Esquema Nacional de Seguridad

Auditoría ENS 2019

Enero 2020

DIPUTACIÓN DE ALMERÍA

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Ingenia – Equipo de Seguridad y Consultoría	Ingenia	Ingenia

HISTORIAL DE CAMBIOS

NOMBRE DEL FICHERO	VERSIÓN	RESUMEN DE CAMBIOS PRODUCIDOS	FECHA
DIPALME Informe Auditoría ENS 2019 v1.0	1.0	Primera versión.	20/01/20

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 de Almería (Servicio de Organización e Información)

REFERENCIAS

Documentos internos	
Título	**Nombre del fichero**
[1] Política de Seguridad (borrador) [2] Informe Análisis de Riesgos [3] Declaración de aplicabilidad ENS [4] Plan de Mejora de la Seguridad de la Información	DIPALME STIC - 01 Política de Seguridad DIPALME STIC-ENS-1 Análisis de Riesgos DIPALME STIC-ENS-4 Declaración de Aplicabilidad ENS DIPALME STIC-ENS-2 Plan de Mejora
Documentos externos	
[5] 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. [6] 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.	
[7] CCN-STIC 802. Esquema Nacional de Seguridad. Guía de Auditoría	
[8] CCN-STIC 808. Verificación del Cumplimiento del ENS	

ÍNDICE DE CONTENIDOS

1. INTRODUCCIÓN 5

2. RESUMEN EJECUTIVO 5

2.1 SITUACIÓN GLOBAL 7

3. DATOS DE LA AUDITORÍA 8

3.1 ALCANCE 8
3.2 METODOLOGÍA 10
3.3 CRITERIOS CONSIDERADOS 11
3.4 EQUIPO AUDITOR 11
3.5 ÁREAS ENTREVISTADAS 12
3.6 FECHA Y LUGAR DE REALIZACIÓN 14
3.7 IDIOMA DE LA AUDITORÍA 15

4. PLAN DE ACCIÓN DE LA AUDITORÍA ACTUAL 15

4.1 NO CONFORMIDADES MAYORES 16
4.2 NO CONFORMIDADES MENORES 27
4.3 OBSERVACIONES 49
4.4 SUGERENCIAS DE MEJORA 57
4.5 CUMPLIMIENTO CORRECTO 58
4.6 NO APLICA 61

5. DICTAMEN FINAL DE AUDITORÍA 62

1. Introducción

El presente documento recoge el resultado de la auditoría realizada a la Diputación Provincial de Almería, en adelante, la Diputación, para dar cumplimiento al artículo 34 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica, y su modificación mediante el Real Decreto 951/2015, de 23 de octubre, así como a lo establecido en su Anexo III, en los que se prescribe una auditoría de verificación de cumplimiento de los preceptos del ENS, y en la que se identifiquen los incumplimientos encontrados y se propongan las acciones correctoras convenientes, así como las recomendaciones de mejora cuando proceda.

El presente informe de auditoría deberá ser evaluado por el Responsable de Seguridad, que presentará sus conclusiones al Responsable del Sistema y demás personal implicado para que adopten las medidas correctoras adecuadas. Podrá ser requerido por el CCN-CERT en los términos previstos en el artículo 37 del ENS.

2. Resumen Ejecutivo

En general, el nivel de madurez global respecto al Esquema Nacional de Seguridad y sus medidas asociadas se considera bajo, con un nivel de concienciación del personal inferior a otras normativas de seguridad aplicables a Diputación, más concretamente las relativas a protección de datos personales.

No obstante, desde el Servicio de Organización e Información de la Diputación, se están llevando a cabo acciones para aumentar la cultura general en materia de seguridad y la concienciación del personal de Diputación en dichos aspectos, dando a conocer las normativas aplicables y previniendo de los riesgos que pueden presentarse al incumplir las normas relativas a seguridad de la información.

Desde el citado Servicio se ha llevado a cabo el Plan de Adecuación el Esquema Nacional de Seguridad, tomando como punto de partida la realización de un análisis de riesgos [2] para identificar la situación actual y el nivel de cumplimiento de las medidas del ENS, y que deriva en el Plan de Mejora de la Seguridad [4], en el que se han incluido las acciones necesarias para mitigar el nivel de riesgo y conseguir el cumplimiento necesario y nivel de madurez suficiente de todas las medidas incluidas en el Anexo II del ENS.

Respecto a la Política de Seguridad de la Información, la Diputación tiene pendiente finalizar el proceso de revisión, y aprobar y publicar la política de seguridad [1]. Por otro lado, la Diputación ha conformado un Comité de Seguridad, que además actúa como Órgano al que se han atribuido las funciones de Delegado de Protección de Datos, y que se reúne de forma periódica para tratar los aspectos relativos a seguridad de la información, privacidad y protección de datos, y gobierno abierto y transparencia.

Respecto al marco normativo asociado a la Política, a fecha actual no existe un cuerpo normativo ni procedimientos de seguridad asociados.

Respecto al análisis de riesgos, se llevó a cabo un análisis de riesgos en 2010, el cual no ha sido actualizado ni revisado, por lo que el análisis de riesgos impulsado desde el Servicio de Organización e Información, y el Servicio de Informática, realizado en el último trimestre de 2019, se considera como referencia y base para futuras actualizaciones en función de los cambios que se produzcan en los sistemas de información, y en las vulnerabilidades y amenazas identificadas para Diputación [2].

Adicionalmente, es necesario destacar que desde el Servicio de Organización e Información se han impulsado acciones formativas relativas al Esquema Nacional de Seguridad, impartidas durante el último trimestre de 2019.

Se han identificado varios aspectos que requieren atención preferente respecto a los requisitos del ENS:

- La Diputación deberá finalizar el proceso de revisión del documento de política de seguridad, y aprobar la Política, en la que se designan los roles asociados al ENS. Posteriormente, se deben elaborar las normativas y procedimientos de seguridad necesarios en función del análisis de riesgos realizado.
- Se debe dar continuidad a la acción relativa al análisis de riesgos, realizando la revisión anual correspondiente a finales de 2020, y actualizando dicho análisis si procede.
- Se debe establecer un inventario de activos de información: servicios, información, aplicaciones, hardware, comunicaciones, elementos auxiliares, servicios subcontratos, instalaciones, personal.
- Se deben llevar a cabo acciones de programación de auditorías técnicas y pen-testing. Se deberían abordar en primer término los sistemas de información más críticos. Cuando se realicen las auditorías y se detecten vulnerabilidades, se deben priorizar las acciones y medidas para contrarrestar los riesgos producidos por dichas vulnerabilidades.
- Se debe instalar, configurar y poner en marcha una herramienta específica para la gestión de incidencias relativas a seguridad de la información.
- Se debe establecer, en la Normativa de Contratación, que se deben tener en cuenta los aspectos sobre seguridad, propiedad intelectual, y cumplimiento normativo relativo a Seguridad de la Información en las licitaciones y en los contratos menores.
- Se debe redactar y poner en marcha un protocolo que contemple la coordinación con terceros con los que trabaja la Diputación, y que accedan o puedan acceder a los sistemas de información de la Diputación (in situ o en remoto), y por tanto a la información que manejan dichos sistemas. Se deben elaborar informes de seguimiento donde se verifiquen los aspectos de seguridad de la información incluidos en los contratos.
- Realización de BIAs (Business Impact Analysis) en relación a los servicios de la Diputación, realizando previamente una categorización de los servicios en base a su criticidad y la sensibilidad de la información que se maneja. Se deben identificar para dichos sistemas tanto el RTO (tiempos de recuperación objetivos), como el RPO (punto de recuperación objetivo o cantidad máxima de información que podría perderse o destruirse).
- Se debe propiciar que el personal de Diputación se comprometa y obligue al buen uso de los medios tecnológicos puestos a su disposición para el desempeño de sus funciones, y al cumplimiento de las políticas y normativas de seguridad de Diputación, incluida la política de mesas limpias y puesto despejado. Se deberá redactar una normativa de buen uso de los medios tecnológicos de cara al usuario.
- Se debe dar continuidad a las acciones formativas y de concienciación en materia de seguridad de la información y protección de datos personales, haciendo hincapié en las necesidades formativas de personal técnico que pudiera estar dedicado a seguridad, y las del personal de seguridad de la información que gestiona la seguridad en Diputación. Se deben realizar acciones formativas dirigidas a los Responsables de Servicio de Diputación, con el doble objetico de concienciación en aspectos de seguridad, e incidir en sus deberes y obligaciones respecto al ENS y al RGPD/LOPDgdd.
- Se recomienda la implantación de un SOC para la vigilancia continua (prevención), detección temprana de ciberataques, y respuesta a dichos incidentes, incluyendo la generación de alertas que permitan gestionar y controlar los incidentes relacionados con la seguridad de la información. Se recomienda la conexión del SOC a los aplicativos que se pretendan utilizar para la gestión y registro de ciberincidentes, la gestión de los activos de información, y los sistemas de correlación de eventos.

- Se debe procurar la utilización de protocolo seguro de comunicaciones (HTTP) en todas las páginas Web de la Diputación.
- Se deben implantar las medidas técnicas necesarias para cumplir con las políticas de contraseñas definidas, incidiendo en la fortaleza de las contraseñas, en los requisitos de doble factor de autenticación, en el cambio periódico de las mismas, y en los registros de accesos exitosos y fallidos, revisión de los mismos y generación de alertas asociadas.

2.1 Situación global

El resumen de las valoraciones del ENS a nivel global, desglosando en primer término en los artículos del ENS auditables, y en segundo término en los tres grandes tipos de medidas, organizativas, operacionales y de protección, puede visualizarse en la siguiente tabla:

VALORACIONES/ MEDIDAS	No conformidad mayor	No conformidad menor	Observación	Sugerencia de mejora	Correcto	No aplica
Cumplimiento de artículos del ENS	0	0	0	0	4	0
org. Marco Normativo	3	1	0	0	0	0
op. Marco Operacional	7	10	8	0	1	5
mp. Medidas de Protección	2	17	8	0	6	7
TOTAL	**12**	**28**	**16**	**0**	**11**	**12**

Tabla 1. Resumen Valoración Global ENS

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

VALORACIONES/ MEDIDAS	No conformidad mayor	No conformidad menor	Observación	Sugerencia de mejora	Correcto	N/A
Cumplimiento de artículos del ENS	0	0	0	0	4	0
org.- Marco Normativo	3	1	0	0	0	0
op.pl.- Planificación	0	2	2	0	0	1
op.acc- Control de acceso	0	4	3	0	0	0
op.exp.- Explotación	4	4	2	0	0	1
op.ext.- Servicios externos	2	0	0	0	0	1
op.cont- Continuidad del servicio	1	0	0	0	0	2
op.mon- Monitorización del sistema	0	0	1	0	1	0
mp.if.- Protección de las instalaciones e infraestructuras	0	3	1	0	3	1
mp.per- Gestión del personal	0	4	0	0	0	1
mp.eq- Protección de los equipos	0	2	0	0	2	0
mp.com- Protección de las Comunicaciones	0	1	1	0	1	2

VALORACIONES/ MEDIDAS	No conformidad mayor	No conformidad menor	Observación	Sugerencia de mejora	Correcto	N/A
mp.si.- Protección de los soportes de información	0	3	2	0	0	0
mp.sw.- Protección de las aplicaciones informáticas	1	1	0	0	0	0
mp.info.- Protección de la Información	0	3	2	0	0	2
mp.s.- Protección de los servicios	1	0	2	0	0	1
TOTAL	**12**	**28**	**16**	**0**	**11**	**12**

Tabla 2. Resumen Valoración Medidas ENS

3. Datos de la auditoría

3.1 Alcance

El alcance de la auditoría son los sistemas de información que sirven de base a la actividad de la Diputación.

Se ha identificado un único sistema de información (ya que los diferentes aplicativos comparten siempre algunos elementos comunes de comunicaciones y hardware). Como activos esenciales, se ha trabajado con los sub-sistemas de información que dan soporte a los servicios ENS de la Diputación, y con los tratamientos de datos personales asociados, que son los mostrados en la siguiente tabla.

SERVICIOS ESENCIALES ENS	VALORACIÓN DE LA DIMENSIÓN				
	D	I	C	A	T
Gestión Recursos Humanos	M	M+	M	M	M
Gestión Control de Presencia	B	B	B	B	B
Web Corporativa	M	B	B	B	B
Prevención y Salud Laboral	B	M	M	M	M
Gestión de la Contabilidad	B	M	B	B	B
Oficina Virtual	M+	M+	M+	M+	M+
Recaudación	B	M+	M+	M	M
Sede Electrónica Red Provincial	M+	M	M	M	M
Registro Electrónico	M	M+	M+	M	M
Archivo Electrónico	M+	M+	M+	M+	M+
Perfil del Contratante	M	M+	M+	M+	M+
Intranet	M	M	M	M	M
Portal del Empleado	M	M+	M	M	M
Servicio de Correo Electrónico	M	M+	M+	M+	M
BOP	B	B	B	B	B
Blog	B	B	0	0	B
Gestiones Deportivas Red Provincial	B	B	M+	B	B
Web Deportivas	B	B	B	B	B
Empresarias Almería	B	B	B	B	B
Procesos de Selección	B	M	B	B	B

SERVICIOS ESENCIALES ENS	VALORACIÓN DE LA DIMENSIÓN				
	D	I	C	A	T
Sistema de Información Territorial	B	0	0	0	0
Instituto de Estudios Almerienses	B	B	0	0	0
Actuaciones en Ayuntamientos	M	M	M	B	B
Acceso a Entidades Financieras	B	M	B	B	B
Peticiones Inversiones Ayuntamientos	B	B	B	B	B
Nóminas Fomento Empleo	M	M+	M	M	M
Servicios Sociales	M	M	M+	M	M+
Igualdad	M+	M+	M+	M+	M+
Residencia Asistida	M	M	M+	M	M+
Drogodependencia	M	M+	M+	M+	M+
Sabores de Almería	B	B	B	0	0
Formación	B	B	B	B	B
Servicio Atención al Usuario	B	B	B	B	B
Filming	B	B	B	0	0

Tabla 3. Valoración Servicios ENS

TRATAMIENTOS DATOS PERSONALES	VALORACIÓN DE LA DIMENSIÓN					
	D	I	C	A	T	DP
Recursos Humanos						M
Gestión de Reservas de Recursos por la Web						B
Guía de Actividades						B
Inscripción en Actividades y Eventos por la Web						B
Solicitud de Información y Consultas						B
Prevención y Salud Laboral						M
Gestión Económico-Contable						B
Gestión de Terceros						B
Registro de Entrada y Salida						B
Gestión de Tesorería						B
Gestión de Usuarios Red Provincial						B
VPN Usuarios Red Provincial						B
Archivo General de Diputación de Almería						M
Gestión y Control de la Biblioteca						B
Contratación						B
Gestión de Solicitudes de Atención a Usuarios y Ciudadanos						B
Gestión de Teléfonos Fijos y Móviles						B
Suscripción a actividades, eventos y blog						B
Acciones Formativas						B
Gestión Correos Electrónicos RPC						B
Boletín Oficial de la Provincia						B
Acciones Deportivas						M
Igualdad y Mujeres						B
Igualdad. Violencia de Género						M+
Selección de Personal						B
Publicaciones IEA						B
Actuaciones Judiciales						M
Obras						B

TRATAMIENTOS DATOS PERSONALES	VALORACIÓN DE LA DIMENSIÓN					
	D	I	C	A	T	DP
Fomento Empleo						M
Servicios Sociales Comunitarios						M
Atención Residencial a Personas Mayores						M
Servicio Provincial de Drogodependencia y Adiciones						M
Sabores Almería						B
Gestión de Solicitudes Atención Usuarios y Ciudadanos						B
Filming Almería						B

Tabla 4. Valoración Tratamientos de Datos Personales

La categoría del Sistema de Información, considerando todos los subsistemas conjuntamente, es MEDIA.

3.2 Metodología

La metodología de trabajo empleada ha seguido las directrices generales recogidas en la guía 802 del CCN [7] y se ha utilizado como referencia la guía 808 del CCN [8]

Se ha realizado previamente una planificación de las entrevistas necesarias para la auditoría en la que se han identificado los interlocutores necesarios para responder a las cuestiones de las diferentes áreas que abarca el ENS y se ha recabado la documentación existente, y pertinente para el análisis de riesgos realizado y para la presente auditoría, tanto para verificar el cumplimiento de aquellos aspectos que estuvieran documentados, como para la obtención de evidencias.

En base a lo exigido en el Anexo III del ENS se han auditado los siguientes aspectos:

- Que la política de seguridad define los roles y funciones de los responsables de la información, los servicios, los activos y la seguridad del sistema de información.
- Que existen procedimientos para resolución de conflictos entre dichos responsables.
- Que se han designado personas para dichos roles a la luz del principio de "separación de funciones".
- Que se ha realizado un análisis de riesgos, con revisión y aprobación anual.
- Que se cumplen las recomendaciones de protección descritas en el anexo II, sobre Medidas de Seguridad, en función de las condiciones de aplicación en cada caso.
- Que existe un sistema de gestión de la seguridad de la información, documentado y con un proceso regular de aprobación por la dirección.

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.

Para cada una de las cuestiones a auditar se ha requerido evidencia suficiente que demostrara su cumplimiento.

3.3 Criterios considerados

Se ha auditado el ENS conforme al cumplimiento de:

- 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.
- 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.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales.

Puesto que la Categoría del Sistema de Información es MEDIA, el presente informe consiste en una auditoría de tipo FORMAL.

Los hallazgos de no conformidad se han clasificado atendiendo a los criterios de la guía 802 del CCN [7] atendiendo a los siguientes grados:

- **No Conformidad Menor:** Se documenta una "No Conformidad Menor" ante la ausencia o el fallo en la implantación o mantenimiento de uno o más de los requisitos del ENS, incluyendo cualquier situación que pudiese, en base a una evidencia objetiva, sustentar una duda significativa sobre la conformidad del sistema de información con uno más de tales requisitos.
- **No Conformidad Mayor**: Se documenta una "No Conformidad Mayor" cuando se detecten "No Conformidades Menores" en relación con cualquiera de los preceptos contenidos en el ENS, o en el Marco Organizativo, o en alguno de los subgrupos que integran el Marco Operacional o las Medidas de Seguridad que, evaluadas en su conjunto, puedan implicar el incumplimiento del objetivo del Grupo o Subgrupo considerados.
- Se documenta una **Observación** cuando se han encontrado evidencias de, una debilidad, una vulnerabilidad o una situación que, sin comprometer cualquier área del ENS pueda, en la actualidad o en el futuro, derivar en un problema. Las acciones asociadas a las observaciones identificadas deben llevarse a cabo en todos los casos.
- Se documenta una **Sugerencia de Mejora**, cuando se han encontrado medidas del ENS en las que, no existiendo incumplimientos, pueden llevarse a cabo acciones que supongan una mejor eficacia en el cumplimiento.

3.4 Equipo auditor

Auditor Jefe: David López Gutiérrez, CRISC[1], CISM[2], CDPP[3].

Consultora ENS: Antonia Pilar Farfán Madrid, CISA[4], CISM, CDPP

[1] Certified in Risk and Information Systems Control (ISACA)
[2] Certified Information Security Management (ISACA)
[3] Certified Data Privacy Professional (ISMS FORUM)

[4] Certified Information Systems Auditor (ISACA)

Los miembros del equipo auditor no han participado en el mantenimiento de ninguno de los aspectos del ENS que auditan, por lo que sus conclusiones se consideran objetivas e imparciales.

3.5 Áreas entrevistadas

Se ha entrevistado a las siguientes áreas de Diputación, para medir el nivel de cumplimiento actual de las medidas del ENS:

ENTREVISTA	ÁREAS	CONTENIDO	DURACIÓN
Entrevista 1	Servicio de Organización e Información; Servicio de Informática	Análisis de cumplimiento ENS	2,5 horas
Entrevista 2	Servicio de Organización e Información	Análisis de cumplimiento RGPD / LOPDgdd Análisis de cumplimiento ENS (mp.info.1)	1,5 horas
Entrevista 3	Servicio de Organización e Información; Servicio de Personal (Departamento de Personal; Departamento de Formación)	Análisis de cumplimiento ENS	30 min
Entrevista 4	Servicio de Organización e Información; Régimen Interior (Negociado de Contratación)	Análisis de cumplimiento ENS	30 min
Entrevista 5	Servicio de Organización e Información; Informática; Archivo	Análisis de cumplimiento ENS	30 min
Entrevista 6	Servicio de Organización e Información; Informática; Régimen Interior (Sección de Mantenimiento)	Análisis de cumplimiento ENS	30 min

Tabla 5. Entrevistas Análisis Medidas ENS

Adicionalmente, se han llevado a cabo entrevistas a las diferentes Áreas de Diputación, al objeto de verificar el cumplimiento del ENS y del RGPD/LOPDgdd, identificando adicionalmente todos los sub-sistemas de información y tratamientos de datos personales asociados a los servicios prestados por Diputación en el marco del ENS.

ENTREVISTA	ÁREA
Entrevista 7	PRESIDENCIA, LUCHA CONTRA LA DESPOBLACIÓN Y TURISMO GABINETE
Entrevista 8	HACIENDA
Entrevista 9	RECURSOS HUMANOS

ENTREVISTA	ÁREA
Entrevista 10	FOMENTO, MEDIOAMBIENTE Y AGUA
Entrevista 11	BIENESTAR SOCIAL, IGUALDAD Y FAMILIA
Entrevista 12	ASISTENCIA A MUNICIPIOS
Entrevista 13	PROMOCIÓN AGROALIMENTARIO Y RÉGIMEN INTERIOR
Entrevista 14	CULTURA Y CINE DEPORTES Y JUVENTUD
Entrevista 15	ÁREA DE CULTURA GABINETE DE PRESIDENCIA ARCHIVO Y BIBLIOTECA JUNTA ARBITRAL DE CONSUMO ÁREA DE DEPORTES SERVICIO DE INFORMÁTICA
Entrevista 16	SERVICIO DE RÉGIMEN INTERIOR SERVICIO DE ORGANIZACIÓN E INFORMACIÓN DIRECCIÓN DE ÁREA INFRAESTRUCTURA URBANA SECCIÓN DE PROYECTOS E INFRAESTRUCTURAS SECCIÓN DE APOYO TERRITORIAL SERVICIO DE PLANIFICACIÓN Y GESTIÓN INFRAESTRUCTURA URBANA SERVICIO DE MEDIO AMBIENTE

Tabla 6. Entrevistas de Auditoría. Áreas Diputación

3.6 Fecha y lugar de realización

La auditoría se llevó a cabo en las siguientes fechas y lugares:

ENTREVISTA	FECHA	LUGAR
Entrevista 1	09/09/2019	Ctra., de Ronda, 216. Edificio de Usos Múltiples. C.P. 04009. Almería
Entrevista 2	10/09/2019	C/ Navarro Rodrigo, 17. Palacio Provincial. C.P. 04001. Almería
Entrevista 3	12/09/2019	C/ Navarro Rodrigo, 17. Palacio Provincial. C.P. 04001. Almería
Entrevista 4	12/09/2019	C/ Navarro Rodrigo, 17. Palacio Provincial. C.P. 04001. Almería
Entrevista 5	12/09/2019	C/ Navarro Rodrigo, 17. Palacio Provincial. C.P. 04001. Almería
Entrevista 6	12/09/2019	C/ Navarro Rodrigo, 17. Palacio Provincial. C.P. 04001. Almería
Entrevista 7	03/10/19	C/ Navarro Rodrigo, 17. Palacio Provincial. C.P. 04001. Almería
Entrevista 8	04/10/19	C/ Navarro Rodrigo, 17. Palacio Provincial. C.P. 04001. Almería
Entrevista 9	04/10/19	C/ Navarro Rodrigo, 17. Palacio Provincial. C.P. 04001. Almería
Entrevista 10	07/10/19	C/ Hermanos Machado, 27. C.P. 04004. Almería
Entrevista 11	09/10/19	Rambla Alfareros, 30. C.P. 04003. Almería
Entrevista 12	09/10/19	Rambla Alfareros, 30. C.P. 04003. Almería
Entrevista 13	11/10/19	C/ Navarro Rodrigo, 17. Palacio Provincial. C.P. 04001. Almería
Entrevista 14	15/10/19	C/ Navarro Rodrigo, 17. Palacio Provincial. C.P. 04001. Almería
Entrevista 15	29/10/19	C/ Navarro Rodrigo, 17. Palacio Provincial. C.P. 04001. Almería Ctra., de Ronda, 216. C.P. 04009. Almería

ENTREVISTA	FECHA	LUGAR
Entrevista 16	30/10/19	C/ Navarro Rodrigo, 17. Palacio Provincial. C.P. 04001. Almería C/ Hermanos Machado, 27. C.P. 04004. Almería

Tabla 7. Fechas y lugares de las entrevistas

3.7 Idioma de la auditoría

La auditoría se llevó a cabo totalmente en castellano.

4. Plan de Acción de la Auditoría Actual

Para cada no conformidad, observación y sugerencia de mejora detectada durante esta auditoría se indica su situación actual y la propuesta de acción correctiva o mejora.

Los hallazgos de auditoría que requieren de una acción se agrupan según la clasificación descrita en el *Apartado 3.3*:

4.1 No conformidades mayores

CONTROL	REQUISITO	SITUACIÓN ACTUAL	INCUMPLIMIENTO	CORRECCIÓN	VALORACIÓN	EVIDENCIA
org.1	Política de Seguridad La Política de Seguridad será aprobada por el órgano superior competente que corresponda de acuerdo al art.11 y se plasmará en un documento escrito. PUNTOS CLAVE: Debe definir los roles y funciones del RINF, RSERV, RSEG, RSIS. Debe incluir procedimientos de resolución de conflictos Se da la separación de funciones con el RSEG	No hay aprobada política de seguridad. Se elaboró una Política en 2010 y trabajos de adecuación. Se elaboró un manual de procedimientos y normativas, pero no se ha actualizado (tampoco se llegó a aprobar). Hay un comité de seguridad formalizado, con reuniones periódicas, con representantes de cada unidad. Últimas reuniones en junio y septiembre. Periodicidad de reuniones: 1 vez al mes. Se aglutina ENS/RGPD y Transparencia. A la vez que se creó el Comité de Seguridad, se nombró al Responsable de Seguridad a través de la correspondiente resolución (2016). Se ha trabajado en un borrador de la política durante el mes de julio de 2019. Pendiente revisión, aprobación, publicación.	No está aprobada la Política de Seguridad	Revisar, aprobar y publicar la Política de Seguridad de la Información de la Diputación. Tareas: 1.- Terminar de revisar el borrador de Política de Seguridad trabajado en Julio 2019 2.- Aprobar la Política de Seguridad en Junta de Gobierno 3.- Publicación de la Política de Seguridad	No conformidad mayor	Entrevista Auditoría; Borrador Política de Seguridad

CONTROL	REQUISITO	SITUACIÓN ACTUAL	INCUMPLIMIENTO	CORRECCIÓN	VALORACIÓN	EVIDENCIA
org.2	Normativas de Seguridad Se dispondrá de una serie de documentos que describan: a) el uso correcto de equipos, servicios e instalaciones; b) lo que se considerará uso indebido; c) la responsabilidad del personal con respecto al cumplimiento o violación de estas normas: derechos, deberes y medidas disciplinarias de acuerdo a la legislación vigente	Cuerpo normativo de seguridad: se elaboró en 2010 y no se ha actualizado. Hay alguna norma que no emana de la política	No se ha redactado un conjunto de normativas que contemplen todos los aspectos de seguridad de la información	Se deberán redactar las normativas de seguridad de la información que emanen de la Política de Seguridad, siguiendo como referencia la Guía CCN-STIC 883, concretamente el Apartado 6 relativo al desarrollo de normativas de seguridad. Tareas: 1.- Redactar borrador de las Normativas, y definir los responsables de revisión y de aprobación 2.- Adaptar las Normativas a la operativa de Diputación de Almería 3.- El Responsable de Seguridad convocará al comité de seguridad para la aprobación de las normativas de seguridad.	No conformidad mayor	Entrevista Auditoría;

CONTROL	REQUISITO	SITUACIÓN ACTUAL	INCUMPLIMIENTO	CORRECCIÓN	VALORACIÓN	EVIDENCIA
org.3	Procedimientos operativos Se dispondrá de una serie de documentos que detallen de forma clara y precisa: a) cómo llevar a cabo las tareas habituales, b) quién debe hacer cada tarea; c) cómo identificar y reportar comportamientos anómalos	Cuerpo normativo de seguridad: se elaboró en 2010 y no se ha actualizado. Hay alguna norma que no emana de la política	No se ha redactado un conjunto de procedimientos que contemplen todos los aspectos de seguridad de la información	Se deberán redactar los procedimientos de seguridad de la información que emanen de la Normativas de Seguridad, en base a lo exigido en las diferentes medidas del ENS que impliquen elaboración de protocolos o procedimientos. Tareas: 1.- Redactar borrador de los Procedimientos, y definir los responsables de revisión y de aprobación 2.- Adaptar los Procedimientos a la operativa de Diputación de Almería 3.- El Responsable de Seguridad convocará al comité de seguridad para la aprobación de los procedimientos de seguridad.	No conformidad mayor	Entrevista Auditoría;

CONTROL	REQUISITO	SITUACIÓN ACTUAL	INCUMPLIMIENTO	CORRECCIÓN	VALORACIÓN	EVIDENCIA
op.exp.3	Gestión de la configuración Se gestionará de forma continuada la configuración de los componentes del sistema de forma que: a) Se mantenga en todo momento la "regla de funcionalidad mínima (op.exp.2)"; b) Se mantenga en todo momento la regla de "seguridad por defecto (op.exp.2)"; c) El sistema se adapte a las nuevas necesidades, previamente autorizadas (op.acc.4); d) El sistema reacciones a vulnerabilidades reportadas (op.exp.4); e) El sistema reacciones a incidentes (op.exp.7)	No hay nada por escrito referente a gestión de la configuración, gestión de vulnerabilidades, etc. No existen protocolos de gestión de vulnerabilidades de seguridad. Acceso a equipo: el propio usuario es administrador local de su máquina, por lo que puede instalar aplicaciones, puede modificar configuraciones. Securización teléfonos: están abiertos y el usuario puede instalar y configurar las aplicaciones que desee. Uno de los pasos a dar sería que le usuario únicamente pueda instalar aplicaciones corporativas. Aplicaciones corporativas: correo electrónico en el móvil. El resto son aplicativos Web. No hay aplicaciones que accedan a LAN. En algunos casos se instala VPN en el propio teléfono. Por otro lado, se puede firmar a digitalmente a través del teléfono. Antivirus no se instalan.	No existen protocolos de gestión de vulnerabilidades de seguridad que puedan identificarse en los procesos de gestión continuada de la configuración de los diferentes elementos del sistema de información de Diputación. Los usuarios pueden cambiar la configuración de seguridad de sus ordenadores, y pueden realizar instalaciones de cualquier software.	Redactar y aprobar procedimiento de gestión de vulnerabilidades, en el que se refleje al menos lo siguiente: - Tipo de auditorías técnicas a realizar - Medios a utilizar para la identificación de vulnerabilidades - Plan de acción para la corrección de las vulnerabilidades encontradas. Se indicará en las normativas correspondientes que el usuario no podrá realizar instalaciones de aplicaciones por su cuenta, en PC o dispositivo móvil, sin la asistencia de Informática. Únicamente se instalarán aplicaciones corporativas en el móvil. Si se decidiera permitir a los usuarios este tipo de instalaciones, se deberán contemplar los criterios y medidas a utilizar para que el proceso se realice de forma segura.	No conformidad mayor	Entrevista Auditoría;

CONTROL	REQUISITO	SITUACIÓN ACTUAL	INCUMPLIMIENTO	CORRECCIÓN	VALORACIÓN	EVIDENCIA
op.exp.4	Mantenimiento Para mantener el equipamiento físico y lógico que constituye el sistema, se aplicará lo siguiente: a) Se atenderá a las especificaciones de los fabricantes en lo relativo a instalaciones y mantenimiento de los sistemas; b) Se efectuará un seguimiento continuo de los anuncios de defectos; c) Se dispondrá de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones. La priorización tendrá en cuenta la valoración del riesgo en función de la aplicación o no de la actualización.	Existen equipos con SO sin soporte técnico; De forma genérica todos los equipos en CPD disponen de contrato de mantenimiento. Existe al menos una app importante instaladas en XP. Sistemas de copias de seguridad: sin licencia ni soporte a nivel SW, las máquinas sin disponen de mantenimiento. También se utiliza Presto sin mantenimiento. NAS de Hermanos Machado sin mantenimiento. Puede haber casos en los que el usuario instale app que no tienen licencia (ejemplo AutoCAD). Otro escenario es la compra de SW desde un Departamento concreto, sin que haya conocimiento por parte de Informática	Existencia de equipos y sistemas sin soporte técnico y mantenimiento, que no cuentan con los parches de seguridad y actualizaciones necesarias para estar correctamente protegidos. Algunas compras de SW/aplicaciones se realizan de forma descentralizada, sin que exista conocimiento por parte de informática ni por parte del equipo de seguridad de la información.	Se deberá realizar la migración de aplicaciones de sistemas sin soporte técnico, tipo Windows XP. Todos los sistemas de información deberán contar con el correspondiente soporte técnico y mantenimiento que permita minimizar las vulnerabilidades de seguridad y mantener los equipos y sistemas correctamente actualizados. Las compras de SW, aplicativos, o de cualquier elemento asociado a los sistemas de información de Diputación, debe ser conocida por el responsable de seguridad y el responsable de sistemas, al objeto de especificar los requisitos de seguridad necesarios para asegurar una correcta protección y el cumplimiento normativo en materia de seguridad de la información.	No conformidad mayor	Entrevista Auditoría;

CONTROL	REQUISITO	SITUACIÓN ACTUAL	INCUMPLIMIENTO	CORRECCIÓN	VALORACIÓN	EVIDENCIA
op.exp.7	MEDIA: Se dispondrá de un proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema, incluyendo: a) Procedimiento de reporte de eventos de seguridad y debilidades, detallando los criterios de clasificación y el escalado de la notificación; b) Procedimiento de toma de medidas urgentes, incluyendo la detención de servicios, el aislamiento del sistema afectado, la recogida de evidencias y protección de los registros, según convenga al caso; c) Procedimiento de asignación de recursos para investigar las causas, analizar las consecuencias y resolver el incidente; d) Procedimiento para informar a las partes interesadas, internas y externas; e) Procedimientos para: prevenir que se repita el incidente; incluir en los procedimientos de usuario la identificación y forma de tratar el incidente; actualizar, extender, mejorar y optimizar los procedimientos de resolución de incidentes.	Se puso en marcha hace 2 años un gestor de incidencias informáticas. En primera instancia llega al CAU (soporte 1er nivel), en segunda instancia a nivel técnico (2ndo nivel). Tipo de incidencias: incidencias de usuarios. No hay app de incidencias de seguridad aparte. Tampoco están categorizadas. No hay nada por escrito. Para incidentes críticos (afectan a disponibilidad de la información), documentan de forma interna cómo se han gestionado los incidentes. ¿Sondas CERT? No disponen.	No existe un aplicativo para gestión de ciberincidentes, ni protocolos de actuación al respecto. No se han implantado sondas de equipos CERT para la detección de ciberincidentes.	Se deberá redactar y aprobar normativa y procedimiento de gestión de ciberincidentes, que contenga al menos: - Procesos de detección de incidentes de seguridad de la información - Notificación de incidentes y escalado - Categorización y clasificación de incidentes - Comunicación de incidentes a terceras partes, CERTS y Fuerzas y Cuerpos de Seguridad - Gestión y resolución de incidentes - Aplicación de medidas urgentes en su caso - Análisis post-incidente Conexión mediante sondas a CERTS a nivel autonómico/estatal (equipos de respuesta ante incidentes)	No conformidad mayor	Entrevista Auditoría;

CONTROL	REQUISITO	SITUACIÓN ACTUAL	INCUMPLIMIENTO	CORRECCIÓN	VALORACIÓN	EVIDENCIA
op.exp.9	Registro de la gestión de incidencias MEDIA: Se registrarán todas las actuaciones relacionada con la gestión de incidentes, de manera que: a) Se registrará el reporte inicial, las actuaciones de emergencia y las modificaciones del sistema derivadas del incidente; b) Se registrará aquella evidencia que pueda, posteriormente, sustentar una demanda judicial, o hacer frente a ella, cuando el incidente pueda llevar actuaciones disciplinarias sobre el personal interno, sobre proveedores externos o la persecución de delitos; c) Como consecuencia del análisis de los incidentes, se revisará la determinación de los eventos auditables.	Se puso en marcha hace 2 años un gestor de incidencias informáticas. En primera instancia llega al CAU (soporte 1er nivel), en segunda instancia a nivel técnico (2ndo nivel). Tipo de incidencias: incidencias de usuarios. No hay app de incidencias de seguridad aparte. Tampoco están categorizadas. No hay nada por escrito.	No existe un aplicativo para gestión de ciberincidentes, ni protocolos de actuación al respecto.	Implantación de herramienta para el registro, la gestión y seguimiento de incidentes de seguridad de la información.	No conformidad mayor	Entrevista Auditoría;
op.ext.1	Contratación y acuerdos de nivel de servicio MEDIA: Previa a la utilización de recursos externos se establecerán contractualmente las características del servicio prestado y las responsabilidades de las partes. Se detallará lo que se considera calidad mínima del servicio prestado y las consecuencias de su incumplimiento.	Contratación está centralizado. Algunas áreas pueden realizar contrataciones informáticas por su cuenta (a través de Contratación/Patrimonio), pero sin contar con Informática). No hay requisitos de seguridad. Hay una cláusula genérica, que varía en función de que sea encargado del tratamiento, que va referida únicamente a protección de datos, confidencialidad y deber de secreto. ENS no se tiene en cuenta	No existe una normativa por escrito para la contratación de terceros para la ejecución de servicios o TIC o adquisición de productos y equipos asociados al sistema de información de Diputación. Algunos contratos relacionados con elementos del sistema de información de Diputación se gestionan de forma específica por un área o departamento determinado, sin consultar a Seguridad de la Información o Informática sobre los requisitos de seguridad y normativos	Se redactará normativa de contratación y relaciones con terceros, y procedimientos asociados. Los contratos realizados de forma no centralizada, desde cada área, se deberán comunicar al Servicio de Organización e Información:	No conformidad mayor	Entrevista Auditoría;

CONTROL	REQUISITO	SITUACIÓN ACTUAL	INCUMPLIMIENTO	CORRECCIÓN	VALORACIÓN	EVIDENCIA
op.ext.1 Continuac.	Contratación y acuerdos de nivel de servicio MEDIA: Previa a la utilización de recursos externos se establecerán contractualmente las características del servicio prestado y las responsabilidades de las partes. Se detallará lo que se considera calidad mínima del servicio prestado y las consecuencias de su incumplimiento.	Como regla general, los menores los gestiona cada Área, y las licitaciones estarían implicadas dos áreas, Servicios (Fomento) y el resto (Patrimonio). La persona que solicita el servicio/producto es el que marca los requisitos de seguridad y se convierte en el responsable posterior de la ejecución. Propiedad intelectual. Si lo considera el responsable del servicio, lo añade. En cada contrato, añaden cláusulas de encargo de tratamiento en su caso, pero no existe un inventario de encargos del tratamiento. Devolución de información. Las copias en papel deben destruirse, y se les pide certificado de destrucción. En electrónico, por ejemplo spamina, deben destruir la información a los 15 días, pero no está por contrato.	En algunos casos la información es tratada en los Ayuntamientos, y en los convenios no se especifica ningún requisito normativo o medidas mínimas de protección para mantener la seguridad de la información cuando ésta se encuentre en sus instalaciones.	- si implica contrataciones relacionadas con sistemas de información (aplicativos, servicios de comunicaciones, páginas Web, etc.), para evaluación de posibles necesidades en cuanto a definición de requisitos de seguridad y parámetros de respuesta ante posibles incidentes - y/o si implica tratamiento de datos personales, para evaluación del tercero como posible encargado del tratamiento, necesidad de adaptación de formularios, o posibles nuevos tratamientos. En los convenios con Ayuntamientos se debe indicar que éstos deberán disponer de las medidas suficientes para asegurar la protección de los datos que almacenan en sus instalaciones, relacionados con los trabajos de personal de Diputación en dichos Ayuntamientos. Se ha detectado en las entrevistas (oct19) realizadas a las áreas de Diputación, como es el caso de Servicios Sociales Comunitarios, o Igualdad y Mujeres.		

CONTROL	REQUISITO	SITUACIÓN ACTUAL	INCUMPLIMIENTO	CORRECCIÓN	VALORACIÓN	EVIDENCIA
op.ext.2	Gestión diaria MEDIA: Para la gestión diaria del sistema, se establecerán los siguientes puntos: a) Un sistema rutinario para medir el cumplimiento de las obligaciones de servicio y el procedimiento para neutralizar cualquier desviación fuera del margen de tolerancia acordado (op.ext.1); b) El mecanismo y los procedimientos de coordinación para llevar a cabo las tareas de mantenimiento de los sistemas afectados por el acuerdo; c) El mecanismo y los procedimientos de coordinación en caso de incidentes y desastres.	No se elabora ningún informe de seguimiento. Lo que se hace es validar facturación pero no hay un informe rutinario, tan solo si se detecta alguna incidencia.	No existen mecanismos para medir el cumplimiento del tercero en cuanto e requisitos de seguridad exigibles. No hay un listado formal de proveedores con información sobre protocolos en caso de fallos crítico	Elaborar un listado de proveedores relacionados con los sistemas de información de Diputación, con todos los datos necesarios que pudieran hacer falta en caso de incidencia relacionada con seguridad. Se debe disponer de forma centralizada de toda la información sobre el contrato, vigencia, condiciones de mantenimiento para cada proveedor, contacto en caso de incidencia y SLA, etc. Para contrato TIC o relacionado con los sistemas de Diputación, se debe elaborar un informe de seguimiento en el que se incluya la evaluación del proveedor en cuanto al cumplimiento de requisitos relacionados con seguridad de la información. En caso de incidencia de seguridad que afecte al proveedor, se evaluará el nivel de cumplimiento en cuanto a eficiencia en los tiempos de comunicación y respuesta, se verificará el cumplimiento de los requisitos del contrato en este sentido, y se anotarán las vulnerabilidades detectadas en los protocolos de respuesta para mejora en contratos similares.	No conformidad mayor	Entrevista Auditoría;

CONTROL	REQUISITO	SITUACIÓN ACTUAL	INCUMPLIMIENTO	CORRECCIÓN	VALORACIÓN	EVIDENCIA
op.cont.1	Análisis de Impacto MEDIO: Se realizará un análisis de impacto que permita determinar: a) Los requisitos de disponibilidad de cada servicio medidos como el impacto de una interrupción durante un cierto periodo de tiempo; b) Los elementos que son críticos para la prestación de cada servicio.	No se ha hecho nada respecto a continuidad de negocio	No se ha realizado un análisis de impacto (BIA)	Se deberá realizar un análisis de impacto en el negocio (BIA) en los sistemas categorizados como de nivel MEDIO en el ENS. Esto implica la realización de, al menos, las siguientes actividades: - Identificación de procesos críticos. - Priorización de la criticidad en función del impacto en términos de interrupción, posibles daños (económicos, impacto en la imagen, posibilidad de incumplimiento normativo, protestas y alteraciones del orden, etc.) - Establecimiento de los objetivos de recuperación para cada proceso crítico (RTO), y para cada información crítica (RPO).	No conformidad mayor	Entrevista Auditoría;

CONTROL	REQUISITO	SITUACIÓN ACTUAL	INCUMPLIMIENTO	CORRECCIÓN	VALORACIÓN	EVIDENCIA
mp.sw.2	Aceptación y puesta en servicio BÁSICA: Antes de pasar a producción se comprobará el correcto funcionamiento de la aplicación. A) Se comprobará que: Se cumplen los criterios de aceptación en materia de seguridad; No se deteriora la seguridad de otros componentes del servicio; b) Las pruebas se realizarán en un entorno aislado; c) Las pruebas de aceptación no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente. MEDIA: Se realizarán las siguientes inspecciones previas a la entrada en servicio: a) análisis de vulnerabilidades; b) pruebas de penetración. ALTA: Se realizarán las siguientes inspecciones previas a la entrada en servicio: a) análisis de coherencia en la integración en los procesos; b) se considerarán la oportunidad de realizar una auditoría de código fuente.	Pruebas. No se documentan. Hay posibilidad de marcha atrás (no por escrito). No se hace Pentesting. Auditorías técnicas de seguridad no se hacen. Una vez en producción se han realizado pen testing puntualmente (último hace dos años). Disponen de herramienta de identificación de vulnerabilidades, pero no se utilizan (el propio FW). Auditorías de código fuente: no	No se dispone de los medios ni se articulan los mecanismos y proyectos de auditoría necesarios para identificar las vulnerabilidades de los sistemas de información de Diputación	Realización periódica de pruebas de pen-testing para la identificación de vulnerabilidades Identificación de vulnerabilidades de forma previa al paso a producción (categoría media ENS). Se deberá disponer de una herramienta para la identificación de vulnerabilidades.	No conformidad mayor	Entrevista Auditoría;
mp.s.2	Protección de servicios y aplicaciones Web BAJO: Se emplearán "certificados de autenticación de sitio web" acordes a la normativa europea en la materia. ALTO: Se emplearán "certificados cualificados de autenticación del sitio web" acordes a la normativa europea en la materia.	No se utiliza en todas las páginas Web HTTPS (no se usa en la Web principal).	Algunas páginas Web de Diputación, como la Web corporativa principal, no utilizan mecanismos y protocolos seguros.	Utilización de HTTPS en todas las páginas Web de Diputación. La página principal corporativa no dispone de HTTPS. Redactar y aprobar normativa sobre protección de los servicios expuestos a Internet	No conformidad mayor	Entrevista Auditoría;

4.2 No conformidades menores

CONTROL	REQUISITO	SITUACIÓN ACTUAL	INCUMPLIMIENTO	CORRECCIÓN	VALORACIÓN	EVIDENCIA
org.4	Proceso de autorización Se establecerá un proceso formal de autorizaciones que cubra todos los elementos del sistema de información: a) utilización de instalaciones, habituales y alternativas; b) entrada de equipos en producción; c) entrada de aplicaciones en producción; d) establecimiento de enlaces de comunicación, habituales y alternativos; f) utilización de soportes de información; g) Utilización de equipos móviles (PDA, portátiles, etc.); h) Utilización de servicios de terceros	No hay nada por escrito. Se hace por la operativa del día a día. En algunos casos lo solicita el responsable del interesado y en otros el propio interesado (por ejemplo, para acceso a carpetas del servidor).	No se encuentra por escrito el proceso formal de autorización que contemple los diferentes aspectos de la seguridad de la información.	Se deberá elaborar un documento en el que se reflejen los diferentes protocolos de autorización para todos los procesos relacionados con seguridad de la información: - Acceso lógico a los sistemas (altas y bajas de usuarios en los diferentes sistemas de información) - Acceso físico a salas de servidores y CPD - Entrada de equipos y aplicaciones en producción - Uso de portátiles y móviles corporativos - Accesos en remoto - Uso de soportes de información (por ejemplo, memorias extraíbles).	No conformidad menor	Entrevista Auditoría;

CONTROL	REQUISITO	SITUACIÓN ACTUAL	INCUMPLIMIENTO	CORRECCIÓN	VALORACIÓN	EVIDENCIA
op.pl.2	Arquitectura de seguridad PUNTO CLAVE (CAT A): Sistema de gestión de la seguridad, documentado y con revisión regular por Dirección Se deberán detallar: BÁSICA: a) Documentación de las instalaciones; b) Documentación del sistema; c) Esquemas de línea de defensa; d) Sistemas de identificación y autenticación de usuarios MEDIA: e) Sistema de gestión, relativo a la planificación, organización y control de los recursos relativos a la seguridad de la información ALTA: f) Sistema de gestión de la seguridad de la información con actualización y aprobación periódica; g) controles técnicos de validación	No tienen nada.	No se dispone de un Sistema de Gestión de la Seguridad de la Información, documentado y con revisión regular por Dirección	Redactar normativa de caracterización y planificación de los sistemas, que comprenda, al menos, las normas relativas a identificación e inventario de activos, arquitectura de Seguridad, gestión del Riesgo, y planificación, dimensionado y gestión de capacidades. Se debe elaborar la descripción técnica de las instalaciones, sistemas de información, redes de comunicaciones, y sistemas de identificación y autenticación de usuarios. Se debe disponer de un documento de cuadro de mando o aplicativo donde se refleje cómo se realizan los procesos relativos a seguridad, con referencia a las normativas y procedimientos asociados. Por ejemplo, altas y bajas de usuarios, autorización para acceso en remoto, autorización para acceso a CPD, entrada en producción de nuevo aplicativo, etc.	No conformidad menor	Entrevista Auditoría;

CONTROL	REQUISITO	SITUACIÓN ACTUAL	INCUMPLIMIENTO	CORRECCIÓN	VALORACIÓN	EVIDENCIA
op.pl.3	Adquisición de nuevos componentes Se establecerá un proceso formal para planificar la adquisición de nuevos componentes del sistemas: a) atenderá a las conclusiones del análisis de riesgos; b) será acorde a la arquitectura de seguridad escogida; c) contemplará las necesidades técnicas, de formación y de financiación de forma conjunta	No hay nada. Nada sobre requisitos de seguridad	Ausencia de proceso formal para la adquisición de nuevos productos o servicios relacionados con los sistemas de información. No se definen requisitos de seguridad a la hora de adquirir nuevos elementos del sistema de información.	Redactar normativa de caracterización y planificación de los sistemas, que comprenda, al menos, las normas relativas a inventario de activos, arquitectura de Seguridad, gestión del Riesgo, y dimensionado y gestión de capacidades. Redactar normativa y procedimiento para la adquisición de nuevos productos y sistemas relacionados con las TIC y los Sistemas de Información de la Diputación. Debe reflejar, al menos, los requisitos de seguridad para: - el diseño de nuevas app - la adquisición de nuevos productos y sistemas TI	No conformidad menor	Entrevista Auditoría;
op.acc.3	Segregación de funciones y tareas El sistema de control de acceso se organizará de forma que se exija la concurrencia de dos o más personas para realizar tareas críticas, anulando la posibilidad de que un solo individuo autorizado, pueda abusar de sus derechos para acometer alguna acción ilícita. Se separarán al menos las funciones: a) desarrollo de operación; b) Configuración y mantenimiento del sistema de operación; c) Auditoría o supervisión de cualquier otra función	No hay matriz de segregación de funciones y tareas.	No se realiza la segregación de funciones y tareas	Elaborar un procedimiento para la evaluación de la segregación de funciones y tareas. Debe determinarse la matriz de compatibilidad o de segregación que se aplicará entre todos los roles (administradores sistemas, comunicaciones, desarrolladores, administradores BBDD, administradores de seguridad, etc.), definidos en Diputación relacionados con los sistemas de información.	No conformidad menor	Entrevista Auditoría;

CONTROL	REQUISITO	SITUACIÓN ACTUAL	INCUMPLIMIENTO	CORRECCIÓN	VALORACIÓN	EVIDENCIA
op.acc.4	Proceso de gestión de derechos de acceso Los derechos de acceso de cada usuario se limitarán atendiendo a: a) Mínimo privilegio; b) Necesidad de conocer; c) Capacidad de autorizar (solo el personal con competencia para ello, podrá conceder, alterar o anular la autorización de acceso a los recursos)	Alta de usuario. Son los propios responsables los que solicitan el alta, pero no para las bajas. Existe un procedimiento a nivel interno para las altas de usuarios. El alta se solicita a través de la Intranet mediante un aplicativo específico (usuarios Diputación y usuarios de EELL). Se le da un usuario de la Red Provincial de Comunicaciones (acceso a buzón de correo, Internet Corporativo). A los usuarios de Diputación además se les de alta en Active Directory más las carpetas a las que se le da acceso por Departamento. Ese mismo usuario se utiliza para dar de alta en carpetas compartidas y acceso a las aplicaciones por Departamento.	No existen procesos definidos para las bajas de usuarios, y para las bajas de cuentas y aplicaciones en los cambios de puesto de trabajo.	Redactar normativa y procedimientos asociados, relativa al control de acceso y gestión de cuentas, que comprenda al menos lo siguiente: - Asignación de privilegios de acceso y revisión de los mismos - Proceso de alta, baja, modificación o bloqueo de cuentas - Política de asignación de contraseñas, robustez y periodicidad de cambio - Autorizaciones para el acceso a los sistemas de información en local y en remoto. Se debe realizar una revisión periódica de las cuentas de usuario, para verificar y eliminar las cuentas de usuarios dados de baja, y eliminar accesos de usuarios que hayan cambiado su rol, o puesto de trabajo y sigan manteniendo acceso a aplicaciones que ya no utilicen, todo en base a las normativa de control de acceso y el procedimiento de alta, baja y modificación de cuentas de usuario.	No conformidad menor	Entrevista Auditoría;

CONTROL	REQUISITO	SITUACIÓN ACTUAL	INCUMPLIMIENTO	CORRECCIÓN	VALORACIÓN	EVIDENCIA
op.acc.5	Mecanismos de autenticación BAJO: a) Se admitirá el uso de cualquier mecanismo de autenticación sustentado en un solo factor b) Si es "algo que se sabe" se aplicarán reglas básicas de calidad de las misma c) Las credenciales se activarán una vez estén bajo el control efectivo del usuarios; estarán bajo el control exclusivo del usuario; el usuario reconocerá que las ha recibido y que conoce y acepta las obligaciones que implica su tenencia; se cambiarán con una periodicidad; se retirarán y serán deshabilitadas cuando la entidad que autentican termine su relación con el sistema MEDIO: a) Se exigirá el uso de al menos 2 factores de autenticación; b) en el caso de contraseña serán rigurosas de calidad y renovación; c) las credenciales deberán haber sido obtenidas tras un registro previo (presencial, telemático usando certificado, telemático tras certificado) ALTO: a) Las credenciales se suspenderán tras un periodo definido de no utilización; b) En el caso de "algo que se tiene", se requerirá el uso de elementos criptográficos hardware; c) las credenciales habrán sido obtenidas tras un registro previo presencial o temático usando certificado electrónico.	Autenticación mediante usuario/contraseña, y mediante firma digital (por ejemplo, portafirmas o tramitador). Control de fichajes: biométrico. Robustez mínima: más de 8 con caracteres especiales; las 10 últimas no se pueden utilizar; El sistema no te deja poner contraseñas sin estas exigencias. PWD Administración y Configuración: se exige la misma robustez. No hay doble factor de autenticación. No hay bloqueo de usuarios por intentos fallidos consecutivos.	No hay implantado un sistema de doble factor de autenticación en los sistemas de nivel MEDIO del ENS. La política de uso de contraseñas de Diputación no está por escrito.	Implantar doble factor de autenticación en las aplicaciones y sistemas que así lo requieran: - Aplicativos y sistemas de categoría MEDIA en el ENS - Aplicativos y sistemas que operen con datos personales de categoría especial Verificar que todas las aplicaciones cumplen con los requisitos de fortaleza de contraseñas definidos en las normas y procedimientos asociados, así como con los requisitos de periodicidad de cambio. Redactar y aprobar un procedimiento de Asignación, Distribución y Almacenamiento de Contraseñas.	No conformidad menor	Entrevista Auditoría;

CONTROL	REQUISITO	SITUACIÓN ACTUAL	INCUMPLIMIENTO	CORRECCIÓN	VALORACIÓN	EVIDENCIA
op.acc.6	Acceso local Acceso local: realizado desde puestos de trabajo en las instalaciones de la organización. BAJO: a) Se prevendrán ataques que puedan revelar información del sistema sin llegar a acceder al mismo; b) el número de intentos permitidos será limitado, bloqueando la oportunidad de acceso una vez efectuados un cierto número de fallos consecutivos; c) Se registrarán los accesos con éxito, y los fallidos; d) el sistema informará al usuario de sus obligaciones inmediatamente después de obtener el acceso MEDIO: Se informará al usuario de su último acceso efectuado con su identidad ALTO: a) El acceso estará limitado por horario, fechas y lugar desde donde se accede; b) Se definirán puntos en los que el sistema requerirá una renovación de la autenticación del usuario.	No se registran los accesos fallidos y exitosos a nivel genérico. Los accesos a app a través de certificado sí generan logs de acceso. No se bloquea la cuenta por intentos fallidos consecutivos. No se muestra información al usuario Salvo caso aislado no te informan sobre los últimos accesos ni sobre los intentos fallidos. No se limita el acceso por fechas/horas.	No se bloquea la cuenta por intentos fallidos consecutivos a los diferentes sistemas y aplicaciones. No se muestra información al usuario cuando accede a los sistemas de información de la Diputación. No se informa al usuario los sistemas de nivel MEDIO sobre los últimos accesos (fecha y hora) ni sobre los intentos fallidos.	Se debe bloquear al usuario tras varios intentos fallidos de acceso consecutivos. El número de intentos deberá estar definido en las normativas de control de acceso y políticas sobre uso seguro de contraseñas. Para los Sistemas de categoría MEDIA en el ENS, se deberá mostrar información sobre fecha y hora del último o últimos accesos, así como información sobre los intentos fallidos de acceso. Se deberán registrar los accesos con éxito y los accesos fallidos a los diferentes sistemas de información. Los diálogos de acceso a los Sistemas de la Diputación deben prevenir sobre el acceso y el correcto uso de los mismos y las obligaciones del usuario. Asimismo, no deben revelar información confidencial, únicamente la indispensable.	No conformidad menor	Entrevista Auditoría;

CONTROL	REQUISITO	SITUACIÓN ACTUAL	INCUMPLIMIENTO	CORRECCIÓN	VALORACIÓN	EVIDENCIA
op.exp.1	Inventario de activos Se mantendrá un inventario actualizado de todos los elementos del sistema, detallando su naturaleza e identificando a su responsable; es decir, la persona que es responsable de las decisiones relativas al mismo	Hay una herramienta de inventario para equipos. Se refleja la ubicación, pero no hay historial, ni información técnica. App: hay un inventario "casero". No hay información cuando un equipo cambia de ubicación. Servidores: misma filosofía, hay un inventario patrimonial, pero sin información técnica. Software: está inventariado, sin información técnica.	No existe un inventario de activos de información que se mantenga actualizado y en el que se refleje el responsable de cada uno de dichos elementos.	Se dispondrá de un inventario de activos de información permanentemente actualizado, en el que se identifique la ubicación, el responsable de cada activo, y los diferentes cambios y actuaciones sobre los mismos. Deberá comprender, al menos: -Aplicaciones SW -Equipos HW -Dispositivos de Red -Dispositivos Móviles Corporativos -Equipos Portátiles -Soportes en su caso (memorias extraíbles) -Relación de personal, que permita asignar responsables de los diferentes sistemas de información o usuarios que interaccionen con los mismos.	No conformidad menor	Entrevista Auditoría;

CONTROL	REQUISITO	SITUACIÓN ACTUAL	INCUMPLIMIENTO	CORRECCIÓN	VALORACIÓN	EVIDENCIA
op.exp.2	Configuración de seguridad Se configurarán los equipos previamente a su entrada en operación de manera que: a) Se retiren cuentas y contraseñas estándar; b) Se apliquen reglas de "mínima seguridad"; c) se aplicarán reglas de "seguridad por defecto"	. - Equipos de usuario: se dispone de un AV corporativo con actualizaciones periódicas. Se instala en todos los casos, el usuario no puede desconfigurarlo. Parches: se comprueba de forma diaria - Equipos de sistemas: contraseñas de ciertos servidores puede ser conocida por varios usuarios. Dispositivos de red: restringido a ciertos administradores. FW si se cambia la contraseña por defecto, el resto de dispositivos no se cambia, pero se tiene configurado para que no se pueda acceder directamente.	Existen dispositivos en los que no se modifica la contraseña por defecto. Las contraseñas de algunos equipos son conocidas por varios usuarios. Se recomienda que los usuarios no sean administradores de sus propias máquinas, y que así se refleje en las diferentes políticas y normativas relacionadas con el control de acceso a los sistemas de información y la asignación de privilegios.	Se deben retirar las contraseñas por defecto de todos los dispositivos de red. Las contraseñas de acceso a los servidores deben ser conocidas únicamente por los usuarios que lo necesiten para el desempeño de sus funciones (revisión regla de funcionalidad y privilegios mínimos). Se dispondrá de una normativa de explotación, y de procedimientos específicos de bastionado de los sistemas previo a su entrada en producción, en el que se deberá reflejar al menos: - se retiran las cuentas por defecto - funcionalidad mínima para el objetivo del sistema o aplicación - requisitos mínimos de seguridad previos a la entrada en explotación	No conformidad menor	Entrevista Auditoría;

CONTROL	REQUISITO	SITUACIÓN ACTUAL	INCUMPLIMIENTO	CORRECCIÓN	VALORACIÓN	EVIDENCIA
op.exp.6	Se dispondrá de mecanismos de prevención y reacción frente a código dañino con mantenimiento de acuerdo a las recomendaciones del fabricante	Medidas frente a código dañino: no existen. En las aplicaciones web, bajo Windows, está asegurado mediante end point. Equipos de usuario: se dispone de un AV corporativo con actualizaciones periódicas. Se instala en todos los casos, el usuario no puede desconfigurarlo. Parches: se comprueba de forma diaria.	No existen procedimientos por escrito que contengan los mecanismos preventivos y reactivos de protección frente a malware. Ausencia de aplicativo anti malware	Se debe redactar y aprobar un procedimiento de protección frente a código dañino, que contemple al menos: - Tipos de malware y medidas de protección - Medidas preventivas - Medidas reactivas Se dispondrá de una herramienta anti malware contra código dañino, capaz de detectar diferentes tipos de malware y actuar según el caso. - BBDD de malware actualizada regularmente - Revisión de cada aplicación al arranque - Bloqueo de acceso a sitios web maliciosos (black lists) - Revisión de los archivos adjuntos recibidos y descargados relativos al sistema de correo electrónico - Comprobación de existencia de malware desde diferentes puntos de la red	No conformidad menor	Entrevista Auditoría;

CONTROL	REQUISITO	SITUACIÓN ACTUAL	INCUMPLIMIENTO	CORRECCIÓN	VALORACIÓN	EVIDENCIA
op.exp.8	Registro de la actividad de los usuarios Se registrarán las actividades de los usuarios en el sistema de forma que: a) El registro indicará quién realiza la actividad, cuándo la realiza y sobre qué información; b) Se incluirá la actividad de los usuarios y, especialmente, la de los operadores y administradores en cuanto puedan acceder a la configuración y actuar en el mantenimiento del sistema; c) Deberán registrarse las actividades realizadas con éxito y los intentos fracasados; d) La determinación de qué actividades deben registrarse y con qué nivel de detalle se adoptará a la vista del análisis de riesgos realizado sobre los sistemas. BAJO: Se activarán los registros de los servidores MEDIO: Se revisarán informalmente los registros de actividad buscando patrones anormales ALTO: Se dispondrá de un sistema automático de recolección de registros y correlación de eventos; es decir, una consola de seguridad centralizada.	En algunas apps críticas se registran los accesos y las acciones realizadas. Se guarda registro del acceso a las aplicaciones ubicadas en la Intranet de cada usuario. Después, a nivel interno de cada app, depende de la app. Documentos. Hay trazabilidad a documentos en Alfresco. Servidores. No están activas las auditorías. Los logs por defecto no se revisan. Los logs de acceso a app se revisan a posteriori si hay algún problema.	No se activan las auditorías para el registro de los usuarios en la mayoría de aplicativos para asegurar la trazabilidad de la información. No se revisan los logs de manera preventiva.	Activación de los registros de auditoría en los servidores y aplicaciones críticas para propiciar la trazabilidad de la información en todos los casos. Se deberán realizar copias de seguridad de los logs. Revisión de los registros de auditoría para la detección de patrones anómalos	No conformidad menor	Entrevista Auditoría;

CONTROL	REQUISITO	SITUACIÓN ACTUAL	INCUMPLIMIENTO	CORRECCIÓN	VALORACIÓN	EVIDENCIA
mp.if.1	Áreas separadas con control de acceso El equipamiento se instalará en áreas separadas específicas para su función. Se controlarán los accesos a las áreas indicadas de forma que sólo se pueda acceder por las entradas previstas y vigiladas	Existen dos centros de procesamientos de datos. El central está en Navarro Rodrigo, con acceso a través de huella, y el secundario de Rambla Alfareros (lo lleva mediante Seguridad, a través de llave), y está previsto que sea a través de huella. En el Palacio también hay gestión de llaves. La empresa de Seguridad lleva la gestión de llaves a nivel de cada edificio, y Mantenimiento dispone de todas las llaves. Palacio tiene seguridad 24 h. En el CPD de Rambla Alfareros no hay, pero en el propio edificio sí. Tampoco CCTV dentro del CPD (sí en los accesos a los edificios).	Ausencia de mecanismos de control de accesos a los dos edificios donde se ubican los CPD, y medios para la identificación, registro y acreditación de visitas. Ausencia de normativa y procedimientos relativos al control de acceso al CPD	Redactar y aprobar normativa de seguridad física y procedimiento asociado de control de acceso al CP Implantación de un sistema de control de accesos al edificio principal de Diputación (donde se ubica el CPD principal), y al edificio ubicado en Rambla Alfareros, donde se ubica el CPD secundario. Se deberá identificar y acreditar a los visitantes que acceden a ambos edificios donde se ubican los CPD. El protocolo de visitas (identificación, registro y acreditación), se ceñirá a los estipulado en los procedimientos de seguridad física y acceso al CPD.	No conformidad menor	Entrevista Auditoría;
mp.if.6	Protección frente a inundaciones MEDIO: Los locales donde se ubiquen los sistemas de información y sus componentes se protegerán frente a incidentes fortuitos o deliberados causados por el agua.	Navarro Rodrigo. Está en planta primera y N/A. No hay núcleos de tuberías. Rambla Alfareros. Está sótano y tiene cerca baños. En el sótano hay una arqueta con una boya de extracción con bomba de achique. Esta medida no fue suficiente, ya que hubo una inundación el año pasado. Se ha elevado 20 cm respecto a la rasante del suelo.	Ausencia de medidas contra inundación suficientes en la sala de CPD ubicada en Rambla Alfareros	Implantación de medias contra inundación en el CPD de Rambla Alfareros (CPD Secundario)	No conformidad menor	Entrevista Auditoría;

CONTROL	REQUISITO	SITUACIÓN ACTUAL	INCUMPLIMIENTO	CORRECCIÓN	VALORACIÓN	EVIDENCIA
mp.if.7	Registro de entrada y salida de equipamiento Se llevará un registro pormenorizado de toda entrada y salida de equipamiento, incluyendo la identificación de la persona que autoriza el movimiento.	Registro como tal no hay, para consultar cuántos equipos hay fuera de las instalaciones. Salida de portátiles: al asignarse un portátil se rellena un documento, Para teléfono sí hay una BBDD para consultar qué modelos ha tenido cada persona y qué modelo tiene actualmente.	No existe un registro de entrada y salida de equipamiento.	A través del sistema implantado para gestión del inventario, se deberán registrar las actuaciones para cada uno de los elementos, incluyendo los registros de las entradas y salidas de equipamiento (PC's, Servidores, HW, equipos de red)	No conformidad menor	Entrevista Auditoría;
mp.per.1	Caracterización del puesto de trabajo MEDIA: Cada puesto de trabajo se caracterizará de la siguiente forma: a) Se definirán las responsabilidades relacionadas con cada puesto de trabajo en materia de seguridad. La definición se basará en el análisis de riesgos; b) Se definirán los requisitos que deben satisfacer las personas que vayan a ocupar el puesto de trabajo, en particular, en términos de confidencialidad; c) Dichos requisitos se tendrán en cuenta en la selección de la persona que vaya a ocupar dicho puesto, incluyendo la verificación de sus antecedentes laborales, formación y otras referencias.	Actualmente no hay diferenciación en responsabilidad en materia de seguridad.	No se definen los requisitos de seguridad y responsabilidades en materia de seguridad de la información en los puestos de trabajo de Diputación.	Caracterización de cada puesto de trabajo, incluyendo al menos: - Responsabilidades en materia de seguridad. Se realizará en función del análisis de riesgos, y de la criticidad de la información manejada en el puesto de trabajo; Requisitos de las personas en materia de seguridad, en función de la relevancia del puesto, de las funciones que se deben desempeñar (si están relacionadas con seguridad de la información, con administración de la seguridad, etc.), y de la información manejada (sensibilidad de los datos, confidencialidad). Los requisitos de seguridad para el puesto de trabajo se tendrán en cuenta en los procesos de selección. Redactar y aprobar normativa relativa a la gestión segura desde RRHH	No conformidad menor	Entrevista Auditoría;

CONTROL	REQUISITO	SITUACIÓN ACTUAL	INCUMPLIMIENTO	CORRECCIÓN	VALORACIÓN	EVIDENCIA
mp.per.2	Deberes y obligaciones Se informará a cada persona que trabaje en el sistema, de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad: a) especificando las medidas disciplinarias; b) se cubrirá tanto el periodo durante el cual se desempeña el puesto, las obligaciones en caso de término de la asignación, o traslado a otro puesto de trabajo; c) Se contemplará el deber de confidencialidad respecto de los datos a los que tenga acceso, tanto durante el periodo que estén adscritos al puesto de trabajo, como posteriormente a su terminación. En caso de personal contratado a través de un tercero: a) Se establecerán los deberes y obligaciones del personal; b) Se establecerán los deberes y obligaciones de cada parte; c) Se establecerá el procedimiento de resolución de incidentes relacionados con el incumplimiento de las obligaciones.	Se proporciona al personal contratado y a miembros de tribunal (oposiciones) un escrito relacionado con la confidencialidad y deber de secreto; Nada de cumplimiento normativo ni de Políticas de Seguridad; Teléfonos - Patrimonio; Informática - PC y Portátiles; No hay nada sobre buen uso de medios tecnológicos; En general, no hay "protocolo de bienvenida"; Altas: inicia el protocolo el responsable del usuario y Personal solicita a Informática la acreditación. Bajas: no está protocolizado de forma regular;	El personal de Diputación no firma un documento que contenga los deberes y obligaciones respecto al buen uso de los medios tecnológicos puestos a su disposición para el correcto desempeño de sus funciones. No existe un manual, guía o normativa con mejores prácticas para el buen uso de medios tecnológicos.	El personal que trabaje con los sistemas de información de Diputación deberá firmar un documento de deberes y obligaciones relativos al buen uso de los sistemas puestos a su alcance para el desempeño de sus funciones, al cumplimiento de la Política de Seguridad y Normativas asociadas, y a la devolución de los activos que se le hubieran proporcionado. Redactar y aprobar una normativa relativa al buen uso de los medios tecnológicos, que incluya al menos las principales normas para una correcta utilización de: - Correo Electrónico - Navegación por Internet - Firma Digital - Uso de impresoras en red - Ordenadores y puesto de trabajo - Memorias Extraíbles	No conformidad menor	Entrevista Auditoría;

CONTROL	REQUISITO	SITUACIÓN ACTUAL	INCUMPLIMIENTO	CORRECCIÓN	VALORACIÓN	EVIDENCIA
mp.per.3	Concienciación Se realizarán las acciones necesarias para concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos. En particular, se acordará: a) La normativa de seguridad relativa al buen uso de los sistemas; b) La identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado; c) El procedimiento de reporte de incidentes de seguridad, sean reales o falsas alarmas	Concienciación. En materia de protección de datos se reciben circulares periódicas con instrucciones concretas. También se organizaron reuniones con los distintos servicios para analizar el tema de transparencia y RGPD.	El personal de Diputación desconoce el Esquema Nacional de Seguridad y no está concienciado respecto a las medidas de seguridad necesarias para proteger la información	Se deberán poner en marcha acciones que permitan la concienciación en materia de seguridad de la información, al menos algunas de las siguientes: - Envío periódico de circulares que incluyan las principales novedades lanzadas por la AEPD para protección de datos personales como por parte del CCN y/o INCIBE, para la seguridad de la información y el ENS. - Publicación en el Blog de las novedades citadas anteriormente, así como de las principales noticias que afecten tanto a la seguridad de la información como a la protección de datos personales. - Charlas periódicas en las diferentes Áreas de Diputación por parte del personal de Seguridad de la Información y Protección de Datos Personales - Envío de las actualizaciones de normativas y procedimientos de seguridad a cada área afectada - Diseño de díptico para los responsables de área de Diputación, en el que se muestren sus principales funciones relacionadas con seguridad de la información y protección de datos personales.	No conformidad menor	Entrevista Auditoría;

CONTROL	REQUISITO	SITUACIÓN ACTUAL	INCUMPLIMIENTO	CORRECCIÓN	VALORACIÓN	EVIDENCIA
mp.per.3 Continuac.	Concienciación Se realizarán las acciones necesarias para concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos. En particular, se acordará: a) La normativa de seguridad relativa al buen uso de los sistemas; b) La identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado; c) El procedimiento de reporte de incidentes de seguridad, sean reales o falsas alarmas	Tanto la formación y la concienciación se han centrado más en RGPD que en ENS.	El personal de Diputación desconoce el Esquema Nacional de Seguridad y no está concienciado respecto a las medidas de seguridad necesarias para proteger la información	- Envío de circulares que prevengan de diferentes campañas de ataques, especialmente las relacionadas con ingeniería social (phising, vishing, smishing). En caso de detección de ataque, se deberá enviar información a toda la organización para que puedan estar alerta respecto al tipo de ataque (por ejemplo, entrada de un correo electrónico malicioso), incluyendo además los pasos a seguir por los usuarios para obrar de forma correcta, tanto si han recibido un intento de ataque, como si han sido víctimas del mismo. .- Acciones formativas específicas para los responsables de área, centradas en los aspectos del apartado anterior. - Acciones formativas genéricas ENS, y LOPDgdd/RGPD		
mp.per.4	Formación Se formará regularmente al personal en aquellas materias que requieran para el desempeño de sus funciones, en particular en lo relativo a: a) Configuración de sistemas; b) Detección y reacción de incidentes; c) Gestión de la información en cualquier soporte (almacenamiento, transferencia, copias, distribución...)	Plan de formación. Abarca todas las áreas de la casa dentro del Plan Agrupado Dip/Ayunt, en función de las necesidades cada Servicio, de forma genérica ENS y RGPD. No de forma planificada junto con Formación; En Protección de Datos se hizo un curso para las jefaturas en 2018.	No se realiza un análisis de las necesidades formativas en materia de seguridad de la información por cada área de Diputación	Cada Área de Diputación debe definir las necesidades de formación en materia de seguridad, específica de cada puesto de trabajo (formación genérica, formación técnica de seguridad, formación para alta dirección, formación específica sobre administración de seguridad y vulnerabilidades técnicas, etc.).	No conformidad menor	Entrevista Auditoría;

CONTROL	REQUISITO	SITUACIÓN ACTUAL	INCUMPLIMIENTO	CORRECCIÓN	VALORACIÓN	EVIDENCIA
mp.eq.1	Puesto de trabajo despejado BÁSICA: Se exigirá que los puestos de trabajo permanezcan despejados, sin más material encima de la mesa que el requerido para la actividad que se está realizando en cada momento MEDIA: Este material se guardará en lugar cerrado cuando no se esté utilizando.	No hay política de mesas limpias	No hay política de mesas limpias	Redactar, aprobar e implantar una política de mesas limpias.	No conformidad menor	Entrevista Auditoría;
mp.eq.3	Protección de portátiles BASICO: Los equipos que deban salir de las instalaciones serán protegidos adecuadamente. Se adoptarán las medidas siguientes: a) Se llevará un inventario de equipos portátiles junto con una identificación de la persona responsable del mismo y un control regular de que está positivamente bajo su control; b) Se establecerá un canal de comunicación para informar de pérdidas o sustracciones; c) Cuando se conecte remotamente a través de redes distintas al control de la red de la organización, se limitará el ámbito de operación a los mínimos imprescindibles, requiriendo autorización previa de los responsables de la información y los servicios afectados; d) Se evitará, en la medida de lo posible, que el equipo contenga claves de acceso remoto a la organización. ALTA: a) Se dotará al dispositivo de detectores de violación que permitan saber el equipo ha sido manipulado y activen los procedimientos previstos	Los equipos portátiles de servicios sociales están encriptados. Los portátiles se pueden sacar fuera de la Diputación. No hay protocolo para perdida de portátiles. Av en todos los portátiles. No se hace un análisis de qué información se va a manejar en cada portátil.	No se ha establecido un canal de comunicación para informar de pérdidas o sustracciones.	Redactar y aprobar normativa de uso de equipos portátiles. Dicha Normativa debe reflejar, al menos: - Proceso de autorización para uso de portátil - Proceso de autorización para utilización del portátil fuera de las instalaciones de Diputación - Securización mínima del portátil. Estudio de necesidades de cifrado en determinados casos (datos sensibles) - Acciones permitidas y no permitidas para los usuarios (uso de USB en el portátil, instalación de aplicaciones, administración y configuración, etc.) - Protocolo a seguir por el usuario en caso de pérdida o sustracción	No conformidad menor	Entrevista Auditoría;

CONTROL	REQUISITO	SITUACIÓN ACTUAL	INCUMPLIMIENTO	CORRECCIÓN	VALORACIÓN	EVIDENCIA
mp.com.3	Protección de la Autenticidad y de la Integridad BAJO: a) Se asegurará la autenticidad del otro extremo de un canal de comunicaciones antes de intercambiar información (op.acc.5); b) Se prevendrán ataques activos, garantizando que al menos serán detectados y se activarán los procedimientos previstos de tratamiento del incidentes; c) Se aceptará cualquier mecanismo de autenticación de los previstos en la normativa de aplicación MEDIO: a) Se emplearán redes privadas virtuales cuando la comunicación discurra por redes fuera del propio dominio de seguridad; b) Se emplearán algoritmos acreditados por el CCN; c) Se aceptará cualquier mecanismo de autenticación de los previstos en las normativa de aplicación. En caso de claves concertadas se utilizarán exigencias medias de calidad de las contraseñas. ALTO: a) Se valorará el empleo de dispositivos hardware en el establecimiento y utilización de la red VPN; b) Se emplearán productos certificados conforme a lo establecido en op.pl.5; c) Se aceptarán cualquier mecanismo de autenticación de los previstos en normativa de aplicación. En caso de claves concertadas se aplicarán exigencias altas en cuanto a su calidad.	Se asegura la autenticidad, pero sin procedimiento formal. Medidas específicas contra la integridad no se aplican.	No se utilizan mecanismos para la prevención de ataques activos en los diferentes canales de comunicaciones.	Se debe asegurar la autenticación del otro extremo del canal antes de intercambiar información alguna. Además, se deben utilizar de mecanismos para la prevención de ataques activos (alteración de la información en tránsito, inyección de información espuria, secuestro de la sesión por terceras partes, etc.) en todos los canales de comunicación utilizados y, en caso de ocurrir, su detección con la consiguiente activación de los procedimientos previstos de tratamiento del incidente	No conformidad menor	Entrevista Auditoría;

CONTROL	REQUISITO	SITUACIÓN ACTUAL	INCUMPLIMIENTO	CORRECCIÓN	VALORACIÓN	EVIDENCIA
mp.si.2	Criptografía Aplicable a dispositivos removibles, CD, DVD, USB. MEDIO: Se aplicarán mecanismos criptográficos que garanticen la confidencialidad y la integridad de la información contenida ALTO: a) Se emplearán algoritmos acreditados por el CCN; b) Se emplearán productos certificados conforme a lo establecido en op.pl.5	No disponen de una AC reconocida. Se emiten certificados de admin lotus a nivel provincial (firma acordada entre Diputación y EELL). No son reconocidos, aunque tienen validez. Cifrado: los portátiles de servicios sociales. No se hace un análisis de qué información se va a manejar en cada portátil u otros soportes.	No se ha realizado un análisis de la necesidad de cifrado de los portátiles en función de la información que puedan contener.	Análisis de necesidad de cifrado de soportes de información en función de la información contenida (sensibilidad, confidencialidad, criticidad), e implantación de las medidas criptográficas que se determinen.	No conformidad menor	Entrevista Auditoría;
mp.si.3	Custodia Se aplicará la debida diligencia y control a los soportes de información que permanecen bajo la responsabilidad de la organización mediante las siguientes actuaciones: a) Garantizando el control de acceso con medidas físicas y/o lógicas; b) Garantizando que se respetan las exigencias de mantenimiento del fabricante, en especial, en lo referente a temperatura, humedad y otros agresores medioambientales.	Las copias de seguridad se almacenan en los propios CPD. Archivo de Oficina. Los expedientes están en los archivos de oficina y a los 5 años pasa al Archivo General donde la custodia es de Archivo. La Conservación es permanente, y allí se etiqueta y se clasifica (hay documentos de acceso general y otro de acceso confidencial). Los archivos de oficina pueden ser gestionados por negociado/sección y servicio.	Diputación no dispone de un Archivo Electrónico para el almacenamiento de documentación y expedientes electrónicos. No se ha realizado un análisis de espacios para saber qué áreas/departamentos no cuentan con armarios u otros medios necesarios para custodiar la información en papel.	Implantación de un archivo electrónico. Todas las áreas de Diputación deben disponer de armarios suficientes para almacenar la documentación de trabajo diario e intermedia (previa a Archivo) de forma adecuada y con los mecanismos adecuados que permitan almacenar la información de forma segura. En las entrevistas a las áreas de Diputación (oct19) se han detectado algunos casos: - Contratación. El archivo intermedio y los armarios no se cierran bajo llave	No conformidad menor	Entrevista Auditoría;

CONTROL	REQUISITO	SITUACIÓN ACTUAL	INCUMPLIMIENTO	CORRECCIÓN	VALORACIÓN	EVIDENCIA
mp.si.5	Borrado y destrucción BAJO: a) Los soportes que vayan a ser reutilizados para otra información o liberados a otra organización serán objeto de un borrado seguro de su contenido. MEDIO: b) Se destruirán de forma segura los soportes en los siguientes casos: Cuando la naturaleza del soporte no permite un borrado seguro; cuando así lo requiera el procedimiento asociado al tipo de información contenida. c) Se emplearán productos certificados.	Todo lo electrónico se mantiene de forma indefinida de momento. Borrado de discos duros: se formatea el PC y se instala de nuevo el SO. Hay formateo con más rigor en el caso de donaciones de PC. ARCHIVO. Se destruyen series documentales, pero depende de la Comisión de Valoración, indicando número de caja, etc. También hay una destructora grande de papel. OFICINAS. Hay una destructora de papel, pero no hay protocolo ni control. No hay destrucción a través de empresa tercera de información más sensible.	No se ha realizado un análisis para conocer qué áreas no cuentan con destructora de papel, necesaria para el proceso de destrucción de la información de forma segura. No existe un procedimiento para el borrado/destrucción de información.	Identificar las áreas de Diputación que no cuentan con destructora de papel. Ya sea de forma centralizada, o específicamente desde dichas áreas, se deberá proceder a la implantación de destructora de papel en las áreas que no disponen de ella (o que la destructora más cercada se encuentra demasiado alejadas de la zona de trabajo). En las reuniones con las áreas (oct19) se han identificado algunos casos: atención residencial a personas mayores. Utilizan la destructora de Archivo, pero no tienen ninguna cerca. Redacción de normativa de gestión de soportes y procedimientos asociados, que contengan al menos: - Inventariado de soportes - Etiquetado y Almacenamiento - Criptografía - Traslado - Destrucción	No conformidad menor	Entrevista Auditoría;

CONTROL	REQUISITO	SITUACIÓN ACTUAL	INCUMPLIMIENTO	CORRECCIÓN	VALORACIÓN	EVIDENCIA
mp.sw.1	Desarrollo de aplicaciones MEDIA: a) El desarrollo de aplicaciones se realizará sobre un sistema diferente y separado del de producción, no debiendo existir herramientas o datos de desarrollo en el entorno de producción; b) Se aplicará una metodología de desarrollo reconocida que: Tome en consideración los aspectos de seguridad a lo largo de todo el ciclo de vida; Trate específicamente los datos usados en pruebas; Permita la inspección de código fuente; Incluya normas de programación segura; c) Los siguientes elementos serán parte integral del diseño del sistema: Los mecanismos de identificación y autenticación; los mecanismos de protección de la información tratada; la generación y tratamiento de pistas de auditoría; d) las pruebas anteriores a la implantación o modificación de los sistemas de información no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente.	Se establecen algunas medidas: autenticación de usuario, no hay diferentes usuarios de acceso en base a roles; Hay un entorno separado pero dentro del mismo segmento de red; Hay distinción de acceso en cuanto a desarrollo.	Ausencia de normativa de gestión segura del SW	Redactar y aprobar normativa relativa a seguridad de aplicaciones y SW, y procedimientos asociados. Deberá contener al menos: - Control del SW existente - Desarrollo de aplicaciones (formación necesaria, contratos, entornos de desarrollo, metodología de desarrollo segura) - Adquisición de SW - Pruebas y aceptación - Repositorio de SW - Retirada de SW - Gestión de vulnerabilidades técnicas	No conformidad menor	Entrevista Auditoría;

CONTROL	REQUISITO	SITUACIÓN ACTUAL	INCUMPLIMIENTO	CORRECCIÓN	VALORACIÓN	EVIDENCIA
mp.info.2	Calificación de la información BAJO: .- Para calificar la información se estará a lo establecido legalmente sobre la naturaleza de la misma .- La Política de Seguridad establecerá quién es el responsable de cada información manejada por el sistema y recogerá, directa o indirectamente, los criterios que determinen el nivel de seguridad requerido .- El responsable de cada info en cada momento tendrá en exclusiva la potestad de modificar el nivel de seguridad requerido. MEDIO: Se redactará los procedimientos necesarios que describan, en detalle, la forma en que se ha de etiquetar y tratar la info en consideración al nivel de seguridad que requiere y precisando cómo se ha de realizar: a) Su control de acceso; b) Su almacenamiento; c) la realización de copias; d) el etiquetado de soportes; e) su transmisión telemática.	No existe una normativa de clasificación de la información	No existen mecanismos ni protocolos para clasificar la información, ni se han analizado los criterios para poderlo llevar a cabo.	Redactar y aprobar normativa de clasificación de la información	No conformidad menor	Entrevista Auditoría;

CONTROL	REQUISITO	SITUACIÓN ACTUAL	INCUMPLIMIENTO	CORRECCIÓN	VALORACIÓN	EVIDENCIA
mp.info.4	Firma electrónica BAJO: Se empleará cualquier tipo de firma electrónica prevista en la legislación vigente. MEDIO: a) Cuando se empleen sistemas de firma electrónica avanzada basados en certificados, estos serán cualificados. b) Se emplearán algoritmos y parámetros acreditados por el CCN c) Se garantizará la verificación y validación de la firma electrónica durante el tiempo requerido por la actividad administrativa que aquélla soporte, sin perjuicio de que se pueda ampliar este período de acuerdo con lo que establezca la Política de Firma Electrónica y de Certificados que sea de aplicación. Para tal fin: d) Se adjuntará a la firma, o se referenciará, toda la información pertinente para su verificación y validación. ALTO: 1. Se usará firma electrónica cualificada, incorporando certificados cualificados y dispositivos cualificados de creación de firma. 2. Se emplearán productos certificados conforme a lo establecido en [op.pl.5].	Firma digital: @firma. Se utiliza en varias apps con acceso a través de firma electrónica. No hay política de firma electrónica. Hay un borrador sin revisar.	Ausencia de política de firma electrónica	Redactar y aprobar política de firma electrónica en la Diputación	No conformidad menor	Entrevista Auditoría;
mp.info.6	Limpieza de documentos En el proceso de limpieza de documentos, se retirará toda la información adicional contenida en campos ocultos, meta-datos, comentarios o revisiones anteriores, salvo cuando dicha información sea pertinente para el receptor del documento	No se hace	No se realiza limpieza de documentos previa publicación en la Web	Redactar normativa relativa a la gestión de metadatos y publicación Web Utilizar herramientas para la gestión de metadatos	No conformidad menor	Entrevista Auditoría;

4.3 Observaciones

CONTROL	REQUISITO	SITUACIÓN ACTUAL	CORRECCIÓN	VALORACIÓN	EVIDENCIA
op.pl.1	Análisis de Riesgos (PUNTO CLAVE. Que se haga y revisado anualmente) BÁSICA: Bastará un análisis informal, realizado en lenguaje natural MEDIA: Realizar un análisis semi-formal, usando un lenguaje específico, con un catálogo básico de amenazas y una semántica definida. ALTA: Realizar un análisis formal, usando un lenguaje específico, con un fundamento matemático reconocido internacionalmente.	Último AR en 2010. Se está realizando actualmente en el presente proyecto. Se ha realizado un análisis de la situación actual respecto a cada medida del ENS, se han identificados los sistemas de información a incluir en el ENS, se han valorado, se han evaluado las amenazas y riesgos, y se ha planificado un plan de tratamiento del riesgo para mejora de la seguridad.	El análisis de riesgos se debe revisar anualmente. La siguiente revisión sería en diciembre de 2020.	Observación	Entrevista Auditoría; Documento que contiene la identificación de activos; fichero PILAR; informe análisis de riesgos; plan de mejora; declaración de aplicabilidad
op.pl.4	Dimensionamiento / gestión de capacidades MEDIO: Con carácter previo a la puesta en explotación, se realizará un estudio previo que cubra: a) necesidades de procesamiento; necesidades de almacenamiento de la información; d) necesidades de comunicación; e) necesidades de personal; f) necesidades de instalaciones y medios auxiliares	Se tiene en cuenta todo (excepto personal), pero no está por escrito en ninguna Normativa	Redactar normativa de caracterización y planificación de los sistemas, que comprenda, al menos, las normas relativas a identificación e inventario de activos, arquitectura de Seguridad, gestión del Riesgo, y planificación, dimensionado y gestión de capacidades. Se deberán tener en cuenta las necesidades de personal, y su cualificación y formación necesaria en materia de seguridad, a la hora de un nuevo proyecto TI (nuevo aplicativo, nuevo sistema de información, nuevo servicio TI, etc.).	Observación	Entrevista Auditoría;

CONTROL	REQUISITO	SITUACIÓN ACTUAL	CORRECCIÓN	VALORACIÓN	EVIDENCIA
op.acc.1	Identificación La identificación de los usuarios se realizará: 1.- Se podrán utilizar como identificador único los sistemas de identificación previstos en la normativa de aplicación 2.- Cuando el usuario tenga diferentes roles frente al sistema, recibirá identificadores singulares para cada uno de los casos, para que estén limitados los privilegios y los registros de actividad 3.- Cada entidad (usuario o proceso) que accede al sistema contará con un identificador singular 4.- a) Cada cuenta estará asociada a un identificador único; b) las cuentas deben ser inhabilitadas cuando el usuario dela la organización; cuando el usuario cesa en la función para la cual se requería la cuenta; o cuando la persona que la autorizó, da orden en sentido contrario; c) las cuentas se retendrán durante el periodo necesario para atender a las necesidades de trazabilidad de los registros de actividad asociadas a las mismas.	Se genera un usuario con pwd aleatoria y se le entrega el documento, en el que le dice que se cambie periódicamente cada 6 meses. Esto no está por escrito. El sistema lo recuerda, y cuando llega la fecha se debe cambiar (Windows). El ID de Notes sí se cambia. El correo no. ¿Identificador único? Si Hay usuarios genéricos (por ejemplo, buzones departamentales). A esos usuarios no se les da permiso para acceso a aplicaciones, únicamente el mail. No se permite que los usuarios se loguen con los identificadores genéricos (se hace pero no está por escrito).	Redactar normativa y procedimientos asociados, relativos al control de acceso y gestión de cuentas, que comprenda al menos lo siguiente: - Asignación de privilegios de acceso y revisión de los mismos - Proceso de alta, baja, modificación o bloqueo de cuentas - Política de asignación de contraseñas, robustez y periodicidad de cambio - Autorizaciones para el acceso a los sistemas de información en local y en remoto	Observación	Entrevista Auditoría;
op.acc.2	Requisitos de acceso Los requisitos de acceso se atenderán a: a) los recursos del sistema se protegerán con algún mecanismo que impida su utilización, salvo las entidades que disfruten de derechos de acceso suficientes; b) los derechos de acceso de cada recurso, se establecerán según las decisiones de la persona responsable del recurso; c) Se controlará el acceso a los componentes del sistema y a sus ficheros o registros de configuración	Autenticación mediante usuario/contraseña, y mediante firma digital (por ejemplo, portafirmas o tramitador). Control de fichajes: biométrico.	Redactar normativa y procedimientos asociados, relativa al control de acceso y gestión de cuentas, que comprenda al menos lo siguiente: - Asignación de privilegios de acceso y revisión de los mismos - Proceso de alta, baja, modificación o bloqueo de cuentas - Política de asignación de contraseñas, robustez y periodicidad de cambio - Autorizaciones para el acceso a los sistemas de información en local y en remoto	Observación	Entrevista Auditoría;

CONTROL	REQUISITO	SITUACIÓN ACTUAL	CORRECCIÓN	VALORACIÓN	EVIDENCIA
op.acc.7	Acceso remoto Acceso remoto: Al realizado desde fuera de las propias instalaciones de la organización a través de redes de terceros BAJO: Se garantizará la seguridad del sistema cuando accedan remotamente usuarios u otras entidades, lo que implicará proteger tanto el acceso en sí mismo (op.acc.6) como el canal de acceso remoto (mp.com.2 // mp.com.3) MEDIO: Se establecerá una política específica de lo que puede hacerse remotamente, requiriéndose autorización positiva	El acceso remoto a la red provincial es mediante VPN/SSL. No hay nada por escrito.	Redactar normativa y procedimientos asociados, relativa al control de acceso y gestión de cuentas, que comprenda al menos lo siguiente: - Asignación de privilegios de acceso y revisión de los mismos - Proceso de alta, baja, modificación o bloqueo de cuentas - Política de asignación de contraseñas, robustez y periodicidad de cambio - Autorizaciones para el acceso a los sistemas de información en local y en remoto	Observación	Entrevista Auditoría;
op.exp.5	Gestión de cambios MEDIA: Se mantendrá un control continuo de los cambios realizados en el sistema de manera que: a) Todos los cambios anunciados por el fabricante o proveedor serán analizados para determinar su conveniencia para ser incorporados, o no; b) Antes de poner en producción una nueva versión o una versión parcheada, se comprobará	No se hace con procedimiento formal	Redactar y aprobar un procedimiento de gestión de cambios y versiones	Observación	Entrevista Auditoría;

CONTROL	REQUISITO	SITUACIÓN ACTUAL	CORRECCIÓN	VALORACIÓN	EVIDENCIA
op.exp.11	Protección de claves criptográficas Las claves criptográficas se protegerán durante todo su ciclo de vida BASICA: a) Los medios de generación estarán aislados de los medios de explotación; b) Las claves retiradas de operación que deban ser archivadas, lo serán en medios aislados de los de explotación. MEDIA: a) Se usarán programas evaluados o dispositivos criptográficos certificados (op.pl.5); b) Se emplearán algoritmos acreditados por el CCN.	Nada por escrito	Redactar y aprobar normativa de controles criptográficos, que deberá contener al menos: - Definiciones: firma electrónica, sellos de tiempo, certificado de empleado público - Necesidades de cifrado - Protección de las claves criptográficas	Observación	Entrevista Auditoría;
op.mon.2	Sistema de métricas BÁSICA: Se recopilarán los datos necesarios atendiendo a la categoría del sistema para conocer el grado de implantación de las medidas de seguridad que apliquen de las detalladas en el Anexo II del ENS y, en su caso, promover el informe INES MEDIA: Además, se recopilarán datos para valorar el sistema de gestión de incidentes permitiendo conocer: .- Número de incidentes de seguridad tratados; .- Tiempo empleado para cerrar el 50% de los incidentes; .- Tiempo empleado para cerrar el 90% de los incidentes ALTA: Se recopilarán datos para conocer la eficiencia del sistema de seguridad TIC: Recursos consumidos: horas y presupuesto	Se está realizando en la actualidad el Informe INES y se está recopilando toda la información necesaria.	Realización del Informes INES de forma anual (el siguiente sería en diciembre 2020/enero 2021). Se deberán recopilar todos los datos exigidos en el Informes INES relacionados con seguridad de la información, y con el histórico anual del sistema de gestión de incidentes. Se deberá conocer, al menos: - Número de incidentes de seguridad tratados - Tiempo empleado para resolución del 50 % de los incidentes - Tiempo empleado para resolución del 90 % de los incidentes - Resto de cuestiones planteadas en el Informe INES	Observación	Entrevista Auditoría;

CONTROL	REQUISITO	SITUACIÓN ACTUAL	CORRECCIÓN	VALORACIÓN	EVIDENCIA
mp.if.2	Identificación de las personas El mecanismo de control de acceso se atendrá a lo que se disponga a continuación: a) Se identificará a todas las personas que accedan a los locales donde hay equipamiento que forme parte del sistema de información; b) Se registrarán las entradas y salidas de personas.	Autorizaciones. No hay listado de personal autorizado. Únicamente acceden 3 o 4 personas a cada CPD. Faltaría tener un listado de autorizados revisado por el responsable de seguridad. Cuando viene alguna empresa siempre están acompañados. Limpieza: no se realiza. Medidas de Seguridad. Ventanas no hay. Contactos magnéticos no hay. Sensores de intrusión a nivel general en ambos edificios	Se debe disponer de un listado de personal autorizado a acceder a ambos CPD, principal y secundario, supervisado y revisado por el Responsable de Seguridad. Se deben registrar los accesos a ambos CPD. El Responsable de Seguridad debe revisar de forma periódica los registros para detección de accesos no autorizados.	Observación	Entrevista Auditoría;
mp.com.1	Perímetro seguro BASICA: Se dispondrá de un sistema cortafuegos que separe la red interna del exterior. Todo el tráfico deberá atravesar dicho cortafuegos que solo dejará transitar los flujos previamente autorizados. ALTA: a) El sistema cortafuegos constará de dos o más equipos de diferente fabricante dispuestos en cascada; d) se dispondrá de sistemas redundantes	Existen dos FW en cascada. Uno en modo transparente y otro en modo routing. Disponen de DMZ. Sistemas redundantes: se cumple.	Redactar y aprobar normativa sobre seguridad de la red y procedimiento sobre acceso a redes y acceso remoto	Observación	Entrevista Auditoría;
mp.si.1	Etiquetado Los soportes de información se etiquetarán de forma que, sin revelar su contenido, se indique el nivel de seguridad de la información contenida de mayor calificación. Los usuarios han de estar capacitados para entender el significado de las etiquetas.	Al inventariarse los equipos se etiquetan.	Redacción de normativa de gestión de soportes y procedimientos asociados, que contengan al menos: inventariado de soportes; Etiquetado y Almacenamiento; Criptografía; Traslado; Destrucción	Observación	Entrevista Auditoría;

CONTROL	REQUISITO	SITUACIÓN ACTUAL	CORRECCIÓN	VALORACIÓN	EVIDENCIA
mp.si.4	Transporte El responsable de sistemas garantizará que los dispositivos permanecen bajo control y que satisfacen sus requisitos de seguridad mientras están siendo desplazados de un lugar a otros. Para ello: a) Se dispondrá de un registro de salida que identifique el transportista que recibe el soporte para su traslado; b) Se dispondrá de un registro de entrada que identifique al transportista que lo entrega; c) Se dispondrá de un procedimiento rutinario que coteje las salidas con las llegadas y levante alarmas pertinentes cuando se detecte algún incidente; d) Se utilizarán los medios de protección criptográfica (mp.si.2) correspondientes al nivel de calificación de la información contenida de mayor nivel; e) Se gestionarán las claves según (op.exp.11).	Los archivos finales están en la Cañada de San Urbano. El transporte lo hacen ellos mismos, utilizando cajas de plástico, en función del cuadro de clasificación ordenan las cajas. En el transporte no hay paradas. Cuando hay cambio de áreas de dependencias, no hay protocolo pero se asegura que no se quede documentación en el destino.	Redacción de normativa de gestión de soportes y procedimientos asociados, que contengan al menos: inventariado de soportes; Etiquetado y Almacenamiento; Criptografía; Traslado; Destrucción	Observación	Entrevista Auditoría;
mp.info.1	Datos de carácter personal Cuando el sistema trate datos de carácter personal, se estará a lo dispuesto en la LOPD, y normas de desarrollo, sin perjuicio de cumplir, además, las medidas establecidas en el ENS.	La Diputación está en proceso avanzado de adecuación al RGPD/LOPDgdd	Finalizar el plan de adecuación al RGPD y acometer todas las medidas jurídicas del plan de mejora de la seguridad	Observación	Entrevista Auditoría;

CONTROL	REQUISITO	SITUACIÓN ACTUAL	CORRECCIÓN	VALORACIÓN	EVIDENCIA
mp.info.9	Copias de Seguridad (backup) Se realizarán copias de seguridad que permitan recuperar datos perdidos, accidental o intencionadamente con una antigüedad determinada. Poseerán el mismo nivel de seguridad que los datos originales en lo que se refiere a integridad, confidencialidad, autenticidad y trazabilidad. En particular, se considerará la conveniencia o necesidad, según proceda, de que las copias de seguridad estén cifradas para garantizar la confidencialidad. Las copias de seguridad deberán abarcar: a) Información de trabajo de la organización; b) Aplicaciones en explotación, incluyendo los sistemas operativos; c) Datos de configuración, servicios, aplicaciones, equipos, u otros de naturaleza análoga; d) Claves utilizadas para preservar la confidencialidad de la información.	Se hace, pero no está por escrito. Tipo de copia: incremental a diario. Alguna diferencial.	Redactar normativa y procedimientos de copias de seguridad y restaurado de información.	Observación	Entrevista Auditoría;
mp.s.1	Protección del correo electrónico El correo electrónico se protegerá frente a las amenazas que le son propias: a) La información distribuida por medio de correo electrónico, se protegerá, tanto en el cuerpo de los mensajes, como en los anexos; b) Se protegerá la información de encaminamiento de mensajes y establecimiento de conexiones; c) Se protegerá a la organización frente a problemas que se materializan por medio del correo electrónico (spam Programas dañinos, constituidos por virus, gusanos, troyanos, espías, u otros de naturaleza análoga, código móvil de tipo «applet»); d) Se establecerán normas de uso del correo electrónico por parte del personal determinado	Medidas actuales: existen 3 servidores que soportan el mail, hay un sistema antispam y av (archivos maliciosos), no entrega el mail. Correo saliente: no hay medidas de seguridad. Algunos usuarios utilizan el correo particular; ¿nube corporativa? owncloud; Phishing: el propio FW dispone de medidas antiphishing; se envían circulares en el caso de detección.	Redactar y aprobar normativa de uso y protección del correo electrónico, que contenga al menos: - requisitos de protección de la parte servidora - requisitos de protección de la parte cliente	Observación	Entrevista Auditoría;

CONTROL	REQUISITO	SITUACIÓN ACTUAL	CORRECCIÓN	VALORACIÓN	EVIDENCIA
mp.s.8	Protección frente a la denegación de servicio MEDIO Se establecerán medidas preventivas y reactivas frente a ataques de denegación de servicio (DOS Denial of Service): a) Se planificará y dotará al sistema de capacidad suficiente para atender a la carga prevista con holgura; b) Se desplegarán tecnologías para prevenir los ataques conocidos. ALTO: a) Se establecerá un sistema de detección de ataques de denegación de servicio. b) Se establecerán procedimientos de reacción a los ataques, incluyendo la comunicación con el proveedor de comunicaciones. c) Se impedirá el lanzamiento de ataques desde las propias instalaciones perjudicando a terceros.	Existen medios contra los ataques de negación de servicio en el FW y en el WAF	Redactar y aprobar procedimiento de actuación ante ataques de denegación de servicio	Observación	Entrevista Auditoría;

4.4 Sugerencias de Mejora

No se han identificado sugerencias de mejora.

4.5 Cumplimiento correcto

CONTROL	REQUISITO	SITUACIÓN ACTUAL	VALORACIÓN	EVIDENCIA
Art. 29	¿Conoce y mantiene actualizada la relación de las instrucciones técnicas de seguridad y guías de seguridad que le son de aplicación a su sistema?	Conocen las Guías de Aplicación del CCN-CERT respecto al ENS, y se utilizan.	Correcto	Entrevista Auditoría
Art. 35	¿Cumplimenta la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad regulada por Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas	Se cumplimenta el Informe INES anualmente	Correcto	Entrevista Auditoría
Art. 36	¿Notifica al CCN-CERT (Centro Criptológico Nacional- Computer Emergency Response Team) aquellos incidentes de seguridad que tengan un impacto significativo en la seguridad de la información manejada y de los servicios prestados en relación con la categorización de sistemas recogida en el Anexo I del RD 3/2010?	Se notifican al CCN-CERT los incidentes de seguridad con impacto significativo	Correcto	Entrevista Auditoría
Art. 43, 44	¿Existe un proceso formal para la determinación de la categoría del sistema de información en función de la valoración del impacto que tendría un incidente que afectara a la seguridad de la información o de los servicios con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad siguiendo el procedimiento establecido en el Anexo I del RD 3/2010?	Se ha determinado la categoría de todos los sub-sistemas de información identificados en el marco del ENS, en las dimensiones de Disponibilidad, Integridad, Autenticidad, Confidencialidad y Trazabilidad.	Correcto	Entrevista Auditoría
op.mon.1	Detección de intrusión MEDIA: Se dispondrán de herramientas de detección o de prevención de intrusión	El propio FW funciona como IDS/IPS.	Correcto	Entrevista Auditoría;

CONTROL	REQUISITO	SITUACIÓN ACTUAL	VALORACIÓN	EVIDENCIA
mp.if.3	Acondicionamiento de los locales Los locales donde se ubiquen los sistemas de información y sus componentes dispondrán de elementos adecuados para el eficaz funcionamiento del equipamiento allí instalado. Y, en especial: a) Condiciones de temperatura y humedad; b) Protección frente a las amenazas identificadas en el análisis de riesgos; c) Protección del cableado frente a incidentes fortuito o deliberados.	Aire acondicionado: hay en ambos CPD, sistema principal y sistema de apoyo. Sensores de T y H. En Navarro Rodrigo existen sensores. Suena una alarma cuando se supera el umbral.	Correcto	Entrevista Auditoría;
mp.if.4	Energía eléctrica BAJO: Los locales donde se ubiquen los sistemas de información y sus componentes dispondrán de la energía eléctrica, y sus tomas correspondientes, necesaria para su funcionamiento, de forma que en los mismos: a) Se garantizará el suministro de potencia eléctrica; b) Se garantizará el correcto funcionamiento de las luces de emergencia. MEDIO: Se garantizará el suministro eléctrico a los sistemas en caso de fallo del suministro general, garantizando el tiempo suficiente para una terminación ordenada de los procesos, salvaguardando la información.	Ambos CPD cuentan con grupo electrógeno de apoyo, y ambos lleva asociado un SAI. Se les va a meter un duplicado de SAI para mayor seguridad, y en Palacio se instalará un grupo electrógeno independiente (actualmente está en el edificio). El de Rambla Alfareros sí es exclusivo. Luces de emergencia. Autoprotección ok.	Correcto	Entrevista Auditoría;
mp.if.5	Protección frente a incendios Los locales donde se ubiquen los sistemas de información y sus componentes se protegerán frente a incendios fortuitos o deliberados,	Ambos edificios constan con sistema automático de extinción mediante Halón. Hay extintores de CO2 en ambos. Hay detectores de incendio en ambos edificios, central conectada CRA, controlada por empresa de protección contra incendios. Pulsadores de alarma también hay en ambos.	Correcto	Entrevista Auditoría;

CONTROL	REQUISITO	SITUACIÓN ACTUAL	VALORACIÓN	EVIDENCIA
mp.eq.2	Bloqueo del puesto de trabajo MEDIO: El puesto de trabajo se bloqueará al cabo de un tiempo prudencial de inactividad, requiriendo una nueva autenticación del usuario para reanudar la actividad en curso ALTO: Pasado un cierto tiempo, se cancelarán las sesiones abiertas desde dicho puesto de trabajo	Se bloquea el monitor al cabo de x tiempo. Las sesiones se quedan bloqueadas pero abiertas.	Correcto	Entrevista Auditoría;
mp.eq.9	Medios alternativos MEDIO: Se garantizará la existencia y disponibilidad de medios alternativos de tratamiento de la información para el caso de que fallen los medios habituales. Se establecerá un tiempo máximo para que los equipos alternativos entren en funcionamiento	Existe un CPD Alternativo	Correcto	Entrevista Auditoría;
mp.com.2	Protección de la confidencialidad MEDIO: a) Se emplearán redes privadas virtuales cuando la comunicación discurra por redes fuera del propio dominio de seguridad; b) Se emplearán algoritmos acreditados por el CC ALTO: a) Se emplearán, preferentemente, dispositivos hardware en el establecimiento y utilización de la VPN; b) Se emplearán productos certificados conforme a lo establecido en [op.pl.5]	Se emplean VPN cuando las comunicaciones transcurren fuera de la oficina. Las VPN se realizan contra los cortafuegos	Correcto	Entrevista Auditoría;

4.6 No aplica

Las medidas que no aplican se han incluido en la documentación del Plan de Adecuación al ENS de Diputación, y se puede consultar en el documento de declaración de aplicabilidad de las medidas del ENS [3]

5. Dictamen final de auditoría

A raíz de los hallazgos detectados, y en base al Aptdo. 3.7 de la Guía CCN-STIC-802, se puede dictaminar que el resultado de esta auditoría es FAVORABLE CON NO CONFORMIDADES.

La decisión sobre el dictamen de auditoría tiene en consideración que se han evidenciado “No Conformidades Menores” y “No Conformidades Mayores”, y que la Diputación, como organismo responsable del sistema de información auditado, dispone de un Plan de Acciones Correctivas (PAC) que se ha incluido en el presente Informe de Auditoría y que se puede encontrar también en el Plan de Mejora de la Seguridad asociado a la documentación del Plan de Adecuación al ENS [4], para paliar las no conformidades identificada das, concretamente en el *Apartado 4* del presente documento.

No obstante, es necesario indicar que, el dictamen de la auditoría como favorable con no conformidades, implica que la Diputación debe realizar una correcta planificación de las medidas incluidas en el Plan de Acción propuesto, incluyendo la estimación los medios necesarios para llevarlas a cabo y los plazos de tiempo necesarios, debiendo realizar además un proceso continuo de seguimiento del citado Plan y una evaluación de la eficiencia de las medidas que se llevan a cabo. Únicamente de esta forma podrán mitigarse los riesgos de seguridad derivados de las no conformidades encontradas.

Fdo. Auditor Jefe

David López Gutiérrez. Consultor Seguridad Estratégica en Ingenia.