Ingenia
INGENIERÍA E INTEGRACIÓN AVANZADAS

Esquema Nacional de Seguridad

Auditoría Interna ENS 2021

DIPUTACIÓN DE ALMERÍA

MÁLAGA
SEVILLA
MADRID
BARCELONA
SANTIAGO DE CHILE
LIMA

ingenia.es info@ingenia.es

HISTORIAL DE CAMBIOS

NOMBRE DEL FICHERO	VERSIÓN	RESUMEN DE CAMBIOS PRODUCIDOS	FECHA
DIPALME - Informe de auditoria ENS	No aplica		25/11/21

CLASIFICACIÓN DEL DOCUMENTO

CONFIDENCIAL

Nota de confidencialidad: La información contenida en este documento es CONFIDENCIAL y sólo se puede utilizar de acuerdo a la cláusula de CONTROL DE DISTRIBUCIÓN.

Es responsabilidad del Área o Departamento receptor de este documento su distribución interna en base a la necesidad de conocer la información aquí contenida.

CONTROL DE DISTRIBUCIÓN

AUTOR(ES): Ingenia

DISTRIBUCION:

Diputación Provincial de Almería

(DIPALME)

REFERENCIAS

Documentos externos	
[1]	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.
[2]	Real Decreto 951/2015, de 23 de octubre, de modificación del 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.
[3]	CCN-STIC 802. Esquema Nacional de Seguridad. Guía de Auditoría
[4]	CCN-STIC 808. Verificación del Cumplimiento del ENS

ÍNDICE DE CONTENIDOS

Indice de gráficos

Indice de tablas

1. INTRODUCCIÓN

El presente documento recoge el resultado de la auditoría interna realizada al Sistema de información de la **Diputación Provincial de Almería (en adelante DIPALME)** respecto al cumplimiento del Esquema Nacional de Seguridad. El objeto final de este documento es el de evidenciar las deficiencias detectadas, de forma que estas puedan ser subsanadas de conformidad con el plan de correcciones contenido en este documento.

Respecto a las recomendaciones de protección descritas en el anexo II del ENS, se han verificado completamente los tres grupos de medidas identificados en la normativa:

- Marco organizativo [org]: Medidas relacionadas con la organización global de la seguridad.
- Marco operacional [op]: Medidas para proteger la operación del sistema como conjunto integral de componentes para un fin.
- Medidas de protección [mp]: Medidas centradas para proteger activos concretos, según su naturaleza y la calidad exigida por el nivel de seguridad de las dimensiones afectadas.

Las personas asistentes y entrevistadas fueron las siguientes:

PERSONAS	ROLES ENS
ISABEL GÓMEZ POLO	Responsable de Seguridad del ENS.
ALICIAS MOZOS HIDALGO	Responsable del Sistema del ENS.
ANDRÉS ORENCIO RAMÍREZ	Responsable del Sistema Delegado para BBDD y Aplicaciones en el ENS.
ANTONIO GONZÁLEZ GARCÍA	Responsable del Sistema Delegado para Sistemas y Comunicaciones en el ENS.
CÉSAR ARTEAGA FERNÁNDEZ	Servicio de Organización e Información
PILAR GIMÉNEZ PIZARRO	Jefa de Sección de Organización

2. RESUMEN

Cod.	Medidas de Seguridad	No conformidad mayor	No conformidad menor	Observación	Sugerencia de Mejora	Conformidad	No aplica	Vacío	Totales
art	Cumplimiento de los articulos del ENS	0	1	0	1	0	0	0	2
org	Marco organizativo	0	1	0	0	3	0	0	4
op	Marco operacional	0	11	0	5	9	6	0	31
mp	Medidas de protección	0	4	2	4	23	7	0	40
	TOTAL	**0**	**17**	**2**	**10**	**35**	**13**	**0**	**77**

Tabla 1. Situación global

A continuación, se muestra un cuadro resumen del estado, así como la distribución las no conformidades y sugerencias de mejora para cada una de las medidas de seguridad del ENS:

Cod.	Medidas de Seguridad	No conformidad mayor	No conformidad menor	Observación	Sugerencia de Mejora	Conformidad	No aplica	Vacío	Totales
art	**Cumplimiento de los articulos del ENS**	1	0	0	3	1	0	0	5
org	**Marco organizativo**	1	0	0	0	3	0	0	4
op	**Marco operacional**	**0**	**11**	**0**	**5**	**9**	**6**	**0**	**31**
op.pl	Planificación	0	1	0	1	2	1	0	**5**
op.acc	Control de acceso	0	4	0	1	2	0	0	**7**
op.exp	Explotación	0	5	0	2	2	2	0	**11**
op.ext	Servicios externos	0	1	0	0	1	1	0	**3**
op.cont	Continuidad del servicio	0	0	0	0	1	2	0	**3**
op.mon	Monitorización del sistema	0	0	0	1	1	0	0	**2**
mp	**Medidas de protección**	**0**	**4**	**2**	**4**	**23**	**7**	**0**	**40**
mp.if	Protección de las instalaciones e infraestructuras	0	0	1	0	6	1	0	8
mp.per	Gestión del personal	0	0	0	2	2	1	0	5
mp.eq	Protección de los equipos	0	1	0	1	2	0	0	4
mp.com	Protección de las comunicaciones	0	0	0	0	3	2	0	5
mp.si	Protección de los soportes de información	0	0	1	0	4	0	0	5
mp.sw	Protección de las aplicaciones informáticas (SW)	0	1	0	0	1	0	0	2
mp.info	Protección de la información	0	2	0	1	2	2	0	7
mp.s	Protección de los servicios	0	0	0	0	3	1	0	4

Tabla 2. Resumen del estado de cumplimiento

3. HALLAZGOS Y SUGERENCIAS

Para cada una de las medidas en las que se ha encontrado un incumplimiento se ha establecido una propuesta/sugerencia de acción correctiva o de mejora, que no excluye que la propia DIPALME deba realizar su correspondiente Plan de Acciones Correctivas asociado al presente informe de auditoria.

Articulo/Control	Estado	Hallazgo	Sugerencia
Declaración de Aplicabilidad	**Oportunidad de mejora**	Darle formato de Manual de Seguridad o del SGSI, indicando una breve reseña de como se aplica el control en la organización y/o los documentos-registros donde se detalla dicha aplicación	
Categorización	**No conformidad**	No se dispone de la aprobación formal por parte de los responsbales de servicio/sistemas correspondientes.	Obtener dicho consentimiento mediante la formula del "silencio administrativo", es decir, enviar la valorqción y dar un plazo de respuesta tras el cual se de por cerrada y validada.
Proceso de autorización	**No conformidad**	Control definido pero no implantado	Generar un tipo de ticket en la herramienta RPC (a modo de workflow de soporte para las autorizaciones indicadas en la matriz RACI del procedimiento
Adquisición de Componentes	**Oportunidad de mejora**	Priorizar, incluso indicar como requisito de solvencia técnica que los compones hardware/software deben estar incluidos en la guia CCN-STIC-105 para la categoría ENS-MEDIO	
Dimensionamiento	**No conformidad**	Sin aplicar	Documentar la previsión de recursos prevista a corto-medio plazo (año 2022) para poder llevar a cabo las actuaciones procedimentales, organizativas y técnicas definidas en los correspondientes planes de emejora y/o acciones correctivas
Identificación	**No conformidad**	Sin aplicar	Son funciones organizativas que deben llevarse a cabo en el maroc del Comité de Seguridad, y con el máximo apoyo tecnológico posible, es decir, disponer de soluciones de gestión de identidades facilita en gran medida el cumplimiento de estos controles de seguridad
Requisitos de acceso	**No conformidad**	Sin aplicar	Sistemas no debe dar de alta a usuarios en los sistemas de información sin autorización previa explita del responsable correspondiente, para lo cual se puede utilizar la herramienta RPC
Proceso de gestión de derechos de acceso	**Oportunidad de mejora**	Inhabilitación automática de acceso a cuenta de usuario tras un periodo (prudencial) de no utilización/acceso a la misma	

Mecanismos de autenticación	**No conformidad**	Sin aplicar	Varias modalidad, los cambios en el ENS evitan la necesidad de aplicar 2FA a los usuarios internos
Acceso local (local login)	**No conformidad**	Sin aplicar	Se deben aplicar las GPOs que determina el ENS sobre este control:
Configuración y Gestión de seguridad (Bastionado)	**No conformidad**	No se aplica, no existe checklist de configuración/bastionado, ni evidencias	1.-Seleccionar aquellos controles de las guias del CCN-CERT que se van a aplicar y generar el correspondiente checklis 2.-Crear un ticket a modo de evidencia de que se aplicado dicho checklist al equipo/servidor correspondiente
Mantenimiento	**Oportunidad de mejora**	Escaneo activo de vulnerbailidades	
Gestión de cambios	**No conformidad**	Procedimentado pero sin aplicar	Diferenciar incidencias de cambios conforme se reciben a través de RPC, y aplicar el proceso definido sobre esta tipología.
Gestión de incidentes	**No conformidad**	se comprueba durante la auditoria la carencia de soporte para la aplicación del procedimiento	Durante la auditoria se mencinó la posible contratación de una herramienta que facilitaría en gran medida la aplicación practiva de este control
Actividad de los usuarios	**No conformidad**	Activado el registro de actividad de servidores Windows, Linux pero sin evidencia de revisión de los mismos	La única forma de que este control, y la dimensión trazabilidad en si misma del ENS, puedan tener una aplicación practica real, es a través de la contratación de un sercicio de SIEM-SOC
Gestión de servicios externos	**No conformidad**	Sin aplicar	Seleccionar de los proveedores registrados aquellos a los que aplicaría este control en base al SLA establecido, y requerir informes periódicos d ecumplimiento de dicho SLA
Métricas	**Oportunidad de mejora**	Establecer un conjunto de indicadores/métricas con periodos y responsabilidaes definidas respecto a su feed y control de las mismas a través de herramienta de cuadro de mando	
Identificación de personas	**Observación**	El acceso biometrico actual no cubre del todo los requerimientos del ENS, que exige un registro de entrada y salida del CPD tanto de personas como de materiales.	
Caracterización del puesto	**Oportunidad de mejora**	Asociar dicha caracterización, en la propia Declaración de Aplicabilidad, al conocimiento y cumplimiento por parte de los usuarios de la NOR19, y añadir características relacionadas con seguridad a los puestos mas técnicos	
Formación	**Oportunidad de mejora**	Realizar ejercicios de simulación y entrenamiento de ciberataques (blue/red Team)	

Bloqueo del puesto	**No conformidad**	Sin aplicar	Es mandatorio en el ENS la desconexion automática de terminal tras un tiempo de inactividad
Medios alternativos	**Observación**	En el inventario de activos deben existir portátiles o cualquier otro activo de reserva para casos de necesidad/urgencia.	
Borrado/Destrucción de Soportes	**Observación**	Dejar constancia del proceso de formateo y/o destrucción mediante video-imágenes y ticket correspondiente o alterntivamente contratar los servicios de una empresa externa	
Aceptación y puesta en servicio	**No conformidad**	Sin aplicar	Realización de auditorias de caja blanca-gris sobre las aplicaciones/funcionalidades antes de su puesta en producción
LOPD	**Oportunidad de mejora**	Eliminar del RAT, en su apartado de medidas de seguridad, las relacionadas con cuestiones de índole jurídico/organizativo	
Clasificación de la información	**No conformidad**	Procedimentado pero sin aplicar	La única forma de que este control, pueda tener una aplicación practica real, es mediante la adopción de soluciones IRM tipo Sealpath-CARLA
Limpieza de metadatos	**No conformidad**	Procedimentado pero sin aplicar	Durante la auditoria se mencinó la posible contratación de una herramienta que facilitaría en gran medida la aplicación de este control

4. DETALLE DE LA AUDITORIA

4.1 MARCO ORGANIZATIVO [ORG]

Id	Controles	Estado	Detalle	Evidencias
[org.1]	Política de seguridad	**Conforme**	Publicada en el BOP con fecha 26 de Agosto de 2020, correctamente definida y estrucuturada incluyendo los olres determinaods por la guia CCN-STIC-801, y con un enfoque integrador de seguridad y privacidad conforme modelo establecido por la la propia AEPD	https://www.dipalme.org/Servicios/Boletin/BOP5Anteriores.nsf/fechabop/C1257E260069CFD5C12585CF00416C91/$file/20-03001.pdf
[org.2]	Normativa de seguridad	**Conforme**	La versión vigente de la normativa STIC-NOR-19 que aplica a este control, es decir, la que regula la responsabilidad de los usuarios, es la v1.4 del 22-07-2021 y está publicada en la Intranet y con acceso a todos los trabajadores. Incluye todas las responsabilidades en la materia, confidencialidad, uso de activos, puesto despejado, etc.. y la posibilidad de monitorización y acceso a los buzones de correo@ por parte de la organización.	Se evidencia el envio de circulares a todo el personal donde se inciden en dicha normativa
[org.3]	Procedimientos de seguridad	**Conforme**	Se evidencia la existencia de varios procedimientos en distintas materias	Procedimientos vigentes
[org.4]	Proceso de autorización	**No conformidad**	Se ha definido un procedimiento en la materia que incluye una matriz RACI de autorizaciones, pero no está implantado en la organización.	

4.2 MARCO OPERACIONAL [OP]

4.2.1 PLANIFICACIÓN

Id	Controles	Estado	Detalle	Evidencias revisadas
[op.pl.1]	Análisis de riesgos	**Conforme**	Basado en la metodología MAgerit V3 y su herramienta de soporte PILAR.	Informe de análisis de riegos y su plan de mejora/tratamiento asociado, aprobados formalmente en la RES 2976/2020

[op.pl.2]	Arquitectura de seguridad	**Conforme**	Se dispone de varios diagramas de arquitectura correctamwnte definidos, tanto a nivel lógico como físico (CPDs)	Diagramas de arquitectura de red
[op.pl.3]	Adquisición de nuevos componentes	**Oportunidad de mejora**	Se recomienda priorizar desde ya en los pliegos de contratación los componentes presentes en la ultima versión de la guia CCN-STIC-105	Varios pliegos
[op.pl.4]	Dimensionamiento/Gestión de capacidades	**No conformidad**	Control sin aplicar en la actualidad	

4.2.2 CONTROL DE ACCESO

Id	Controles	Estado	Detalle	Evidencias revisadas
[op.acc.1]	Identificación	**No conformidad**	No estan definidos/aprobados formalmente los periodos de retención de cuentas de usuario. No se realiza la revisión de cuentas cada 12 meses por parte de los responsables de servicio indicada en el procedimiento	NOR5 y PRO7
[op.acc.2]	Requisitos de acceso	**No conformidad**	No hay evidencia de la aplicación de la regla del mínimo privilegio y necesidad de conocer, puesto que responsables de los sistemas de información no solictan/aprueban previamente el acceso de los usuarios	Registro de usuarios con acceso al sistema “Firma_Notifica”
[op.acc.3]	Segregación de funciones y tareas	**Conforme**	Correctamente definido en el PRO-09, Segregación de funciones y treas	Cuadro de funciones
[op.acc.4]	Proceso de gestión de derechos de acceso	**Oportunidad de mejora**	Procesos de alta y baja definidos con soporte por parte de Intranet y RPC, llega un correo a Sistemas que se encarga del alta/baja en LDAP. Periodo máximo sin acceso a cuenta tras la cual se inhabilita	Aplicación “Gestión de Bajas de Usuario”
[op.acc.5]	Mecanismos de autenticación	**No conformidad**	Control sin aplicar en la actualidad	

[op.acc.6]	Acceso local (local login)	**No conformidad**	Solo está aplicada la GPO que limita el número máximo d eintentos de login fallidos, el resto de las exigidas por este control estan sin aplicar.	GPO aplicadas sobre LDAP
[op.acc.7]	Acceso remoto	**Conforme**	VPN site to site a empresas externas VPN SSL con certificado validado por la FNMT	

4.2.3 EXPLOTACIÓN

Id	Controles	Estado	Detalle	Evidencias revisadas
[op.exp.1]	Inventario de activos	**Conforme**	En proceso de actualización a herramienta iTOP en formato Base de datos de configuración (CMDB)	ITOP
[op.exp.2]	Configuración de seguridad	**No conformidad**	No se aplica, no existe checklist de configuración/bastionado, ni evidencias.	
[op.exp.3]	Gestión de la configuración			
[op.exp.4]	Mantenimiento	**Oportunidad de mejora**	No se realiza a dia de hoy un escaneo activo de vulnerbabilidades en esots momentos solo se controla a nivel de equipos por parte del WSUS de Microsoft y mediante las emitidas por el CCN-CERT. Respecto al software, se asquiere con garantía a 5 años y al terminar se valora si renovarla o no, y en ese caso el equipo se da por amortizado y se gestiona conforme al control Mp.SI.5	WSUS y pliegos de contratación de suministros de material Hardware: cabinas de almacenamiento para sustituir las VNX 5200
[op.exp.5]	Gestión de cambios	**No conformidad**	Procedimentado en NOR6 y PRO12, pero sin implementar.	
[op.exp.6]	Protección frente a código dañino	**Conforme**	Sistema antimalaware Karpesky Endpoint	Consola del antimalware
[op.exp.7-9]	Gestión de incidentes	**No conformidad**	Si bien se dispone de un procedimiento correctamente definido y estrucuturado, se comprueba durante la auditoria la carencia de soporte y responsbailidades respecto a su aplicación práctica	
[op.exp.8]	Actividad de los usuarios	**No conformidad**	Activado el registro de actividad de servidores Windows, Linux pero sin evidencia de revisión de los mismos	

			No se dispone de servicio de SIEM	
[op.exp.11]	claves criptográficas	**Oportunidad de mejora**	No se generan claves criptográficas, las contraseñas de LDAP se guardan via HASH de manera cifrada. No se dispone de HSM	

4.2.4 SERVICIOS EXTERNOS

Id	Controles	Estado	Detalle	Evidencias revisadas
[op.ext.1]	Contratación y acuerdos de nivel de servicio	**Conforme**	Definido en NOR 18 y PRO22 e implantado a través deñ resgistro de proveedores/servicios TI asociado.	Registro de prestadores TI/proveedores para cada servicio/sistema Pliego de licitación correo@ en la nube donde se soliciya certificación en ENS
[op.ext.2]	Gestión diaria	**No conformidad**	No se estan solicitando informes de seguimiento de SLA	

4.2.5 CONTINUIDAD DEL SERVICIO

Id	Controles	Estado	Detalle	Evidencias revisadas
[op.cont.1]	Análisis de impacto	**Conforme**	Se han definido RTOs asociados a la dimensión disponibilidad de los servicios categorizados en el análisis de riesgos	BIA

4.2.6 MONITORIZACIÓN DEL SISTEMA

Id	Controles	Estado	Detalle	Evidencias revisadas
[op.mon.1]	Detección de intrusión	**Conforme**	Dos firewall PALO-ALTO + FORTIGATE, ambos acreditados en la guia CCN-STIC 105	Características del firewall
[op.mon.2]	Sistema de métricas	**Oportunidad de mejora**	Se revisa el INES 25/03/2021, firmada por CISO	Excel INES 2020

4.3 MEDIDAS DE PROTECCIÓN [MP]

4.3.1 PROTECCIÓN DE LAS INSTALACIONES E INFRAESTRUCTURAS

Id	Controles	Estado	Detalle	Evidencias revisadas
[mp.if.1]	Áreas separadas y con control de acceso	Conforme	Dispositivo de acceso biométrico para los miembros de sistemas.	Normativa de Seguridad Física
[mp.if.2]	Identificación de las personas	Observación		
[mp.if.3]	Acondicionamiento de los locales	Conforme	El CPD propio cuenta con sistemas de control de temperatura, humedad, detección de incendios y extinción.	
[mp.if.4]	Energía eléctrica	Conforme	Se dispone de SAIs en CPD cuyas características se describen en la normativa de seguridad física	
[mp.if.5]	Protección frente a incendios	Conforme	Se dispone de extintores en CPD cuyas características se describen en la normativa de seguridad física	
[mp.if.6]	Protección frente a inundaciones	Conforme	Ver Mp.if.3	
[mp.if.7]	Registro de entrada y salida de equipamiento	Conforme	Dispositivo biometrico	

4.3.2 GESTIÓN DEL PERSONAL

Id	Controles	Estado	Detalle	Evidencias revisadas
[mp.per.1]	Caracterización del puesto de trabajo	**Oportunidad de mejora**	Faltaría profundizar en los otros puestos/roles que no son propiamente los indicados en el ENS pero también pueden tener incidencia en la seguridad.	STIC-ENS-11, Caracteristización de Roles ENS
[mp.per.2]	Deberes y obligaciones	Conforme	Ver ORG 2	Normativa STIC-NOR-19

[mp.per.3]	Concienciación	**Conforme**	Amplia variedad de formatos y periodicidad adecuada.	Videopildoras, correos, avisos/alertas
[mp.per.4]	Formación	**Oportunidad de mejora**	Se imparten cursos en la materia por personal interno o empresa especializada, asociados a una iniciativa/catalogo formativo de la Junta de Andalucía	Catalogo de Cursos: 210401 (privacidad) + 210403 (seguridad)

4.3.3 PROTECCIÓN DE LOS EQUIPOS

Id	Controles	Estado	Detalle	Evidencias revisadas
[mp.eq.1]	Puesto de trabajo despejado	**Conforme**	Ver ORG 2	Normativa STIC-NOR-19
[mp.eq.2]	Bloqueo de puesto de trabajo	**No conformidad**	Control sin aplicar en la actualidad	
[mp.eq.3]	Protección de equipos portátiles	**Conforme**	50% de portátiles cifrados con la solución de Kaspersky endpoint.	Videopildoras, correos, avisos/alertas
[mp.eq.9]	Medios alternativos	**Observación**	Se debe disponer e inventariar el material alternativo o de respaldo, en especial en lo referido a puesto de usuario.	Ver Op.exp.1

4.3.4 PROTECCIÓN DE LAS COMUNICACIONES

Id	Controles	Estado	Detalle	Evidencias revisadas
[mp.com.1]	Perímetro seguro	**Conforme**	Doble línea de defensa con Paloalato activo-activo salidad corproativa a Intenet, filtrado web que pasa a la pareja de Forti activo-pasivo y una tercera línea de defensa, firewall a nivel de aplicación web (web aplication Firewall)	Diagramas de arquitectura d ered
[mp.com.2]	Protección de la confidencialidad	**Conforme**	VPNs con cifrado AES 256 Pentesting previsto para 2022 ya presupuesto	

[mp.com.3]	Protección de la autenticidad y de la integridad	**Conforme**	Es válido lo comentado para mp.com.2 y op.acc.7.	

4.3.5 PROTECCIÓN DE SOPORTES

Id	Controles	Estado	Detalle	Evidencias revisadas
[mp.si.1]	Etiquetado	**Conforme**	Los puertos de los equipos de usuarios estan inhabilitados por lo tanto no se pueden conectar soportes que permitan extraer información, y las cintas de backup se almacenan cifradas en el propio CPD (valorar ubicación diferente para prevenir que queden inutilizadas en caso de amenaza N y/o I del catalogo Magerit.	
[mp.si.2]	Cifrado	**Conforme**		
[mp.si.3]	Custodia	**Conforme**		
[mp.si.4]	Transporte	**Conforme**		
[mp.si.5]	Borrado y Destrucción	**Observación**	Se formatean los equipos antes de cambio de usuario pero sin ticket/evidencia, se desmonta, se destruyen físicamente y se llevan a un punto limpio por parte de una persona interna.	

4.3.6 PROTECCIÓN DE LAS APLICACIONES INFORMÁTICAS

Id	Controles	Estado	Detalle	Evidencias revisadas
[mp.sw1]	Desarrollo	**Conforme**	Los requerimientos de desarrollo software seguro se encuentran documentados en la normativa correspondiente.	Normativa de Desarrollo Software
[mp.sw2]	Aceptación y puesta en servicio	**No conformidad**	Control sin aplicar en la actualidad	

4.3.7 PROTECCIÓN DE LA INFORMACIÓN

Id	Controles	Estado	Detalle	Evidencias revisadas
[mp.info.1]	Datos de carácter personal	**Oportunidad de mejora**	DPD ejercido a través de Comité de Seguridad de la información, se reúne 1 al mes RAT publicado Varios modelos de contratos de encargado de tratamiento	Acta del Octubre del Comité
[mp.info.2]	Calificación de la información	**No conformidad**	Definido en NOR02 y PRO01 pero sin aplicación en la actualidad	
[mp.info.4]	Firma electrónica	**Conforme**	Política de firma@, sellos y certificado digital	Resolución 2069/2020 publicada en el BOP
[mp.info.6]	Limpieza de documentos	**No conformidad**	Definido en PRO18 pero sin aplicación en la actualidad	
[mp.info.9]	Copias de seguridad (backup)	**Conforme**	NOR8+PRO15 (copia@) + PRO 16 (restaurado) Sistema on-premise a disco (1 CPD y se replica al otro) y a cinta (librería y estan cifradas) Base de datos de los servidores de SGBD Infraestructura de maquinas virtuales, con RPO de 8 dias Servidor de correo@ y aplicaciones diaria y RPO de 180 dias Petición de restauración a través de RPC sobre el backup de cintas, apate se hacen pruebas cada 15 dias	

4.3.8 PROTECCIÓN DE LOS SERVICIOS

Id	Controles	Estado	Detalle	Evidencias revisadas
[mp.s.1]	Protección del correo electrónico	**Conforme**	Correo on-premise IMB- Lotus Notes Domino, con prevision de paso a Google Workspace	Consola
[mp.s.2]	Protección de servicios y aplicaciones web	**Conforme**	Hacking ético realizado a principios de año 2021	Informe de auditoria
[mp.s.8]	Protección frente a la denegación de servicio	**Conforme**	Primera línea de defensa a través los firewall Paloalto	Especificaciones firewall

Anexo. Listado de Evidencias

- Declaración de aplicabilidad
- Política de Seguridad
- Normativa de Seguridad
- Análisis de riesgos
- Plan de Capacidad-Dimensionamiento
- Diagramas de arquitectura de red
- Normativa de control de acceso y procedimientos de altas y bajas de usuario
- Registro de usuarios con acceso y rol por cada sistema de información categorizado
- Tickets de altas y bajas realizadas durante el presente 2021
- GPOs aplicadas sobre directorio activo conforme requerimientos ENS
- Evidencias de aplicación de 2FA en los sistemas con categoría media
- Procedimiento de configuración (servidores y equipos) y evidencias de bastionado
- Inventario de activos
- Procedimiento de gestión de cambios y evidencias/tickets asociados
- Procedimiento de gestión de incidentes de seguridad e informes asociados
- Correlación de eventos/logs (o en su defecto sistema SIEM)
- Auditorias técnicas y parcheo de vulnerabilidades detectadas
- Video o fotografías de los sistemas de protección del CPD
- Formación y concienciación recibida por el personal
- Definición de competencias en materia de seguridad de la información
- Cifrado de equipos
- Firewall, tipología y reglas de configuración
- Lo mismo para la VPN/mecanismo de acceso remoto
- Gestión de soportes y sistema para su aplicación
- Normativa de desarrollo software y pruebas de seguridad requeridas-realizadas

- Clasificación de la información y sistema para su aplicación
- Esquema de la infraestructura tecnológica.
- Correo@, sistema de backup y AntiDdos utilizado por la Diputación