentos son dejados sobre el escritorio para seguir trabajando al día siguiente en los mismos. más allá de la aplicación o no de medidas concretas, una falta clara de homogeneidad en las medidas de protección quedando a criterio del usuario su aplicación o no.

Un total de 7 entrevistas anónimas han sido realizadas a diferentes perfiles de PAS y PDI:

Empleados	Puesto de trabajo despejado
PAS	0/5
PDI	1/2

Tabla 5-43. Uso de medidas de protección de seguridad en equipos de escritorio

De las 7 personas entrevistadas, 2 PDI y 5 PAS solamente uno de los PDI reconoce etener despejado su puesto al terminar su jornada guardando la documentación relativa a exámenes e investigaciones en cajones protegidos por llave.

Recomendaciones:

Por su impacto en la seguridad global del sistema de información se recomienda concienciar al usuario en la necesidad de recoger el puesto de trabajo una vez finalizada su jornada poniendo especial atención a los documentos que tengan información sensible y que deberán ser almacenados en cajones o espacios protegidos con algún tipo de control de acceso.

5.3.12 Bloqueo puesto de trabajo. Protección de equipos portátiles [mp.eq.2-3]

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

Tabla 5-44. Bloqueo del puesto de trabajo. Protección de equipos portátiles. Nivel de madurez

Valoración:

No existe una política homogénea de protección de los equipos del usuario, ni de sus equipos portátiles, ni de la información gestionada por estos. El usuario con perfil PAS está integrado dentro de un dominio corporativo, pero no se aplican políticas de seguridad de dominio sobre el equipo, siendo el usuario administrador del equipo y pudiendo, en consecuencia, habilitar y deshabilitar cualquier medida de seguridad. El usuario con perfil PDI no está integrado dentro del dominio corporativo y cuenta con total autonomía para la gestión de su equipo de usuario.

Evidencias:

Durante el proceso de auditoría un total de 10 entrevistas anónimas han sido realizadas a diferentes perfiles de PAS y PDI.

Respecto a las medidas de protección de los equipos de Escritorio, se evidencia más allá de la aplicación o no de medidas concretas, una falta clara de homogeneidad en las medidas de protección quedando a criterio del usuario su aplicación o no.

Escritorio	Sin actualizar	Sin antivirus	Sin firewall	Sin cifrado	Sin bloqueo
PAS	4/7	1/7	5/7	7/7	3/7
PDI	0/3	2/3	0/3	3/3	0/3

Tabla 5-45. Uso de medidas de protección de seguridad en equipos de escritorio

De las 10 personas entrevistadas, 2 PDI y 1 PAS hacen uso de un equipo adicional "móvil" a su equipo de Escritorio, bien sea mediante Tableta, Móvil o Portátil. Se vuelve a evidenciar disparidad de políticas y la ausencia de políticas de cifrado en dispositivos móviles, fundamentales para garantizar la seguridad de la información contenida en ellos ante robo o pérdida.

Móvil / Tableta / Portátil	Sin Bloqueo	Sin Cifrado
PAS	1/1	1/1
PDI	0/2	2/2

Tabla 5-46. Uso de medidas de protección de seguridad en equipos móviles

Finalmente, ante la proliferación del uso de tecnologías como Dropbox o Google Drive para el almacenamiento de ficheros en el ámbito laboral, se ha preguntado por el uso de estas tecnologías para almacenaje de información de la organización.

Uso Ficheros "Nube"	Uso de Dropbox / Google Drive
PAS	2/7
PDI	2/3

Tabla 5-47. Uso de almacenamiento en la nube.

Recomendaciones:

Se recomienda, por su significativo impacto en la seguridad global del sistema de información, la homogeneización de medidas de protección en los equipos de usuario y en los equipos portátiles. Sería muy recomendable la actualización de políticas globales de dominio para la actualización de equipos, configuración de firewalls, estado de antivirus y similares tareas administrativas.

De igual forma es necesaria la concienciación en materia de protección de equipos portátiles y de la necesidad de cifrar la información que estos contienen. Finalmente, se recomienda una política uniforme sobre el uso de tecnologías de almacenamiento en la nube y la información corporativa que en ellas puede ser almacenada.

5.3.13 Equipos: medios alternativos [mp.eq.9]

Sistemas a los que aplica	Sistema AE
Madurez evaluada	L0

Tabla 5-48. Equipos: medios alternativos. Nivel de madurez

No se cuenta con equipamiento alternativo para llevar a cabo las tareas habituales en caso de que falle el equipamiento actual. Es cierto que algunos empleados cuentan con un equipo portátil proporcionado por la organización pero su existencia atiende más a criterios de comodidad y movilidad de los propios usuarios que a criterios de continuidad de los procesos de la organización que dan soporte a los servicios. De hecho mucho de los portátiles con los que cuentan algunos empleados carecen del software instalado en sus equipos de escritorio con el que realizan las tareas diarias.

Recomendaciones:

Se recomienda contar con equipos alternativos para el acceso a los servicios de AE. No obstante estará sujeto a la disponibilidad presupuestaria.

5.3.14 Perímetro seguro. Protección de la confidencialidad, integridad y la autenticidad [mp.com.1-3]

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

Tabla 5-49. Perímetro seguro. Protección de la la confidencialidad, integridad y autenticidad

Valoración:

La organización cuenta con las medidas de protección exigibles para su nivel de seguridad: ofrece protección del perímetro mediante un firewall perimetral y aplica la utilización de redes privadas virtuales en el acceso a los recursos internos desde el exterior.

Evidencias:

A continuación se adjunta captura de pantalla del firewall perimetral de la organización:

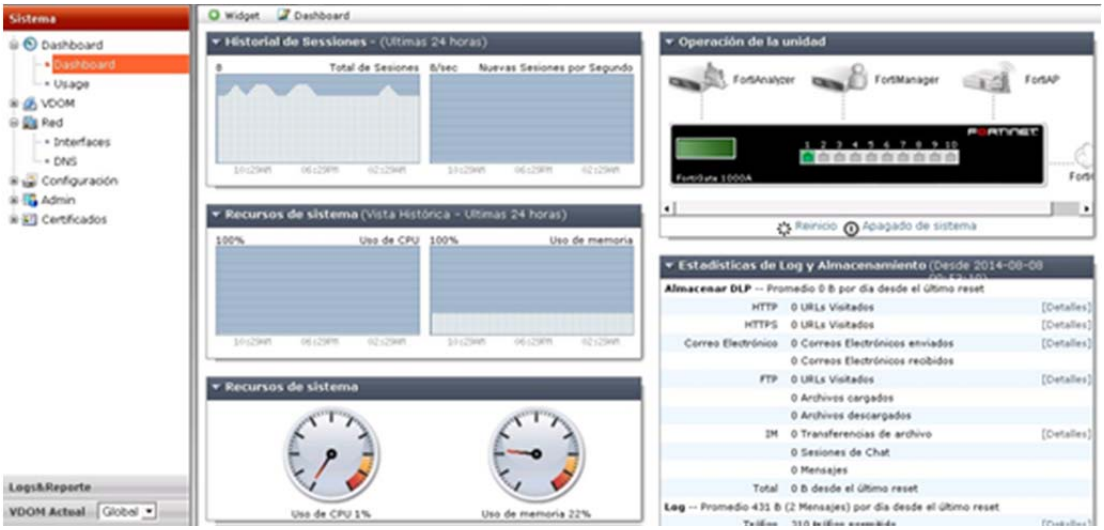

Ilustración 5-39. Menú de gestión de firewall perimetral

A continuación se adjunta captura del servicio de acceso remoto VPN de la organización, con los diferentes perfiles que distingue.

Ilustración 5-40. Entrada al servicio de acceso remoto por VPN

Recomendaciones:

No existen acciones correctivas; la medida se considera suficiente y adecuada para el nivel del sistema de información evaluado.

5.3.15 Segregación de redes [mp.com.4]

Sistemas a los que aplica	No Aplica
Madurez evaluada	L3

Tabla 5-50. Segregación de redes. Nivel de madurez

Existen VLANs creadas para segmentar la red. Esta medida únicamente es aplicable de forma obligatoria a sistemas de nivel alto. La organización no cuenta con ningún sistema de nivel alto.

5.3.16 Medios alternativos [mp.com.9]

Sistemas a los que aplica	No Aplica
Madurez evaluada	L3

Tabla 5-51. Comunicaciones: Medios alternativos. Nivel de madurez

Los equipos a nivel de red están duplicados. Esta medida únicamente es aplicable de forma obligatoria a sistemas de nivel alto. La organización no cuenta con ningún sistema de nivel alto.

5.3.17 Protección de los soportes de información [mp.si.1-4]

Sistemas a los que aplica	Sistema ERP, Sistema AE
Madurez evaluada	L2

Tabla 5-52. Protección de los soportes de información. Nivel de madurez

Valoración:

No existe un procedimiento claro y definido sobre la protección de los soportes de información. En este sentido el único procedimiento, el de ejecución de copia de seguridad, tampoco profundiza en proceso de protección, custodia y transporte de los soportes destinados a copia en cinta.

Adicionalmente, y aun siendo una medida de seguridad exigible, no existen mecanismos de cifrado en los soportes extraíbles (cintas de backup).

Sin embargo, mediante proceso de entrevista se ha determinado que existe una tarea sistemática de custodia, transporte y protección de estas cintas, las cuales son depositadas en caja fuerte de Registro General, una ubicación externa y distante unos 500 metros del CPD. El procedimiento de transporte es efectuado por el propio personal de la sección de TI. Las cintas van identificadas con un código ininteligible que no revela su contenido.

Evidencias:

Las cintas van identificadas con un código ininteligible que no revela su contenido.

Ilustración 5-41. Cintas con copias de seguridad

Recomendaciones:

El procedimiento actual es claramente insuficiente y no satisface las exigencias marcadas por el ENS para el nivel del sistema.

En este sentido sería necesario el desarrollo de un procedimiento que explícitamente definiese los soportes que se operan, incluido el papel, las medidas de protección que les son aplicables (incluido el cifrado en aquellos soportes que lo permitan) y el mecanismo de custodia/transporte a aplicar.

5.3.18 Borrado y destrucción de soportes [mp.si.5]

Sistemas a los que aplica	Sistema ERP, Sistema AE
Madurez evaluada	L0

Tabla 5-53. Destrucción de soportes. Nivel de madurez

Valoración:

No existe un procedimiento de borrado y destrucción de soportes.

Recomendaciones:

Desarrollar un procedimiento de destrucción de soportes para los soportes de la Unidad de TI y ofrecer un servicio de destrucción de soportes al usuario del sistema de información que le permita destruir sus propios soportes.

5.3.19 Protección de las aplicaciones [mp.sw.1-2]

Sistemas a los que aplica	Sistema ERP, Sistema AE
Madurez evaluada	L2-L3

Tabla 5-54. Protección de las aplicaciones. Nivel de madurez

Valoración:

Existen evidencias de la existencia un procedimiento de desarrollo en base a un framework unificado en base a SPRING, que además integra la seguridad de los aplicativos desde su diseño, mediante el uso de Application Security Verification Standard de OWASP hasta nivel 2.

Así mismo existe evidencia de la realización de pruebas de intrusión y análisis de vulnerabilidades siendo algunas de estas pruebas ejecutadas por personal interno y otras externalizadas.

Evidencias:

Se adjunta captura de pantalla del documento de uso interno sobre el uso de ASVS de OWASP.

Ilustración 5-42. Documento interno de la organización sobre uso de ASVS de OWASP

Recomendaciones:

Se recomienda sistematizar la fase de pruebas de seguridad para cada uno de los desarrollos, garantizando que sistemáticamente todas las aplicaciones nuevas o las que sufran cambios significativos serán sometidas a una evaluación de vulnerabilidades.

5.3.20 Información: Calificación y Datos Personales [mp.info.1-2]

Sistemas a los que aplica	Sistema ERP, Sistema AE
Madurez evaluada	L1-L2

Tabla 5-55. Calificación y Datos Personales. Nivel de madurez

Valoración:

La información de la organización se encuentra valorada dentro del proceso de adecuación al ENS y se identifican sus responsables en la política de seguridad de la entidad, sin embargo no existe evidencia de un procedimiento operativo que de forma efectiva regule las actuaciones que se pueden acometer con cada tipo de información existente en la organización.

De la misma forma, aunque la organización se encuentra adecuada a LOPD y han actualizado recientemente la valoración de este ámbito, no existe una constancia que en forma práctica se haya difundido en la organización la importancia de proteger la información personal y los usos aceptables de la misma.

Evidencias:

Existen evidencias de una valoración y catalogación de la información contenida en el sistema. Así, por ejemplo, podemos comprobar que, por ejemplo, la información de tipo académico tiene las siguientes características:

ACADE-Información	Nivel	Motivo
Confidencialidad	Bajo	Información de uso interno para un grupo de 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.

Tabla 5-56. Características de la información académica

Sin embargo, aunque se identifica el nivel de los datos personales que contiene, la confidencialidad requerida y en general las dimensiones de seguridad exigibles, no hay constancia de que exista una trasposición a medidas efectivas sobre el sistema de información.

De tal forma, y de forma efectiva, según se ha comprobado en el proceso de entrevista efectuado, los usuarios del sistema de información mueven, por ejemplo, información académica, conteniendo datos personales de alumnos, a servidores ubicados en países fuera de la UE, para los que no existe con la UPRG un contrato que regule el acceso a esa información por parte del prestador del servicio (dropbox, google, etc). Algo que, a priori, incumple claramente la legislación vigente en materia de protección de datos personales.

Recomendaciones:

Además de calificar la información, es necesario que el comité de seguridad, emita recomendaciones y normas sobre lo que es admisible efectuar con esa información por parte del usuario. Sobre todo, y de forma muy concreta, con aquella información de carácter personal de la que la universidad es responsable.

Se debería prestar especial atención al almacenaje remoto de la información en sistemas ajenos a la UPRG, el transporte de esa información en dispositivos removibles (USB, CD, ...) y el uso de esa información desde dispositivos móviles fuera de las instalaciones de la organización (móviles, tabletas, portátiles, ...).

5.3.21 Cifrado de la información en uso [mp.info.3]

Sistemas a los que aplica	No Aplica
Madurez evaluada	L0

Tabla 5-57. Cifrado de la información en uso. Nivel de madurez

No se cifra la información en uso. Esta medida únicamente es aplicable de forma obligatoria a sistemas de nivel alto. La organización no cuenta con ningún sistema de nivel alto.

5.3.22 Firma electrónica y sellos de tiempo [mp.info.4-5]

Sistemas a los que aplica	Sistema ERP, Sistema AE
Madurez evaluada	L0-L2

Tabla 5-58. Firma electrónica y sellos de tiempo

Valoración:

La organización no dispone de una política de firma electrónica que defina de forma clara qué documentos, de los gestionados electrónicamente en la organización, requieren de capacidad probatoria según la ley vigente y por tanto deben ser firmados mediante firma electrónica.

La organización, no obstante, hace uso de la firma electrónica y de los sellos de tiempo en su sistema de administración electrónico. Además, en la propia sede electrónica de la organización, existe una diferenciación clara entre qué servicios necesitan obligatoriamente de firma digital y qué

servicios pueden ser utilizados simplemente con usuario y contraseña. Hacer notar que los sellos de tiempo sólo son obligatorios para los sistemas con trazabilidad de nivel alto.

En los aspectos técnicos del proceso de firma, algoritmos utilizados y validez del procedimiento, el sistema de tramitación electrónica se basa en una aplicación que cubre las exigencias y requisitos técnicos del proceso mediante la utilización de la plataforma @FIRMA del ministerio de administraciones públicas.

Evidencias:

A continuación se adjunta captura de pantalla de la sede electrónica donde se pueden diferenciar los trámites ejecutables mediante usuario y contraseña, respecto de los trámites que exigen un procedimiento de firma digital.

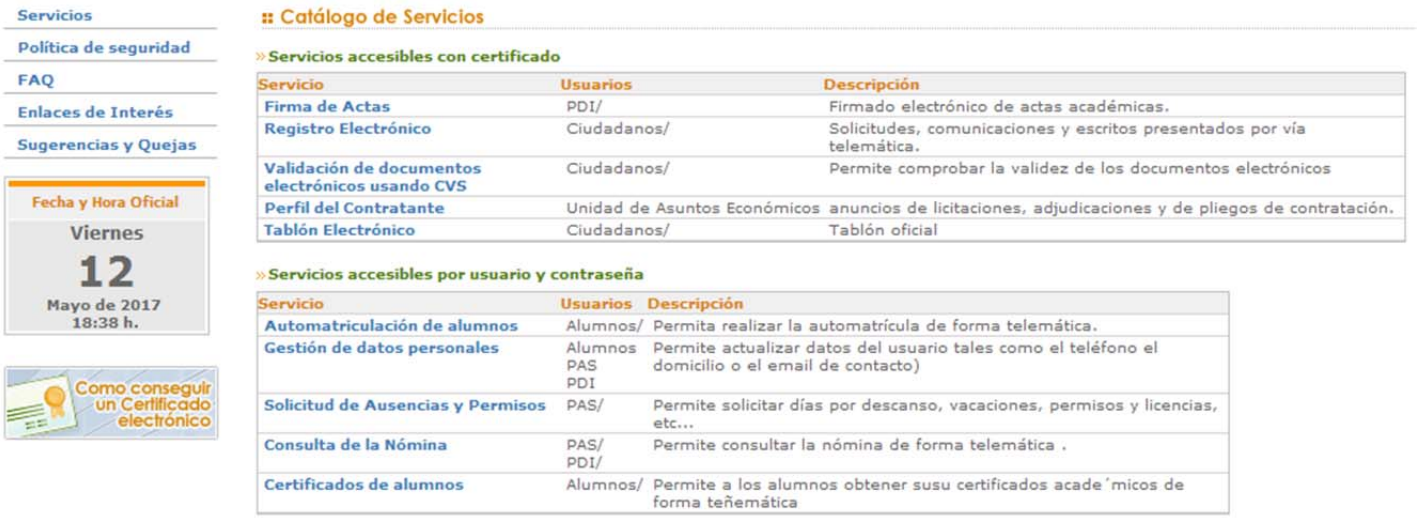

Ilustración 5-43. Servicios ofertados en la sede electrónica

Recomendaciones:

La recomendación es crear una política de firma y sellado tiempo que explicite los motivos por los que la información debe, o no, ser firmada digitalmente y los mecanismos usados para ello.

5.3.23 Limpieza de documentos [mp.info.6]

Sistemas a los que aplica	Sistema ERP, Sistema AE
Madurez evaluada	L0

Tabla 5-59. Limpieza de documentos. Nivel de madurez

Valoración:

No existe un procedimiento de limpieza de documentos, ni evidencias de concienciación en este sentido.

Recomendaciones:

Desarrollar un programa de concienciación al usuario sobre la limpieza de documentos. Implementar, si es posible, un servicio centralizado de limpieza de metadatos en documentos.

5.3.24 Copias de seguridad [mp.info.9]

Sistemas a los que aplica	Sistema ERP, Sistema AE
Madurez evaluada	L2-L3

Tabla 5-60. Copias de seguridad. Nivel de madurez

Valoración:

La organización cuenta con una política de copias de respaldo en múltiples dispositivos, las cuales permiten recuperar los datos en caso de pérdida, respaldan la información afectada por el alcance del ENS, las aplicaciones, los servicios y sus configuraciones asociadas, distinguiendo entre máquinas físicas y virtuales.

Las copias de seguridad se realizan sobre un primer nivel VTL (copias operativas) y posteriormente sobre un segundo nivel en CINTA (copias históricas). Estas cintas son conservadas en ubicación distante entre 500 y 1000 metros de la ubicación del CPD, almacenadas en caja de seguridad. Las cintas no implementan cifrado.

El procedimiento identifica los sistemas a copiar, los responsables del procedimiento, la infraestructura utilizada, el procedimiento de comprobación y el de restauración de información.

Evidencias:

A continuación, y a modo de ejemplo, se adjunta la implementación de la Política de copias de seguridad en la aplicación de tramitación, correspondiente al sistema Administración Electrónica.

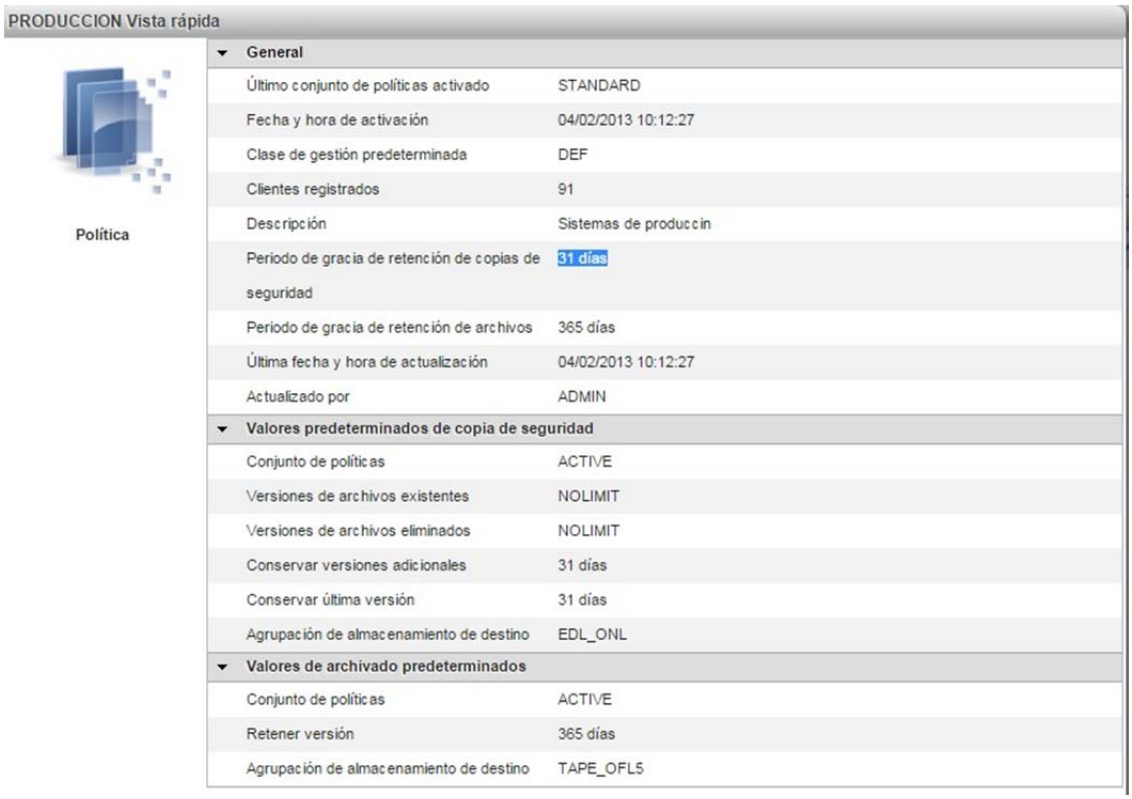

Ilustración 5-44. Política de copias de seguridad de l aapliación de tramitación

Recomendaciones:

Se recomienda el cifrado de las copias de seguridad en cinta. Así mismo se recomienda la ejecución de una prueba de recuperación completa de un servicio, al menos, una vez cada dos años para verificar que el procedimiento se ejecuta de forma correcta, es coherente y produce el resultado esperado.

5.3.25 Protección del correo electrónico [mp.s.1]

Sistemas a los que aplica	Sistema ERP, Sistema AE
Madurez evaluada	L0-L3

Tabla 5-61. Protección del correo electrónico. Nivel de madurez

Valoración:

La organización hace uso de mecanismos de transporte y entrega de correo electrónico mediante protocolos seguros (SMTPS, POP3S e IMAPS). Únicamente en la red interna se permite la conexión haciendo uso de protocolos no seguros de comunicación.

Así mismo, todo el correo entrante en la organización es filtrado mediante el sistema LAVADORA de REDIRIS, sometiéndolo a una serie de filtros anti-spam para marcado de correo no deseado, tecnologías antivirus para detección de malware, así como listas negras para rechazo automático de mensajes.

La organización tiene correctamente configurados los registros SPF para designar de forma adecuada a los servidores de correo aceptados en la organización.

Por otra parte, el correo interno es chequeado con CLAMAV.

Evidencias:

Se adjuntan los registros MX de la organización y el registro SPF, designando como relay de entrada los servicios de RedIris.

```
uprg.es.        86400   IN    MX    10 mx02.puc.rediris.es.
uprg.es.        86400   IN    MX    10 mx01.puc.rediris.es.
uprg.es.        86400   IN    TXT   "v=spf1 include:spf.puc.rediris.es
```

Ilustración 5-45. Registros MX de la organización

Se adjunta la configuración del servicio de correo de salida QMAIL, donde se define el uso de cifrado mediante TLS en SMTP y filtrado mediante CLAMAV. Internamente es posible hacer uso de SMTP sin mecanismos de cifrado.

```
smtpd_tls_auth_only=yes
smtpd_tls_cert_file = /etc/postfix/cert/relay1-all.pem
smtpd_tls_key_file=/etc/postfix/cert/relay1.key
smtpd_milters = unix:/opt/ClamAV/run/clamav-milter.socket
```

Ilustración 5-46. Configuración del servicio de correo de salida

Finalmente la entrega a usuario mediante Dovecot se realiza utilizando POP3 e IMAPS. . Internamente es posible hacer uso de POP3 e IMAP sin mecanismos de cifrado.

```
protocols = "imap pop3"
ssl_cert =          </etc/ssl/certs/ CA.new.crt ssl_key = </etc/ssl/private/privatekey.new.pem
ssl_protocols = TLSv1.1, TLSv1.2
```

Ilustración 5-47. Configuración del servicio de consulta de correo

Recomendaciones:

Se recomienda desarrollar una normativa de uso del correo electrónico y forzar el uso de protocolos sobre SSL/TLS obligatoriamente desde el interior de la organización, debido a que existe un riesgo significativo de captura de credenciales de acceso en caso de ataques tipo MitM o ataques en capa 2.

5.3.26 Protección de los servicios web [mp.s.2]

Sistemas a los que aplica	Sistema ERP, Sistema AE
Madurez evaluada	L1-L2

Tabla 5-62. Protección de los servicio web. Nivel de madurez

Valoración:

No existe evidencia de protección activa, haciendo uso de mecanismos de filtrado web automatizados a nivel de los servicios web.

La protección actual se centra en el uso de ASVS en el desarrollo y en la utilización de librerías que automatizan la limpieza de parámetros de entrada.

No obstante, el último informe de pruebas de intrusión, recoge entre otros, la explotación efectiva de inyecciones de SQL o la explotación de Cross-Site Scripting en servicios web.

Evidencias:

A continuación se recoge registro del último informe de pruebas de intrusión, a fecha septiembre de 2016, el cual incluye evidencias sobre la existencia de XSS e Inyección de SQL en aplicativos.

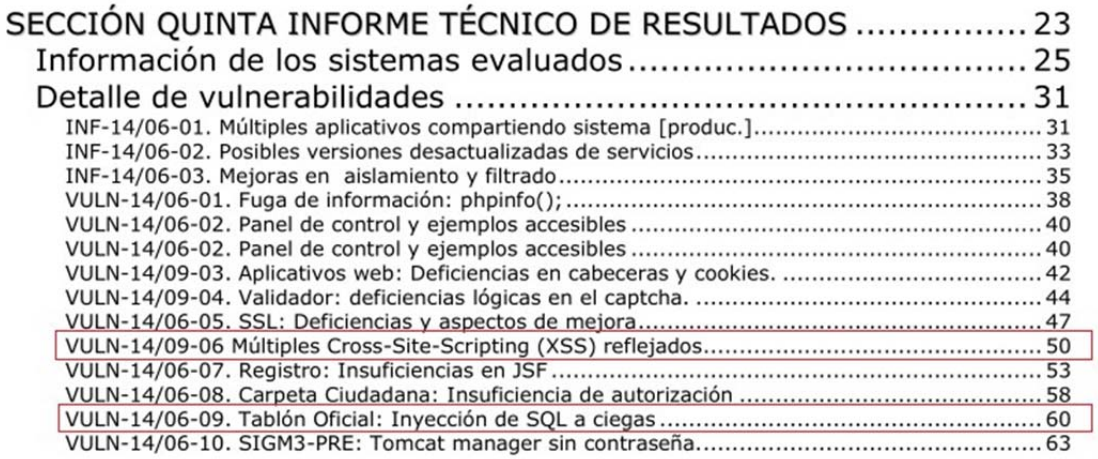

Ilustración 5-48. Informe de pruebas de intrusión

Recomendaciones:

Implementar medidas de protección en los servicios web mediante el uso de técnicas de filtrado a nivel de aplicación, bien mediante el uso de procedimientos homogéneos como puede ser MOD_SECURITY o los propios sistemas de filtrado de los firewall de la organización, o bien mediante el uso de técnicas específicas por aplicación, mediante el uso de control de la entrada de usuario y alerta ante excepciones en filtros y patrones pre-configurados.

5.3.27 Protección de Denegación de Servicio [mp.s.8]

Sistemas a los que aplica	Sistema AE
Madurez evaluada	L2

Tabla 5-63. Protección de Denegación de Servicio. Nivel de madurez

Valoración:

No existe un procedimiento de actuación frente a denegaciones de servicio. Tampoco hay un dimensionamiento específico del sistema, como se ha visto en la medida [op.pl.4], aunque sí existe

un sistema de monitorización de la capacidad que permite alertar en caso de situaciones de sobrecarga o falta de capacidad.

De la misma forma, existe un firewall perimetral con capacidad para medidas de protección antiDoS, no obstante, no existe evidencia de que estén siendo aprovechadas.

Evidencias:

Captura del sistema de firewall perimetral, el cual incluye mecanismos antiDoS.

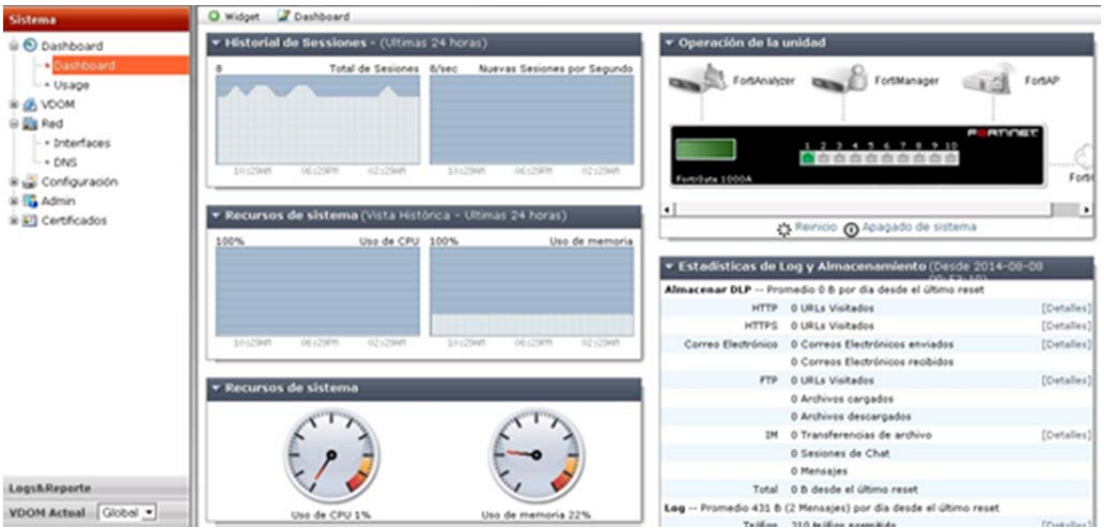

Ilustración 5-49. Menú de gestión de firewall perimetral

Captura del sistema de monitorización PGRT que monitoriza los parámetros de capacidad del sistema: CPU, memoria, ...

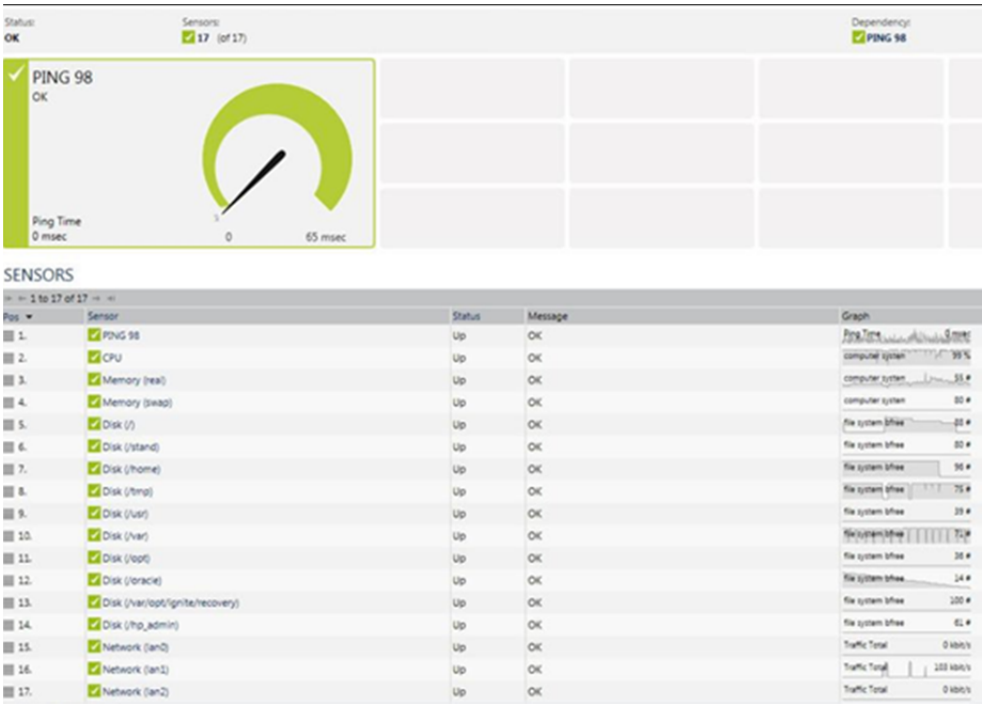

Ilustración 5-50. Sistema de monitorización

Recomendaciones:

Definir un método de actuación ante una denegación de servicio en base a los elementos de protección que ya existen en el sistema de información: sistema de monitorización y sistema IPS del firewall.

5.3.28 Medios alternativos [mp.s.9]

Sistemas a los que aplica	No Aplica
Madurez evaluada	L2

Tabla 5-64. Servicios: Medios alternativos. Nivel de madurez

Los servicios de ambos sistemas se encuentran balanceados en alta disponibilidad de forma que si falla uno de los servidores el servicio seguirá disponible en el resto de servidores, no obstante no se ha encontrado ningún documento ¡que defina esta política como algo común aimplantar en todos los servicios. Esta medida únicamente es aplicable de forma obligatoria a sistemas de nivel alto. La organización no cuenta con ningún sistema de nivel alto.

6 Referencias

- Guías de Seguridad publicadas por el CCN-CERT dentro de la serie CCN-STIC:

    - Guía “CCN-STIC 802. Esquema Nacional de Seguridad: Guía de auditoría”. Versión de Junio de 2010.

    - Guía “CCN-STIC-805. Política de Seguridad de la Información. Versión de Enero de 2015.

    - Guía “CCN-STIC 822. Esquema Nacional de Seguridad: Procedimientos de Seguridad”. Versión de Octubre de 2012.