

1683/22

DECRETO DE LA PRESIDENCIA

Visto el informe propuesta de 26 de abril de la Delegada de Protección de Datos de la Diputación de Salamanca que literalmente señala:

Informe-Propuesta que formula la Delegada de Protección de Datos y se eleva a la Presidencia para su consideración y aprobación, si así lo estima oportuno, conforme a los antecedentes de hecho y legislación jurídica que van a expresarse a continuación:

ANTECEDENTES DE HECHO

PRIMERO. – Mediante Decreto de la Presidencia 1062/22, de fecha 25 de marzo de 2022, se aprobó la siguiente documentación:

- REGISTRO DE BASES DE TRATAMIENTO, que consta de 28 páginas y que se adjunta como Anexo I
- DOCUMENTACIÓN DE SEGURIDAD DE LA INFORMACIÓN, que consta de 45 páginas y se adjunta como Anexo II
- SENSIBILIZACIÓN EN PROTECCIÓN DE DATOS, que consta de 19 páginas y se adjunta como Anexo III
- EVALUACIÓN DE IMPACTO DE PROTECCIÓN DE DATOS EIPD, que consta de 6 páginas y se adjunta como Anexo IV

Dichos documentos sirven para asegurar el cumplimiento por parte de la Diputación Provincial de sus obligaciones legales derivadas del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, en adelante RGPD, así como la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de Derechos Digitales (en los aspectos relativos a la Protección de Datos), en adelante LOPD, y su normativa de desarrollo.

Los citados documentos fueron elaborados por la empresa que ha prestado el servicio de AUDITORÍA DE CUMPLIMIENTO NORMATIVO Y ASESORAMIENTO EN MATERIA DE PROTECCIÓN DE DATOS a la Diputación Provincial.

SEGUNDO. – Dicha empresa, elaboró un documento más, el “PLAN DE ACCIÓN”, que contempla la implantación de las medidas organizativas, físicas e informáticas propuestas.

En el Plan de Acción se establecen los plazos para realizar cada una de las acciones recogidas en el mismo, así como la forma de evaluación de su implantación.

Código Seguro de Verificación	IV7DVXILZEPLXJO4IYW63XEEI	Fecha	28/04/2022 15:07:45
Normativa	Este documento incorpora firma electrónica reconocida de acuerdo a la ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza		
Firmante	DIPUTACIÓN PROVINCIAL DE SALAMANCA (FRANCISCO JAVIER IGLESIAS GARCÍA) (PRESIDENTE DE LA DIPUTACIÓN)		
Firmante	ALEJANDRO MARTÍN GUZMÁN (SECRETARIO GENERAL)		
Url de verificación	https://sede.diputaciondesalamanca.gob.es/moad/verifirma-moad/code/IV7DVXILZEPLXJO4IYW63XEEI	Página	1/7



TRANSCRITO

1683/22

En la parte expositiva del anteriormente mencionado Decreto 1062/22, de 25 de marzo, se explicaba que este documento, por su propio contenido, se aprobaría posteriormente a la aprobación de los otros cuatro.

LEGISLACION APLICABLE

Normativa Europea

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, del 27 de abril de 2016, relativo a las personas físicas sobre el tratamiento de datos personales y la libre circulación de los mismos (RGPD) Norma ISO 9001:2008
- Reglamento (UE) 679/2016 del parlamento europeo y del consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos persona-les y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
- Directiva (UE) 680/2016 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos.
- Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

Normativa interna

- Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos. (BOE, 31-marzo-2021)
- Ley 7/85 de 2 de abril, Reguladora de las Bases del Régimen local
- Ley 39/2015 de 1 de octubre del Procedimiento administrativo Común de las administraciones Públicas.
- Ley 40/2015 de 1 de octubre de Régimen Jurídico del Sector Público.
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. (BOE, 23-junio-2007)

Código Seguro de Verificación	IV7DVXTILZEPLXJO4IYW63XEEI	Fecha	28/04/2022 15:07:45
Normativa	Este documento incorpora firma electrónica reconocida de acuerdo a la ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza		
Firmante	DIPUTACIÓN PROVINCIAL DE SALAMANCA (FRANCISCO JAVIER IGLESIAS GARCÍA) (PRESIDENTE DE LA DIPUTACIÓN)		
Firmante	ALEJANDRO MARTÍN GUZMÁN (SECRETARIO GENERAL)		
Url de verificación	https://sede.diputaciondesalamanca.gob.es/moad/verifirma-moad/code/IV7DVXTILZEPLXJO4IYW63XEEI	Página	2/7



TRANSCRITO

1683/22

Por todo lo expuesto, se eleva a la consideración del órgano decisor, la siguiente

PROPUESTA

Aprobar el documento "PLAN DE ACCIÓN", que consta de 4 páginas y se adjunta como Anexo I.

Dado a la fecha de la firma, en Salamanca, ante mí el Secretario General, que doy fe.

El Presidente

Ante mí:
El Secretario General

Fdo: Francisco Javier Iglesias García

Fdo: Alejandro Martín Guzmán

C/ Felipe Espino, 1. 37002 Salamanca

Asesoría Jurídica. Tel.: 923 293 100/ Ext. 252 y 214

Código Seguro de Verificación	IV7DVXTILZEPLXJO4IYW63XEEI	Fecha	28/04/2022 15:07:45
Normativa	Este documento incorpora firma electrónica reconocida de acuerdo a la ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza		
Firmante	DIPUTACIÓN PROVINCIAL DE SALAMANCA (FRANCISCO JAVIER IGLESIAS GARCÍA) (PRESIDENTE DE LA DIPUTACIÓN)		
Firmante	ALEJANDRO MARTÍN GUZMÁN (SECRETARIO GENERAL)		
Url de verificación	https://sede.diputaciondesalamanca.gob.es/moad/verifirma-moad/code/IV7DVXTILZEPLXJO4IYW63XEEI	Página	3/7



ANEXO I
 PLAN DE ACCIÓN
 ADECUACIÓN A LA LEGISLACIÓN DE PROTECCIÓN DE DATOS DE LA DIPUTACIÓN DE SALAMANCA

Nº	Bloque	Control de Seguridad de la Información	Estado	Acción a realizar	Responsable	Plazo	Forma de evaluación
1	Política de seguridad de la Información						
	Dirigir y dar soporte a la gestión de la seguridad de la Información de acuerdo con los requisitos Institucionales, leyes y reglamentos pertinentes.						
1.1.	Política de seguridad	Se dispone de una política de seguridad aprobada por la dirección, publicada y comunicada a todos los empleados y partes externas pertinentes.	Inicial	Comunicar a todos los empleados	Delegado de Protección de datos	2º trimestre 2022	enviado y recibido
1.2.		La política de seguridad de información se revisa a intervalos planificados, y si ocurren cambios significativos se asegura su conveniencia, adecuación y eficacia continua.	Inicial	Establecer revisiones periódicas de la Documentación de seguridad	Delegado de Protección de datos	Anual	Informe de revisión de documentación de seguridad
2	Organización de la seguridad de la información						
	Gestionar la organización de la seguridad de información.						
2.1	Organización interna	La Dirección apoya (dirige, se compromete, demuestra y reconoce responsabilidades) activamente la Seguridad de la Información en la Diputación	Gestionado	NA, ver documento de seguridad de la información			
2.2		En las actividades de seguridad participan representantes de todos los departamentos. Tienen roles y funciones.		Sensibilización de protección de datos	Delegado de Protección de datos	2º trimestre 2022	enviado y recibido
2.3		Los roles y responsabilidades en Seguridad de la Información están bien definidos.	Gestionado	NA, ver documento de seguridad de la información			
2.4		Está establecido el proceso de autorización para nuevos activos de información (AI).	Gestionado	NA, ver documento de seguridad de la información			
2.5		Están definidos acuerdos de confidencialidad y se revisa con regularidad.		Establecer revisiones periódicas de la Documentación de seguridad	Delegado de Protección de datos	anual	Informe de revisión de documentación de seguridad
2.6		Se mantiene los contactos apropiados con las autoridades pertinentes.	Gestionado	NA			
2.7		Se mantiene los contactos apropiados con entidades especializadas en Seguridad de la Información: Agencia Española de Protección de Datos, INCIBE.	Gestionado	NA			
2.8		El enfoque de la organización para gestionar la Seguridad de la Información se revisa de manera independiente y periódica.	Gestionado	Contratación de mantenimiento de protección de datos	Delegado de Protección de datos	anual	Informe de revisión de documentación de seguridad
2.9	Entidades externas	Se gestiona (identifica e implementa) los riesgos de acceso a la información de entidades externas.	Inicial	Revisión de todos los contratos vigentes, para incluir si acceden a datos un anexo con la cláusula de confidencialidad.	Delegado de Protección de datos	2º trimestre 2022	Los contratos han sido revisados
2.10		Se trata todos los requerimientos de Seguridad de la Información antes de dar acceso a los clientes.	Inicial	Procedimiento para revisar contratos antes de su firma por el Delegado de Protección de datos	Delegado de Protección de datos	2º trimestre 2022	Existe el procedimiento y se utiliza
2.11		Se establece acuerdos con terceros, que involucren acceder, procesar, comunicar o gestionar la información de la entidad, que abarcan los requerimientos de Seguridad de la Información relevantes.	Inicial	Procedimiento para revisar contratos antes de su firma por el Delegado de Protección de datos	Delegado de Protección de datos	2º trimestre 2022	Existe el procedimiento y se utiliza
3	Gestión de activos de información (AI)						
	Lograr y mantener la protección apropiada de los activos de información						
3.1	Responsabilidad por los activos	Se mantiene un inventario de AI.	Optimizado	NA, realizado por CIPSA			
3.2		Todo AI tiene asignado un responsable (propietario).	Optimizado	NA, realizado por CIPSA			
3.3		Se dispone de una normativa de uso de los AI	Optimizado	NA, realizado por CIPSA			
3.4	Clasificación de la información	La información está clasificada según su valor, requisitos legales, sensibilidad y criticidad	Optimizado	NA, realizado por CIPSA			
3.5		Se dispone del procedimiento de rotulado y manejo de la información.	Optimizado	NA, realizado por CIPSA			
	Seguridad de los recursos humanos						
4	Asegurar que todo el personal involucrado entienda sus responsabilidades, sean apropiados para sus roles y así reducir el riesgo de robo, fraude o mal uso de los activos de información.						
4.1	Antes del empleo	Se tiene documentado (de acuerdo a la política) los roles y responsabilidades de SI, de todo el personal.	Gestionado	NA, ver documento de seguridad de la información			
4.2		Se verifica antecedentes de todo candidato a empleado o contratista.	Optimizado	NA, contratación pública			
4.3		Se firman contratos donde se incluye las responsabilidades de SI.	Gestionado	Definidas cláusulas, revisar contratos y añadir en casos necesarios.	Delegado de Protección de datos	2º trimestre 2022	Revisión de contratos.
4.4		Se procura que todos los empleados apliquen la Seguridad de la Información según la política.	Definido	Sensibilización de protección de datos	Delegado de Protección de datos	2º trimestre 2022	enviado y recibido

TRANSCRITO

1683/22



Código Seguro de Verificación	I7DVX7TILZEP LXJ041YV63XEEI		Fecha	28/04/2022 15:07:45
Normativa	Este documento incorpora firma electrónica reconocida de acuerdo a la ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza			
Firmante	DIPUTACIÓN PROVINCIAL DE SALAMANCA (FRANCISCO JAVIER IGLESIAS GARCIA) (PRESIDENTE DE LA DIPUTACION)			
Firmante	ALEJANDRO MARTÍN GUZMAN (SECRETARIO GENERAL)			
Url de verificación	https://sede.diputaciondesalamanca.gob.es/moad/verifirma-moad/code/I7DVX7TILZEP LXJ041YV63XEEI		Página	4/7

4.5	Durante el empleo	Se sensibiliza, capacita y educa en Seguridad de la Información pertinente a su función de trabajo.	Definido	Sensibilización de protección de datos	Delegado de Protección de datos	2º trimestre 2022	enviado y recibido
4.6		Se tiene establecido un proceso disciplinario ante el incumplimiento de SI.	Inicial	NA, son funcionarios públicos y ya está definido en la legislación			
4.7	Terminación o cambio del empleo	Están definidas las responsabilidades para el término o cambio de empleo.	Gestionado	NA, realizado por CIPSA			
4.8		Se procura la entrega de activos al término de contrato.	Gestionado	NA, realizado por CIPSA			
4.9		Se retira los derechos de acceso al término del contrato.	Gestionado	NA, realizado por CIPSA			
5	Seguridad física y medioambiental						
	Prevenir el acceso físico no autorizado, daño e interferencia en las instalaciones y activos de información.						
5.1		Se utiliza mecanismos de protección perimétrica (muros, vigilantes, etc.) a las áreas que contienen información e instalaciones que procesan información.	Optimizado	NA, realizado por CIPSA			
5.2		Se utiliza mecanismos de control de acceso en entradas críticas.	Optimizado	NA, realizado por CIPSA			
5.3	Áreas seguras	Se utiliza mecanismos de seguridad en oficinas, salas e instalaciones.	Inicial	Poner cartel informático con cláusula de protección de datos en la entrada cuando se recoge nombre y apellidos por el personal de seguridad. Poner cartel de videovigilancia en todas las entradas que se grabe.	Delegado de Protección de datos	2º trimestre 2022	Revisión visual de las entradas de los edificios y comprobación que se han aplicado las medidas.
5.4		Se utiliza mecanismos de protección ante amenazas externas y ambientales.	Optimizado	NA, realizado por CIPSA			
5.5		Se aplica medidas de seguridad física y directrices para trabajar en áreas seguras.	Optimizado	NA, realizado por CIPSA			
5.6		Se aplica medidas de seguridad en áreas de acceso público (entrega/descarga).	Optimizado	NA, realizado por CIPSA			
5.7		Los equipos están ubicados en salas con protección física ante un posible acceso no autorizado.	Optimizado	NA, realizado por CIPSA			
5.8		Los equipos están protegidos frente a fallas de servicios públicos.	Optimizado	NA, realizado por CIPSA			
5.9		El cableado eléctrico y de comunicaciones está protegido frente a interceptación o daños.	Optimizado	NA, realizado por CIPSA			
5.10		Los equipos son mantenidos en forma periódica.	Optimizado	NA, realizado por CIPSA			
5.11		Se aplica seguridad a los equipos fuera del local.	Optimizado	NA, realizado por CIPSA			
5.12		Antes de dar de baja un equipo se elimina la información.	Optimizado	NA, realizado por CIPSA			
5.13		Todo equipo requiere autorización para ser retirado de la Diputación.	Optimizado	NA, realizado por CIPSA			
6	Gestión de operaciones y comunicaciones						
	Asegurar la operación correcta y segura de los activos de información.						
6.1		Procedimientos de operación documentados y disponible a los usuarios.	Optimizado	NA, realizado por CIPSA			
6.2		Gestión del control de cambios en los recursos de procesamiento de información.	Optimizado	NA, realizado por CIPSA			
6.3		Segregación de responsabilidades para reducir el mal uso de los activos.	Optimizado	NA, realizado por CIPSA			
6.4		Separación de los recursos de desarrollo, prueba y producción.	Optimizado	NA, realizado por CIPSA			
6.5		Procurar que los terceros implementen, operen y mantengan los controles de seguridad.	Optimizado	NA, realizado por CIPSA			
6.6		Monitoreo y auditoría regular de los servicios e informes de terceros.	Optimizado	NA, realizado por CIPSA			
6.7		Gestionar los cambios en servicios de terceros, considerando criticidad de sistema de negocio así como procesos involucrados y la evaluación de riesgos.	Optimizado	NA, realizado por CIPSA			
6.8		Monitorear, afinar y realizar proyecciones de uso de recursos para asegurar buen desempeño.	Optimizado	NA, realizado por CIPSA			
6.9		Establecer los criterios de aceptación de sistemas y realizar las pruebas antes de la aceptación.	Optimizado	NA, realizado por CIPSA			
6.10		Implementar controles de prevención, detección y recuperación ante software malicioso, así como controles adecuados para la toma de conciencia.	Optimizado	NA, realizado por CIPSA			
6.11		Asegurar que el código móvil autorizado opere de acuerdo a las políticas de seguridad.	Optimizado	NA, realizado por CIPSA			
6.12		Copias de respaldo (back-up)	Optimizado	NA, realizado por CIPSA			
6.13		Manejar y controlar adecuadamente las redes para proteger la información e infraestructura.	Optimizado	NA, realizado por CIPSA			
6.14		Las características de seguridad, los niveles del servicio, y los requisitos de gestión de todos los servicios en red están identificados e incluido en cualquier acuerdo de servicio de red, ya sea que estos servicios sean proporcionados en la empresa o subcontratos.	Optimizado	NA, realizado por CIPSA			
6.15		Se dispone de procedimientos para la gestión de medios removibles.	Optimizado	NA, realizado por CIPSA			
6.16		Se dispone de procedimientos formales para la eliminación de medios.	Optimizado	NA, realizado por CIPSA			
6.17		Se dispone de procedimientos para el manejo de información de manera confidencial.	Optimizado	NA, realizado por CIPSA			
6.18		La documentación de los sistemas es protegida del acceso no autorizado.	Optimizado	NA, realizado por CIPSA			
6.19		Se dispone de normativa para proteger la información durante su intercambio en cualquier medio de comunicación.	Optimizado	NA, realizado por CIPSA			
6.20		Se firma acuerdos para el intercambio de información y software con entidades externas.	Optimizado	NA, realizado por CIPSA			
6.21		Se protege los medios en tránsito contra acceso no autorizado, mal uso o corrupción durante el transporte más allá de los límites físicos de la institución.	Optimizado	NA, realizado por CIPSA			
6.22		Se protege adecuadamente la información involucrada en los mensajes electrónicos.	Optimizado	NA, realizado por CIPSA			

TRANSCRITO

16/03/22



Código Seguro de Verificación	I7DVX7LZEPJXJ04YVW63XEEI		Fecha	28/04/2022 15:07:45
Normativa	Este documento incorpora firma electrónica reconocida de acuerdo a la ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza			
Firmante	DIPUTACIÓN PROVINCIAL DE SALAMANCA (FRANCISCO JAVIER IGLESIAS GARCÍA) (PRESIDENTE DE LA DIPUTACIÓN)			
Firmante	ALEJANDRO MARTÍN GUZMÁN (SECRETARIO GENERAL)			
Url de verificación	https://sede.diputaciondesalamanca.gob.es/road/verifirma-moad/code/I7DVX7LZEPJXJ04YVW63XEEI		Página	5/7

6.23		Se dispone de normativa para proteger la información asociada con la interconexión de los sistemas de información de la institución.	Optimizado	NA, realizado por CIPSA				
6.24	Servicios de comercio electrónico	Se protege la información de comercio electrónico que se transmite en redes públicas, contra actividades fraudulentas, litigios contractuales y divulgación o modificación.	Optimizado	NA, realizado por CIPSA				
6.25		Se protege la información de las transacciones en línea: De transmisión incompleta, pérdida de rutas, alteración, divulgación y duplicidad.	Optimizado	NA, realizado por CIPSA				
6.26		Se protege la integridad de la información disponible públicamente.	Optimizado	NA, realizado por CIPSA				
6.27	Monitoreo (de actividades no autorizadas)	Se registra pistas de auditoría, excepciones y eventos de seguridad.	Optimizado	NA, realizado por CIPSA				
6.28		Se dispone de procedimientos de monitoreo del uso de recursos y se revisa regularmente.	Optimizado	NA, realizado por CIPSA				
6.29		Se protege la información y los medios de registro frente a acceso manipulado o no autorizado.	Optimizado	NA, realizado por CIPSA				
6.30		Se registra las actividades del administrador y operador del sistema.	Optimizado	NA, realizado por CIPSA				
6.31		Se registran las fallas, se analizan y se toma la acción apropiada.	Optimizado	NA, realizado por CIPSA				
6.32		Los relojes de los sistemas de procesamiento de información se mantienen sincronizados.	Optimizado	NA, realizado por CIPSA				
7	Control de acceso (lógico)							
	Controlar el acceso lógico a los activos de información							
7.1	Requerimientos	Se dispone de una política de control de acceso con base en requerimientos del negocio y de seguridad para el acceso.	Optimizado	NA, realizado por CIPSA				
7.2	Gestión de acceso de usuarios	Se dispone de procedimiento de registro y baja de concesión de acceso a los sistemas y servicios de información.	Optimizado	NA, realizado por CIPSA				
7.3		Se dispone de procedimiento para la gestión (restricción, control y asignación) de privilegios.	Optimizado	NA, realizado por CIPSA				
7.4		Se dispone de procedimiento para la gestión de contraseñas.	Optimizado	NA, realizado por CIPSA				
7.5		Se audita los derechos de acceso de manera regular.	Optimizado	NA, realizado por CIPSA				
7.6	Responsabilidades de usuarios	Se promueve las buenas prácticas de seguridad para la selección y uso de contraseñas seguras.	Optimizado	NA, realizado por CIPSA				
7.7		Se promueve que los usuarios deben asegurar la protección de los equipos desatendidos.	Definido	Sensibilización de protección de datos	Delegado de Protección de datos	2º trimestre 2022	enviado y recibido	
7.8		Se promueve la práctica de escritorio limpio para documentos y dispositivos de almacenamiento removibles, y una política de pantalla limpia.	Definido	Sensibilización de protección de datos	Delegado de Protección de datos	2º trimestre 2022	enviado y recibido	
7.9	Control de acceso a la red	Los usuarios solo tienen acceso a los servicios que están autorizados.	Optimizado	NA, realizado por CIPSA				
7.10		Se utiliza mecanismos apropiados de autenticación para acceso de usuarios externos.	Optimizado	NA, realizado por CIPSA				
7.11		La identificación del equipo forma parte de la autenticación.	Optimizado	NA, realizado por CIPSA				
7.12		Se controla el acceso para el diagnóstico y configuración de puertos.	Optimizado	NA, realizado por CIPSA				
7.13		Se segrega en la red, los usuarios y sistemas de información.	Optimizado	NA, realizado por CIPSA				
7.14		Se restringe la capacidad de conexión de usuarios a redes compartidas.	Optimizado	NA, realizado por CIPSA				
7.15	Control de acceso al sistema operativo	La red se configura de modo que no se infrinja los controles de acceso.	Optimizado	NA, realizado por CIPSA				
7.16		Se controla el acceso al SO en las estaciones o terminales (procedimiento de conexión segura).	Optimizado	NA, realizado por CIPSA				
7.17		Todo usuario dispone de una cuenta de acceso única.	Optimizado	NA, realizado por CIPSA				
7.18		El sistema de gestión de claves asegura su calidad.	Optimizado	NA, realizado por CIPSA				
7.19		Se restringe el uso de utilidades (software) no autorizadas, que podrían eludir las medidas de control del sistema.	Optimizado	NA, realizado por CIPSA				
7.20		Las sesiones inactivas se cierran luego de un tiempo de inactividad.	Optimizado	NA, realizado por CIPSA				
7.21	Control de acceso a las aplicaciones e	Se restringe el horario de acceso a las aplicaciones de alto riesgo.	Optimizado	NA, realizado por CIPSA				
7.22		Se restringe el acceso a los usuarios y al personal de TI.	Optimizado	NA, realizado por CIPSA				
7.23	Computación móvil y teletrabajo	Los sistemas sensibles están en un ambiente aislado.	Optimizado	NA, realizado por CIPSA				
7.24		Se dispone de política de protección de equipos móviles.	Optimizado	NA, realizado por CIPSA				
7.25		Se dispone de política y procedimiento para teletrabajo.	Optimizado	NA, realizado por CIPSA				
8	Adquisición, desarrollo y mantenimiento de sistemas de información							
	Procurar que la seguridad sea una parte integral de los sistemas de información.							
8.1	Requerimientos de seguridad de los sistemas	Se especifican los requerimientos para nuevos sistemas o mejoras, incluyendo los controles de seguridad.	Optimizado	NA, realizado por CIPSA				
8.2	Procesamiento correcto en las aplicaciones	Se validan los datos de entrada a las aplicaciones para asegurar que esta sea correcta y apropiada.	Optimizado	NA, realizado por CIPSA				
8.3		Se incorpora mecanismos de validación en las aplicaciones para detectar corrupción de la información.	Optimizado	NA, realizado por CIPSA				
8.4		Se identifican los requisitos para asegurar la autenticidad e integridad de los mensajes en las aplicaciones.	Optimizado	NA, realizado por CIPSA				
8.5		Se valida la data de salida de las aplicaciones.	Optimizado	NA, realizado por CIPSA				



TRANSCRITO

16/03/22

Código Seguro de Verificación	I7VDVXTLZEPXJ041YV63XEEI		Fecha	28/04/2022 15:07:45
Normativa	Este documento incorpora firma electrónica reconocida de acuerdo a la ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza			
Firmante	DIPUTACIÓN PROVINCIAL DE SALAMANCA (FRANCISCO JAVIER GLESIAS GARCÍA) (PRESIDENTE DE LA DIPUTACIÓN)			
Firmante	ALEJANDRO MARTÍN GUZMÁN (SECRETARIO GENERAL)			
Url de verificación	https://sede.diputaciondesalamanca.gob.es/road/verifirma-moad/code/I7VDVXTLZEPXJ041YV63XEEI		Página	6/7

8.6	Controles	Se dispone de una política de uso de controles criptográficos para proteger la información.	Optimizado	NA, realizado por CIPSA			
8.7	criptográficos	Se realiza gestión de claves para dar soporte al uso de las técnicas criptográficas.	Optimizado	NA, realizado por CIPSA			
8.8	Seguridad de los	Se dispone de procedimientos para la instalación del software de los sistemas.	Optimizado	NA, realizado por CIPSA			
8.9	archivos del sistema	Se selecciona, protege y controla los datos de prueba del sistema.	Optimizado	NA, realizado por CIPSA			
8.10		Se controla el acceso al código fuente del sistema.	Optimizado	NA, realizado por CIPSA			
8.11		Los cambios se controlan mediante el uso de procedimientos de control de cambios.	Optimizado	NA, realizado por CIPSA			
8.12	Seguridad en los	Las aplicaciones se revisan después de haber hecho cambios en el sistema operativo, para observar el impacto generado.	Optimizado	NA, realizado por CIPSA			
8.13	procesos de	Se limita a los cambios necesarios (no se fomenta las modificaciones a los paquetes).	Optimizado	NA, realizado por CIPSA			
8.14	desarrollo y soporte	Se procura evitar las fugas o filtraciones de información.	Optimizado	NA, realizado por CIPSA			
8.15		Se supervisa y monitorea el desarrollo tercerizado de software.	Optimizado	NA, realizado por CIPSA			
8.16	Gestión de vulnerabilidades técnicas	Se procura minimizar la explotación de vulnerabilidades de los sistemas.	Optimizado	NA, realizado por CIPSA			
9	Gestión de Incidentes de seguridad de Información						
	Asegurar que los eventos y debilidades de seguridad de información sean comunicados de manera tal que, permita una acción correctiva						
9.1	Reporte de incidentes y debilidades	Los incidentes de Seguridad de la Información se reportan por los canales apropiados tan rápido como sea posible.	Optimizado	NA, realizado por CIPSA			
9.2		Se promueve que todo el personal reporte las debilidades de SI, que observe o sospeche.	Definido	Sensibilización de protección de datos	Delegado de Protección de datos	2º trimestre 2022	enviado y recibido
9.3	Gestión de incidentes y mejoras	Se dispone de procedimiento para respuesta rápida, eficaz y ordenada ante incidentes de SI.	Optimizado	NA, realizado por CIPSA			
9.4		Se dispone de mecanismos para aprender a resolver incidentes, que permitan cuantificar y realizar el seguimiento de los tipos, volúmenes y costos de los incidentes de SI.	Optimizado	NA, realizado por CIPSA			
9.5		Se recolecta y mantiene evidencias (para fines de auditoría).	Optimizado	NA, realizado por CIPSA			
10	Gestión de continuidad de operaciones						
	Contrarrestar las interrupciones de las actividades del negocio y proteger los procesos críticos, de los efectos de fallas significativas o						
10.1		Se dispone de un proceso de gestión de continuidad de operaciones.	Optimizado	NA, realizado por CIPSA			
10.2	Gestión de la continuidad operativa	Se realiza gestión de riesgos.	Optimizado	NA, realizado por CIPSA			
10.3		Se dispone de un Plan de Continuidad de Operaciones (PCO).	Optimizado	NA, realizado por CIPSA			
10.4		Se maneja un único marco referencial de PCO.	Optimizado	NA, realizado por CIPSA			
10.5		El PCO se prueba y actualiza en forma regular.	Optimizado	NA, realizado por CIPSA			
11	Cumplimiento regulatorio						
	Evitar el incumplimiento de cualquier ley, estatuto, obligación, reglamentación o contractuales, y de cualquier requisito de seguridad.						
11.1		Se ha definido, documentado y mantiene actualizado todos los requisitos legales, reglamentarios, contractuales pertinentes.	Definido	NA, ver documento de seguridad de la información			
11.2		Se dispone de procedimientos para respetar la propiedad intelectual.	Definido	NA, ver documento de seguridad de la información			
11.3	Con los requerimientos legales	Se protege los registros importantes de la organización.	Optimizado	NA, realizado por CIPSA			
11.4		Se protege la privacidad de la información personal, según la regulaciones.	Definido	NA, ver documento de seguridad de la información			
11.5		Se sensibiliza al personal para evitar usos no autorizados.	Definido	1. Sensibilización de protección de datos 2. Firma del comunicado al empleado	Delegado de Protección de datos	2º trimestre 2022	enviado y recibido
11.6		Se hace uso de cifrado, según las regulaciones.	Optimizado	NA, realizado por CIPSA			
11.7	Con las políticas y estándares de S.I.	Se procura el cumplimiento de los procedimientos de SI.	Definido	NA, ver documento de seguridad de la información			
11.8		Se procura el cumplimiento de la normativa de Seguridad de la Información en los sistemas de información.	Definido	NA, ver documento de seguridad de la información			
11.9	Auditoría de los sistemas de información	Se planifica las auditorías internas de sistemas de información.	Optimizado	NA, realizado por CIPSA			
11.10		Se protege el acceso a las herramientas de auditoría de sistemas de información.	Optimizado	NA, realizado por CIPSA			

TRANSCRITO

16/03/22



Código Seguro de Verificación	IV7DVXLTZEPXJO4IYW63XEI		Fecha	28/04/2022 15:07:45
Normativa	Este documento incorpora firma electrónica reconocida de acuerdo a la ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza			
Firmante	DIPUTACIÓN PROVINCIAL DE SALAMANCA (FRANCISCO JAVIER IGLESIAS GARCÍA) (PRESIDENTE DE LA DIPUTACIÓN)			
Firmante	ALEJANDRO MARTÍN GUZMÁN (SECRETARIO GENERAL)			
Un de verificación	https://sede.diputaciondesalamanca.gob.es/road/verifirma-moad/code/IV7DVXLTZEPXJO4IYW63XEI		Página	7/7