

§ 18 Esquema Nacional de Seguridad

- [op.exp.6.1] Se dispondrá de mecanismos de prevención y reacción frente a código dañino, incluyendo el correspondiente mantenimiento de acuerdo a las recomendaciones del fabricante.
- [op.exp.6.2] Se instalará software de protección frente a código dañino en todos los equipos: puestos de usuario, servidores y elementos perimetrales.
- [op.exp.6.3] Todo fichero procedente de fuentes externas será analizado antes de trabajar con él.
- [op.exp.6.4] Las bases de datos de detección de código dañino permanecerán permanentemente actualizadas.
- [op.exp.6.5] El software de detección de código dañino instalado en los puestos de usuario deberá estar configurado de forma adecuada e implementará protección en tiempo real de acuerdo a las recomendaciones del fabricante.

Refuerzo R1-Escaneo periódico.

- [op.exp.6.r1.1] Todo el sistema se escaneará regularmente para detectar código dañino.

Refuerzo R2-Revisión preventiva del sistema.

- [op.exp.6.r2.1] Las funciones críticas se analizarán al arrancar el sistema en prevención de modificaciones no autorizadas.

Refuerzo R3 - Lista blanca.

- [op.exp.6.r3.1] Solamente se podrán ejecutar aquellas aplicaciones previamente autorizadas. Se implementará una lista blanca para impedir la ejecución de aplicaciones no autorizadas.

Refuerzo R4-Capacidad de respuesta en caso de incidente.

- [op.exp.6.r4.1] Se emplearán herramientas de seguridad orientadas a detectar, investigar y resolver actividades sospechosas en puestos de usuario y servidores (EDR - *Endpoint Detection and Response*).

Refuerzo R5-Configuración de la herramienta de detección de código dañino.

- [op.exp.6.r5.1] El software de detección de código dañino permitirá realizar configuraciones avanzadas y revisar el sistema en el arranque y cada vez que se conecte un dispositivo extraíble.
- [op.exp.6.r5.2] El software de detección de código dañino instalado en servidores y elementos perimetrales deberá estar configurado de forma adecuada e implementará protección en tiempo real de acuerdo a las recomendaciones del fabricante.

Aplicación de la medida.

- Categoría BÁSICA: op.exp.6.
- Categoría MEDIA: op.exp.6+ R1 + R2.
- Categoría ALTA: op.exp.6+ R1 + R2 + R3 + R4.

4.3.7 Gestión de incidentes [op.exp.7].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1+R2	+ R1+R2+ R3

Requisitos.

- [op.exp.7.1] Se dispondrá de un proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema, que incluya el informe de eventos de seguridad y debilidades, detallando los criterios de clasificación y el escalado de la notificación.
- [op.exp.7.2] La gestión de incidentes que afecten a datos personales tendrá en cuenta lo dispuesto en el Reglamento General de Protección de Datos; la Ley Orgánica 3/2018, de 5

§ 18 Esquema Nacional de Seguridad

de diciembre, en especial su disposición adicional primera, así como el resto de normativa de aplicación, sin perjuicio de los requisitos establecidos en este real decreto.

Refuerzo R1-Notificación.

– [op.exp.7.r1.1] Se dispondrá de soluciones de ventanilla única para la notificación de incidentes al CCN-CERT, que permita la distribución de notificaciones a las diferentes entidades de manera federada, utilizando para ello dependencias administrativas jerárquicas.

Refuerzo R2 –Detección y Respuesta.

El proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema ([op.exp.7.1]) deberá incluir:

– [op.exp.7.r2.1] Implantación 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.

– [op.exp.7.r2.2] Asignación de recursos para investigar las causas, analizar las consecuencias y resolver el incidente.

– [op.exp.7.r2.3] Informar del incidente a los responsables de la información y servicios afectados y de las actuaciones llevadas a cabo para su resolución.

– [op.exp.7.r2.4] Medidas para:

a) Prevenir que se repita el incidente.

b) Incluir en los procedimientos de usuario la identificación y forma de tratar el incidente.

c) Actualizar, extender, mejorar u optimizar los procedimientos de resolución de incidentes.

Refuerzo R3-Reconfiguración dinámica.

La reconfiguración dinámica del sistema persigue detener, desviar o limitar ataques, acotando los daños.

– [op.exp.7.r3.1] La reconfiguración dinámica incluye, por ejemplo, cambios en las reglas de los enrutadores (*routers*), listas de control de acceso, parámetros del sistema de detección / prevención de intrusiones y reglas en los cortafuegos y puertas de enlace, aislamiento de elementos críticos y aislamiento de las copias de seguridad.

– [op.exp.7.r3.2] El organismo adaptará los procedimientos de reconfiguración dinámica reaccionando a los anuncios recibidos del CCN-CERT relativos a ciberamenazas sofisticadas y campañas de ataques.

Refuerzo R4-Prevención y Respuesta Automática.

– [op.exp.7.r4.1] Se dispondrá de herramientas que automaticen el proceso de prevención y respuesta mediante la detección e identificación de anomalías, la segmentación dinámica de la red para reducir la superficie de ataque, el aislamiento de dispositivos críticos, etc.

Aplicación de la medida.

– Categoría BÁSICA: op.exp.7.

– Categoría MEDIA: op.exp.7+ R1 + R2.

– Categoría ALTA: op.exp.7+ R1 + R2 + R3.

4.3.8 Registro de la actividad [op.exp.8].

dimensiones	T		
nivel	BAJO	MEDIO	ALTO
	aplica	+R1+R2+R3+R4	+R1+R2+R3+R4+R5

Requisitos.

Se registrarán las actividades en el sistema, de forma que:

- [op.exp.8.1] Se generará un registro de auditoría, que incluirá, al menos, el identificador del usuario o entidad asociado al evento, fecha y hora, sobre qué información se realiza el evento, tipo de evento y el resultado del evento (fallo o éxito), según la política de seguridad y los procedimientos asociados a la misma.
- [op.exp.8.2] Se activarán los registros de actividad en los servidores.

Refuerzo R1-Revisión de los registros.

- [op.exp.8.r1.1] Se revisarán informalmente, de forma periódica, los registros de actividad, buscando patrones anormales.

Refuerzo R2-Sincronización del reloj del sistema.

- [op.exp.8.r2.1] El sistema deberá disponer de una referencia de tiempo (*timestamp*) para facilitar las funciones de registro de eventos y auditoría. La modificación de la referencia de tiempo del sistema será una función de administración y, en caso de realizarse su sincronización con otros dispositivos, deberán utilizarse mecanismos de autenticación e integridad.

Refuerzo R3-Retención de registros.

- [op.exp.8.r3.1] En la documentación de seguridad del sistema se deberán indicar los eventos de seguridad que serán auditados y el tiempo de retención de los registros antes de ser eliminados.

Refuerzo R4-Control de acceso.

- [op.exp.8.r4.1] Los registros de actividad y, en su caso, las copias de seguridad de los mismos, solamente podrán ser accedidos o eliminarse por personal debidamente autorizado.

Refuerzo R5-Revisión automática y correlación de eventos.

- [op.exp.8.r5.1] El sistema deberá implementar herramientas para analizar y revisar la actividad del sistema y la información de auditoría, en búsqueda de comprometimientos de la seguridad posibles o reales.
- [op.exp.8.r5.2] Se dispondrá de un sistema automático de recolección de registros, correlación de eventos y respuesta automática ante los mismos.

Aplicación de la medida (por trazabilidad).

- Nivel BAJO: op.exp.8.
- Nivel MEDIO: op.exp.8 + R1 + R2 + R3 + R4.
- Nivel ALTO: op.exp.8 + R1 + R2 + R3 + R4 + R5.

4.3.9 Registro de la gestión de incidentes [op.exp.9].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

Se registrarán todas las actuaciones relacionadas con la gestión de incidentes, de forma que:

- [op.exp.9.1] Se registrarán los reportes iniciales, intermedios y finales de los incidentes, las actuaciones de emergencia y las modificaciones del sistema derivadas del incidente.
- [op.exp.9.2] Se registrará aquella evidencia que pueda dirimirse en un ámbito jurisdiccional, especialmente cuando el incidente pueda comportar acciones disciplinarias sobre el personal interno, sobre proveedores externos o en la persecución de delitos. En la determinación de la composición y detalle de estas evidencias, se recurrirá a asesoramiento legal especializado.
- [op.exp.9.3] Como consecuencia del análisis de los incidentes, se revisará la determinación de los eventos auditables.

§ 18 Esquema Nacional de Seguridad

Aplicación de la medida.

- Categoría BÁSICA: op.exp.9.
- Categoría MEDIA: op.exp.9.
- Categoría ALTA: op.exp.9.

4.3.10 Protección de claves criptográficas [op.exp.10].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+ R1

Requisitos.

- [op.exp.10.1] Las claves criptográficas se protegerán durante todo su ciclo de vida: (1) generación, (2) transporte al punto de explotación, (3) custodia durante la explotación, (4) archivo posterior a su retirada de explotación activa y (5) destrucción final.
- [op.exp.10.2] Los medios de generación estarán aislados de los medios de explotación.
- [op.exp.10.3] Las claves retiradas de operación que deban ser archivadas, lo serán en medios aislados de los de explotación.

Refuerzo R1-Algoritmos autorizados.

- [op.exp.10.r1.1] Se emplearán algoritmos y parámetros autorizados por el CCN.

Refuerzo R2-Protección avanzada de claves criptográficas.

- [op.exp.10.r2.1] Se emplearán cifradores que cumplan con los requisitos establecidos en la guía CCN-STIC que sea de aplicación.

Aplicación de la medida.

- Categoría BÁSICA: op.exp.10.
- Categoría MEDIA: op.exp.10 + R1.
- Categoría ALTA: op.exp.10 + R1.

4.4 Recursos externos [op.ext].

Cuando la organización utilice recursos externos (servicios, productos, instalaciones o personal), mantendrá la plena responsabilidad de los riesgos para la información tratada o los servicios prestados, debiendo adoptar las medidas necesarias para ejercer su responsabilidad y mantener el control en todo momento.

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

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	aplica	aplica

Requisitos.

- [op.ext.1.1] Con anterioridad a la efectiva utilización de los recursos externos se establecerá contractualmente un Acuerdo de Nivel de Servicio, que incluirá las características del servicio prestado, lo que debe entenderse como «servicio mínimo admisible», así como, la responsabilidad del prestador y las consecuencias de eventuales incumplimientos.

Aplicación de la medida.

- Categoría BÁSICA: no aplica.
- Categoría MEDIA: op.ext.1.
- Categoría ALTA: op.ext.1.

4.4.2 Gestión diaria [op.ext.2].

§ 18 Esquema Nacional de Seguridad

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	aplica	aplica

Requisitos.

Se establecerá lo siguiente:

- [op.ext.2.1] Un sistema rutinario para medir el cumplimiento de las obligaciones de servicio, incluyendo el procedimiento para neutralizar cualquier desviación fuera del margen de tolerancia acordado ([op.ext.1]).
- [op.ext.2.2] El mecanismo y los procedimientos de coordinación para llevar a cabo las tareas de mantenimiento de los sistemas comprendidos en el acuerdo, que contemplarán los supuestos de incidentes y desastres (ver [op.exp.7]).

Aplicación de la medida.

- Categoría BÁSICA: no aplica.
- Categoría MEDIA: op.ext.2.
- Categoría ALTA: op.ext.2.

4.4.3 Protección de la cadena de suministro [op.ext.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	n.a.	aplica

Requisitos.

- [op.ext.3.1] Se analizará el impacto que puede tener sobre el sistema un incidente accidental o deliberado que tenga su origen en la cadena de suministro.
- [op.ext.3.2] Se estimará el riesgo sobre el sistema por causa del impacto estimado en el punto anterior.
- [op.ext.3.3] Se tomarán medidas de contención de los impactos estimados en los puntos anteriores.

Refuerzo R1-Plan de contingencia.

- [op.ext.3.r1.1] El plan de continuidad de la organización deberá tener en cuenta la dependencia de proveedores externos críticos.
- [op.ext.3.r1.2] Se deberán realizar pruebas o ejercicios de continuidad, incluyendo escenarios en los que falla un proveedor.

Refuerzo R2-Sistema de gestión de la seguridad.

- [op.ext.3.r2.1] Se implementará un sistema de protección de los procesos y flujos de información en las relaciones en línea (*online*) entre los distintos integrantes de la cadena de suministro.

Refuerzo R3-Lista de componentes software.

- [op.ext.3.r3.1] Se mantendrá actualizado un registro formal que contenga los detalles y las relaciones de la cadena de suministro de los diversos componentes utilizados en la construcción de programas informáticos, acorde a lo especificado en [mp.sw.1.r5]. Esta lista será proporcionada por el proveedor de la aplicación, librería o producto suministrado.

Aplicación de la medida.

- Categoría BÁSICA: no aplica.
- Categoría MEDIA: no aplica.
- Categoría ALTA: op.ext.3.

4.4.4 Interconexión de sistemas [op.ext.4].

Se denomina interconexión al establecimiento de enlaces con otros sistemas de información para el intercambio de información y servicios.

§ 18 Esquema Nacional de Seguridad

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	aplica	+ R1

Requisitos.

– [op.ext.4.1] Todos los intercambios de información y prestación de servicios con otros sistemas deberán ser objeto de una autorización previa. Todo flujo de información estará prohibido salvo autorización expresa.

– [op.ext.4.2] Para cada interconexión se documentará explícitamente: las características de la interfaz, los requisitos de seguridad y protección de datos y la naturaleza de la información intercambiada.

Refuerzo R1-Coordinación de actividades.

– [op.ext.4.r1.1] Cuando se interconecten sistemas en los que la identificación, autenticación y autorización tengan lugar en diferentes dominios de seguridad, bajo distintas responsabilidades, las medidas de seguridad locales se acompañarán de los correspondientes mecanismos y procedimientos de coordinación para la atribución y ejercicio efectivos de las responsabilidades de cada sistema.

Aplicación de la medida.

- Categoría BÁSICA: no aplica.
- Categoría MEDIA: op.ext.4.
- Categoría ALTA: op.ext.4 + R1.

4.5 Servicios en la nube [op.nub].

4.5.1 Protección de servicios en la nube [op.nub.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+R1+R2

Requisitos.

– [op.nub.1.1] Los sistemas que suministran un servicio en la nube a organismos del sector público deberán cumplir con el conjunto de medidas de seguridad en función del modelo de servicio en la nube que presten: Software como Servicio (*Software as a Service*, SaaS), Plataforma como Servicio (*Platform as a Service*, PaaS) e Infraestructura como Servicio (*Infrastructure as a Service*, IaaS) definidas en las guías CCN-STIC que sean de aplicación.

– [op.nub.1.2] Cuando se utilicen servicios en la nube suministrados por terceros, los sistemas de información que los soportan deberán ser conformes con el ENS o cumplir con las medidas desarrolladas en una guía CCN-STIC que incluirá, entre otros, requisitos relativos a:

- a) Auditoría de pruebas de penetración (*pentesting*).
- b) Transparencia.
- c) Cifrado y gestión de claves.
- d) Jurisdicción de los datos.

Refuerzo R1- Servicios certificados.

– [op.nub.1.r1.1] Cuando se utilicen servicios en la nube suministrados por terceros, estos deberán estar certificados bajo una metodología de certificación reconocida por el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información.

– [op.nub.1.r1.2] Si el servicio en la nube es un servicio de seguridad deberá cumplir con los requisitos establecidos en [op.pl.5].

Refuerzo R2-Guías de Configuración de Seguridad Específicas.

§ 18 Esquema Nacional de Seguridad

– [op.nub.1.r2.1] La configuración de seguridad de los sistemas que proporcionan estos servicios deberá realizarse según la correspondiente guía CCN-STIC de Configuración de Seguridad Específica, orientadas tanto al usuario como al proveedor.

Aplicación de la medida.

- Categoría BÁSICA: op.nub.1.
- Categoría MEDIA: op.nub.1 + R1.
- Categoría ALTA: op.nub.1+ R1 + R2.

4.6 Continuidad del servicio [op.cont].

4.6.1 Análisis de impacto [op.cont.1].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	aplica

Requisitos.

– [op.cont.1.1] Se realizará un análisis de impacto que permita determinar los requisitos de disponibilidad de cada servicio (impacto de una interrupción durante un periodo de tiempo determinado), así como los elementos que son críticos para la prestación de cada servicio.

Aplicación de la medida (por disponibilidad).

- Nivel BAJO: no aplica.
- Nivel MEDIO: op.cont.1.
- Nivel ALTO: op.cont.1.

4.6.2 Plan de continuidad [op.cont.2].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	n.a.	n.a.	aplica

Requisitos.

Se desarrollará un plan de continuidad que establezca las acciones a ejecutar en caso de interrupción de los servicios prestados con los medios habituales. Dicho plan contemplará los siguientes aspectos:

- [op.cont.2.1] Se identificarán funciones, responsabilidades y actividades a realizar.
- [op.cont.2.2] Existirá una previsión para coordinar la entrada en servicio de los medios alternativos de forma que se garantice poder seguir prestando los servicios esenciales de la organización.
- [op.cont.2.3] Todos los medios alternativos estarán planificados y materializados en acuerdos o contratos con los proveedores correspondientes.
- [op.cont.2.4] Las personas afectadas por el plan recibirán formación específica relativa a su papel en dicho plan.
- [op.cont.2.5] El plan de continuidad será parte integral y armónica de los planes de continuidad de la organización en otras materias ajenas a la seguridad.

Refuerzo R1-Plan de emergencia y contingencia.

– [op.cont.2.r1.1] Cuando se determine la necesidad de continuidad de los sistemas, deberá existir un plan de emergencia y contingencia en consonancia. En función del análisis de Impacto, se determinarán los aspectos a cubrir.

Refuerzo R2-Comprobación de integridad.

– [op.cont.2.r2.1] Ante una caída o discontinuidad del sistema, se deberá comprobar la integridad del sistema operativo, del firmware y de los ficheros de configuración.

Aplicación de la medida (por disponibilidad).

§ 18 Esquema Nacional de Seguridad

- Nivel BAJO: no aplica.
- Nivel MEDIO: no aplica.
- Nivel ALTO: op.cont.2.

4.6.3 Pruebas periódicas [op.cont.3].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	n.a.	n.a.	aplica

Requisitos.

- [op.cont.3.1] Se realizarán pruebas periódicas para localizar y, en su caso, corregir los errores o deficiencias que puedan existir en el plan de continuidad.

Aplicación de la medida (por disponibilidad).

- Nivel BAJO: no aplica.
- Nivel MEDIO: no aplica.
- Nivel ALTO: op.cont.3.

4.6.4 Medios alternativos [op.cont.4].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	n.a.	n.a.	aplica

Requisitos.

- [op.cont.4.1] Estará prevista la disponibilidad de medios alternativos para poder seguir prestando servicio cuando los medios habituales no estén disponibles. En concreto, se cubrirán los siguientes elementos del sistema:

- Servicios contratados a terceros.
- Instalaciones alternativas.
- Personal alternativo.
- Equipamiento informático alternativo.
- Medios de comunicación alternativos.

- [op.cont.4.2] Se establecerá un tiempo máximo para que los medios alternativos entren en funcionamiento.

- [op.cont.4.3] Los medios alternativos estarán sometidos a las mismas garantías de seguridad que los originales.

Refuerzo R1-Automatización de la transición a medios alternativos.

- [op.cont.4.r1.1] El sistema dispondrá de elementos hardware o software que permitan la transferencia de los servicios automáticamente a los medios alternativos.

Aplicación de la medida (por disponibilidad).

- Nivel BAJO: no aplica.
- Nivel MEDIO: no aplica.
- Nivel ALTO: op.cont.4.

4.7 Monitorización del sistema [op.mon].

El sistema estará sujeto a medidas de monitorización de su actividad y ejecutará acciones predeterminadas en función de las situaciones de compromiso de la seguridad que figuren en el análisis de riesgos. Esto puede incluir la generación de alarmas en tiempo real, la finalización del proceso que está ocasionando la alarma, la inhabilitación de determinados servicios, la desconexión de usuarios y el bloqueo de cuentas.

4.7.1 Detección de intrusión [op.mon.1].

§ 18 Esquema Nacional de Seguridad

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+R1+R2

Requisitos.

- [op.mon.1.1] Se dispondrá de herramientas de detección o prevención de intrusiones.

Refuerzo R1-Detección basada en reglas.

- [op.mon.1.r1.1] El sistema dispondrá de herramientas de detección o prevención de intrusiones basadas en reglas.

Refuerzo R2-Procedimientos de respuesta.

- [op.mon.1.r2.1] Existirán procedimientos de respuesta a las alertas generadas por el sistema de detección o prevención de intrusiones.

Refuerzo R3-Acciones predeterminadas.

- [op.mon.1.r3.1] El sistema ejecutará automáticamente acciones predeterminadas de respuesta a las alertas generadas. Esto puede incluir la finalización del proceso que está ocasionando la alerta, la inhabilitación de determinados servicios, la desconexión de usuarios y el bloqueo de cuentas.

Aplicación de la medida.

- Categoría BÁSICA: op.mon.1.
- Categoría MEDIA: op.mon.1 + R1.
- Categoría ALTA: op.mon.1+ R1 + R2.

4.7.2 Sistema de métricas [op.mon.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1+R2	+ R1+R2

Requisitos.

- [op.mon.2.1] Atendiendo a la categoría de seguridad del sistema, se recopilarán los datos necesarios para conocer el grado de implantación de las medidas de seguridad que resulten aplicables y, en su caso, para proveer el informe anual requerido por el artículo 32.

Refuerzo R1-Efectividad del sistema de gestión de incidentes.

- [op.mon.2.r1.1] Se recopilarán los datos precisos que posibiliten evaluar el comportamiento del sistema de gestión de incidentes, de acuerdo con la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad y con la correspondiente guía CCN-STIC.

Refuerzo R2-Eficiencia del sistema de gestión de la seguridad.

- [op.mon.2.r2.1] Se recopilarán los datos precisos para conocer la eficiencia del sistema de seguridad, en relación con los recursos consumidos, en términos de horas y presupuesto.

Aplicación de la medida.

- Categoría BÁSICA: op.mon.2.
- Categoría MEDIA: op.mon.2 + R1+ R2.
- Categoría ALTA: op.mon.2 + R1 + R2.

4.7.3 Vigilancia [op.mon.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA

§ 18 Esquema Nacional de Seguridad

	aplica	+ R1+R2	+ R1+R2+R3+R4+R5+R6
--	--------	---------	---------------------

Requisitos.

– [op.mon.3.1] Se dispondrá de un sistema automático de recolección de eventos de seguridad.

Refuerzo R1-Correlación de eventos.

– [op.mon.3.r1.1] Se dispondrá de un sistema automático de recolección de eventos de seguridad que permita la correlación de los mismos.

Refuerzo R2-Análisis dinámico.

– [op.mon.3.r2.1] Se dispondrá de soluciones de vigilancia que permitan determinar la superficie de exposición con relación a vulnerabilidades y deficiencias de configuración.

Refuerzo R3-Ciberamenazas avanzadas.

– [op.mon.3.r3.1] Se dispondrá de sistemas para detección de amenazas avanzadas y comportamientos anómalos.

– [op.mon.3.r3.2] Se dispondrá de sistemas para la detección de amenazas persistentes avanzadas (*Advanced Persistent Threat, APT*) mediante la detección de anomalías significativas en el tráfico de la red.

Refuerzo R4-Observatorios digitales.

– [op.mon.3.r4.1] Se dispondrá de observatorios digitales con fines de cibervigilancia dedicados a la detección y seguimiento de anomalías que pudieran representar indicadores de amenaza en contenidos digitales.

Refuerzo R5-Minería de datos.

Se aplicarán medidas para prevenir, detectar y reaccionar frente a intentos de minería de datos:

– [op.mon.3.r5.1] Limitación de las consultas, monitorizando volumen y frecuencia.

– [op.mon.3.r5.2] Alerta a los administradores de seguridad de comportamientos sospechosos en tiempo real.

Refuerzo R6-Inspecciones de seguridad.

Periódicamente, o tras incidentes que hayan desvelado vulnerabilidades del sistema nuevas o subestimadas, se realizarán las siguientes inspecciones:

– [op.mon.3.r6.1] Verificación de configuración.

– [op.mon.3.r6.2] Análisis de vulnerabilidades.

– [op.mon.3.r6.3] Pruebas de penetración.

Refuerzo R7-Interconexiones.

– [op.mon.3.r7.1] En las interconexiones que lo requieran se aplicarán controles en los flujos de intercambio de información a través del uso de metadatos.

Aplicación de la medida.

– Categoría BÁSICA: op.mon.3.

– Categoría MEDIA: op.mon.3 + R1 + R2.

– Categoría ALTA: op.mon.3 + R1 + R2 + R3 + R4 + R5 + R6.

5. Medidas de protección [mp]

Las medidas de protección estarán dirigidas a proteger activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad.

5.1 Protección de las instalaciones e infraestructuras [mp.if].

5.1.1 Áreas separadas y con control de acceso [mp.if.1].

§ 18 Esquema Nacional de Seguridad

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

- [mp.if.1.1] El equipamiento del Centro de Proceso de Datos (CPD) se instalará, en la medida de lo posible, en áreas separadas, específicas para su función.
- [mp.if.1.2] Se controlarán los accesos a las áreas indicadas de forma que sólo se pueda acceder por las entradas previstas.

Aplicación de la medida.

- Categoría BÁSICA: mp.if.1.
- Categoría MEDIA: mp.if.1.
- Categoría ALTA: mp.if.1.

5.1.2 Identificación de las personas [mp.if.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

[mp.if.2.1] El procedimiento de control de acceso identificará a las personas que accedan a los locales donde hay equipamiento esencial que forme parte del sistema de información del CPD, registrando las correspondientes entradas y salidas.

Aplicación de la medida.

- Categoría BÁSICA: mp.if.2.
- Categoría MEDIA: mp.if.2.
- Categoría ALTA: mp.if.2.

5.1.3 Acondicionamiento de los locales [mp.if.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

Los locales donde se ubiquen los sistemas de información y sus componentes esenciales dispondrán de elementos adecuados para el eficaz funcionamiento del equipamiento allí instalado, y, en especial, para asegurar:

- [mp.if.3.1] Las condiciones de temperatura y humedad.
- [mp.if.3.2] La protección frente a las amenazas identificadas en el análisis de riesgos.
- [mp.if.3.3] La protección del cableado frente a incidentes fortuitos o deliberados.

Aplicación de la medida.

- Categoría BÁSICA: mp.if.3.
- Categoría MEDIA: mp.if.3.
- Categoría ALTA: mp.if.3.

5.1.4 Energía eléctrica [mp.if.4].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1	+ R1

§ 18 Esquema Nacional de Seguridad

Requisitos.

– [mp.if.4.1] Los locales donde se ubiquen los sistemas de información y sus componentes esenciales dispondrán de tomas de energía eléctrica, de modo que se garantice el suministro y el correcto funcionamiento de las luces de emergencia.

Refuerzo R1-Suministro eléctrico de emergencia.

– [mp.if.4.r1.1] En caso de fallo del suministro principal, el abastecimiento eléctrico deberá estar garantizado durante el tiempo suficiente para una terminación ordenada de los procesos y la salvaguarda de la información.

Aplicación de la medida (por disponibilidad).

- Nivel BAJO: mp.if.4.
- Nivel MEDIO: mp.if.4 + R1.
- Nivel ALTO: mp.if.4 + R1.

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

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	aplica	aplica	aplica

Requisitos.

– [mp.if.5.1] Los locales donde se ubiquen los sistemas de información y sus componentes esenciales se protegerán frente a incendios atendiendo, al menos, a la normativa industrial de aplicación.

Aplicación de la medida (por disponibilidad).

- Nivel BAJO: mp.if.5.
- Nivel MEDIO: mp.if.5.
- Nivel ALTO: mp.if.5.

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

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	aplica

Requisitos.

– [mp.if.6.1] Los locales donde se ubiquen los sistemas de información y sus componentes esenciales se protegerán frente a incidentes causados por el agua.

Aplicación de la medida (por disponibilidad).

- Nivel BAJO: no aplica.
- Nivel MEDIO: mp.if.6.
- Nivel ALTO: mp.if.6.

5.1.7 Registro de entrada y salida de equipamiento [mp.if.7].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

– [mp.if.7.1] Se llevará un registro pormenorizado de cualquier entrada y salida de equipamiento esencial, incluyendo la identificación de la persona que autoriza el movimiento.

Aplicación de la medida.

§ 18 Esquema Nacional de Seguridad

- Categoría BÁSICA: mp.if.7.
- Categoría MEDIA: mp.if.7.
- Categoría ALTA: mp.if.7.

5.2 Gestión del personal [mp.per].

5.2.1 Caracterización del puesto de trabajo [mp.per.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	aplica	aplica

Requisitos.

- [mp.per.1.1] Para cada puesto de trabajo, relacionado directamente con el manejo de información o servicios, se definirán las responsabilidades en materia de seguridad, que estarán basadas en el análisis de riesgos.
- [mp.per.1.2] Se definirán los requisitos que deben satisfacer las personas que vayan a ocupar el puesto de trabajo, en particular, en términos de confidencialidad. Dichos requisitos se tendrán en cuenta en la selección de la persona que vaya a ocupar el puesto, incluyendo la verificación de sus antecedentes laborales, formación y otras referencias, de conformidad con el ordenamiento jurídico y el respeto a los derechos fundamentales.

Refuerzo R1-Habilitación Personal de Seguridad.

- [mp.per.1.r1.1] Los administradores de seguridad/sistema tendrán una Habilitación Personal de Seguridad (HPS) otorgada por la autoridad competente, como consecuencia de los resultados del análisis de riesgos previo o como requisito de seguridad de un sistema específico.

Aplicación de la medida.

- Categoría BÁSICA: no aplica.
- Categoría MEDIA: mp.per.1.
- Categoría ALTA: mp.per.1.

5.2.2 Deberes y obligaciones [mp.per.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+ R1

Requisitos.

Se informará a cada persona que trabaje en el sistema de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad, contemplando:

- [mp.per.2.1] Las medidas disciplinarias a que haya lugar.
- [mp.per.2.2] Contemplando tanto el periodo durante el cual se desempeña el puesto, como las obligaciones en caso de término de la asignación, o traslado a otro puesto de trabajo.
- [mp.per.2.3] El deber de confidencialidad respecto de los datos a los que tenga acceso, tanto durante el periodo que esté adscrito al puesto de trabajo, como posteriormente a su terminación.
- [mp.per.2.4] En caso de personal contratado a través de un tercero:
 - [mp.per.2.4.1] Se establecerán los deberes y obligaciones de cada parte y del personal contratado.
 - [mp.per.2.4.2] Se establecerá el procedimiento de resolución de incidentes relacionados con el incumplimiento de las obligaciones.

Refuerzo R1-Confirmación expresa.

§ 18 Esquema Nacional de Seguridad

– [mp.per.2.r1.1] Se ha de obtener la confirmación expresa de que los usuarios conocen las instrucciones de seguridad necesarias y obligatorias y su aceptación, así como los procedimientos necesarios para llevarlas a cabo de manera adecuada.

Aplicación de la medida.

- Categoría BÁSICA: mp.per.2.
- Categoría MEDIA: mp.per.2 + R1.
- Categoría ALTA: mp.per.2 + R1.

5.2.3 Concienciación [mp.per.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

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 recordará periódicamente:

- [mp.per.3.1] La normativa de seguridad relativa al buen uso de los equipos o sistemas y las técnicas de ingeniería social más habituales.
- [mp.per.3.2] La identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado.
- [mp.per.3.3] El procedimiento para informar sobre incidentes de seguridad, sean reales o falsas alarmas.

Aplicación de la medida.

- Categoría BÁSICA: mp.per.3.
- Categoría MEDIA: mp.per.3.
- Categoría ALTA: mp.per.3.

5.2.4 Formación [mp.per.4].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

– [mp.per.4.1] Se formará regularmente al personal en aquellas materias relativas a seguridad de la información que requiera el desempeño de sus funciones, en particular en lo relativo a:

- a) Configuración de sistemas.
- b) Detección y reacción ante incidentes.
- c) Gestión de la información en cualquier soporte en el que se encuentre. Se cubrirán al menos las siguientes actividades: almacenamiento, transferencia, copias, distribución y destrucción.

Además, se evaluará la eficacia de las acciones formativas llevadas a cabo.

Aplicación de la medida.

- Categoría BÁSICA: mp.per.4.
- Categoría MEDIA: mp.per.4.
- Categoría ALTA: mp.per.4.

5.3 Protección de los equipos [mp.eq].

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

§ 18 Esquema Nacional de Seguridad

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+ R1

Requisitos.

– [mp.eq.1.1] Los puestos de trabajo permanecerán despejados, sin que exista material distinto del necesario en cada momento.

Refuerzo R1-Almacenamiento del material.

– [mp.eq.1.r1.1] Una vez usado, y siempre que sea factible, el material se almacenará en lugar cerrado.

Aplicación de la medida.

- Categoría BÁSICA: mp.eq.1.
- Categoría MEDIA: mp.eq.1 + R1.
- Categoría ALTA: mp.eq.1 + R1.

5.3.2 Bloqueo de puesto de trabajo [mp.eq.2].

dimensiones	A		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	+ R1

Requisitos.

– [mp.eq.2.1] 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.

Refuerzo R1-Cierre de sesiones.

– [mp.eq.2.r1.1] Pasado un cierto tiempo, superior al anterior, se cancelarán las sesiones abiertas desde dicho puesto de trabajo.

Una Guía CCN-STIC concretará la implementación de la configuración de seguridad adaptada a la categorización del sistema o perfil de cumplimiento asociado.

Aplicación de la medida (por autenticidad).

- Nivel BAJO: no aplica.
- Nivel MEDIO: mp.eq.2.
- Nivel ALTO: mp.eq.2 + R1.

5.3.3 Protección de dispositivos portátiles [mp.eq.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	+R1+R2

Requisitos.

Los equipos (ordenadores portátiles, tabletas, etc.) que sean susceptibles de salir de las instalaciones de la organización y no puedan beneficiarse de la protección física correspondiente, con un riesgo manifiesto de pérdida o robo, serán protegidos adecuadamente.

Sin perjuicio de las medidas generales que les afecten, se adoptarán las siguientes:

- [mp.eq.3.1] Se llevará un inventario de dispositivos portátiles junto con una identificación de la persona responsable de cada uno de ellos y un control regular de que está positivamente bajo su control.
- [mp.eq.3.2] Se establecerá un procedimiento operativo de seguridad para informar al servicio de gestión de incidentes de pérdidas o sustracciones.

§ 18 Esquema Nacional de Seguridad

– [mp.eq.3.3] Cuando un dispositivo portátil se conecte remotamente a través de redes que no están bajo el estricto control de la organización, el ámbito de operación del servidor limitará la información y los servicios accesibles a los mínimos imprescindibles, requiriendo autorización previa de los responsables de la información y los servicios afectados. Este punto es de aplicación a conexiones a través de internet y otras redes que no sean de confianza.

– [mp.eq.3.4] Se evitará, en la medida de lo posible, que el dispositivo portátil contenga claves de acceso remoto a la organización que no sean imprescindibles. Se considerarán claves de acceso remoto aquellas que sean capaces de habilitar un acceso a otros equipos de la organización u otras de naturaleza análoga.

Refuerzo R1– Cifrado del disco.

– [mp.eq.3.r1.1] Se protegerá el dispositivo portátil mediante cifrado del disco duro cuando el nivel de confidencialidad de la información almacenada en el mismo sea de nivel MEDIO.

Refuerzo R2– Entornos protegidos.

– [mp.eq.3.r2.1] El uso de dispositivos portátiles fuera de las instalaciones de la organización se restringirá a entornos protegidos, donde el acceso sea controlado y a salvo de hurtos y miradas indiscretas.

Aplicación de la medida.

- Categoría BÁSICA: mp.eq.3.
- Categoría MEDIA: mp.eq.3.
- Categoría ALTA: mp.eq.3 + R1 + R2.

5.3.4 Otros dispositivos conectados a la red [mp.eq.4].

dimensiones	C		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1	+ R1

Esta medida afecta a todo tipo de dispositivos conectados a la red y que puedan tener en algún momento acceso a la información, tales como:

- a) Dispositivos multifunción: impresoras, escáneres, etc.
- b) Dispositivos multimedia: proyectores, altavoces inteligentes, etc.
- c) Dispositivos internet de las cosas, en inglés *Internet of Things (IoT)*.
- d) Dispositivos de invitados y los personales de los propios empleados, en inglés *Bring Your Own Device (BYOD)*.
- e) Otros.

Requisitos.

– [mp.eq.4.1] Los dispositivos presentes en el sistema deberán contar con una configuración de seguridad adecuada de manera que se garantice el control del flujo definido de entrada y salida de la información.

– [mp.eq.4.2] Los dispositivos presentes en la red que dispongan de algún tipo de almacenamiento temporal o permanente de información proporcionarán la funcionalidad necesaria para eliminar información de soportes de información. (Ver [mp.si.5]).

Refuerzo R1-Productos certificados.

– [mp.eq.4.r1.1] Se usarán, cuando sea posible, productos o servicios que cumplan lo establecido en [op.pl.5].

Refuerzo R2-Control de dispositivos conectados a la red.

– [mp.eq.4.r2.1] Se dispondrá de soluciones que permitan visualizar los dispositivos presentes en la red, controlar su conexión/desconexión a la misma y verificar su configuración de seguridad.

§ 18 Esquema Nacional de Seguridad

Aplicación de la medida (por confidencialidad).

- Nivel BAJO: mp.eq.4.
- Nivel MEDIO: mp.eq.4 + R1.
- Nivel ALTO: mp.eq.4+ R1.

5.4 Protección de las comunicaciones [mp.com].

5.4.1 Perímetro seguro [mp.com.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

- [mp.com.1.1] Se dispondrá de un sistema de protección perimetral que separe la red interna del exterior. Todo el tráfico deberá atravesar dicho sistema.
- [mp.com.1.2] Todos los flujos de información a través del perímetro deben estar autorizados previamente.

La Instrucción Técnica de Seguridad de Interconexión de Sistemas de Información determinará los requisitos establecidos en el perímetro que han de cumplir todos los componentes del sistema en función de la categoría.

Aplicación de la medida.

- Categoría BÁSICA: mp.com.1.
- Categoría MEDIA: mp.com.1.
- Categoría ALTA: mp.com.1.

5.4.2 Protección de la confidencialidad [mp.com.2].

dimensiones	C		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1	+R1+R2+R3

Requisitos.

- [mp.com.2.1] Se emplearán redes privadas virtuales cifradas cuando la comunicación discorra por redes fuera del propio dominio de seguridad.

Refuerzo R1-Algoritmos y parámetros autorizados.

- [mp.com.2.r1.1] Se emplearán algoritmos y parámetros autorizados por el CCN.

Refuerzo R2-Dispositivos hardware.

- [mp.com.2.r2.1] Se emplearán, dispositivos hardware en el establecimiento y utilización de la red privada virtual.

Refuerzo R3-Productos certificados.

- [mp.com.2.r3.1] Se usarán productos o servicios que cumplan lo establecido en [op.pl.5].

Refuerzo R4-Cifradores.

- [mp.com.2.r4.1] Se emplearán cifradores que cumplan con los requisitos establecidos en la guía CCN-STIC que sea de aplicación.

Refuerzo R5-Cifrado de información especialmente sensible.

- [mp.com.2.r5.1] Se cifrará toda la información transmitida.

Aplicación de la medida (por confidencialidad).

- Nivel BAJO: mp.com.2.

§ 18 Esquema Nacional de Seguridad

- Nivel MEDIO: mp.com.2 + R1.
- Nivel ALTO: mp.com.2 + R1 + R2+ R3.

5.4.3 Protección de la integridad y de la autenticidad [mp.com.3].

dimensiones	I A		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4

Requisitos.

– [mp.com.3.1] En comunicaciones con puntos exteriores al dominio propio de seguridad, se asegurará la autenticidad del otro extremo del canal de comunicación antes de intercambiar información. (Ver [op.acc.5]).

– [mp.com.3.2] Se prevendrán ataques activos garantizando que al ser detectados se activarán los procedimientos previstos de tratamiento del incidente. Se considerarán ataques activos:

- La alteración de la información en tránsito.
- La inyección de información espuria.
- El secuestro de la sesión por una tercera parte.

– [mp.com.3.3] Se aceptará cualquier mecanismo de identificación y autenticación de los previstos en el ordenamiento jurídico y en la normativa de aplicación.

Refuerzo R1-Redes privadas virtuales.

– [mp.com.3.r1.1] Se emplearán redes privadas virtuales cifradas cuando la comunicación discurra por redes fuera del propio dominio de seguridad.

Refuerzo R2-Algoritmos y parámetros autorizados.

– [mp.com.3.r2.1] Se emplearán algoritmos y parámetros autorizados por el CCN.

Refuerzo R3-Dispositivos hardware.

– [mp.com.3.r3.1] Se recomienda emplear dispositivos hardware en el establecimiento y utilización de la red privada virtual.

Refuerzo R4-Productos certificados.

– [mp.com.3.r4.1] Se emplearán productos certificados conforme a lo establecido en [op.pl.5].

Refuerzo R5-Cifradores.

– [mp.com.3.r5.1] Se emplearán cifradores que cumplan con los requisitos establecidos en la guía CCN-STIC que sea de aplicación.

Aplicación de la medida (por integridad y autenticidad).

- Nivel BAJO: mp.com.3.
- Nivel MEDIO: mp.com.3 + R1 + R2.
- Nivel ALTO: mp.com.3 + R1 + R2 + R3 + R4.

5.4.4 Separación de flujos de información en la red [mp.com.4].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	+ [R1oR2oR3]	+ [R2oR3]+R4

La segmentación acota el acceso a la información y, consiguientemente, la propagación de los incidentes de seguridad, que quedan restringidos al entorno donde ocurren.

Cuando la transmisión de información por la red se restringe a ciertos segmentos, se acota el acceso a la información y los incidentes de seguridad quedan encapsulados en su segmento.

§ 18 Esquema Nacional de Seguridad

Requisitos.

Los flujos de información se separarán en segmentos de forma que:

- [mp.com.4.1] El tráfico por la red se segregará para que cada equipo solamente tenga acceso a la información que necesita.
- [mp.com.4.2] Si se emplean comunicaciones inalámbricas, será en un segmento separado.

Refuerzo R1-Segmentación lógica básica.

- [mp.com.4.r1.1] Los segmentos de red se implementarán por medio de redes de área local virtuales (*Virtual Local Area Network, VLAN*).
- [mp.com.4.r1.2] La red que conforma el sistema deberá segregarse en distintas subredes contemplando como mínimo:

- Usuarios.
- Servicios.
- Administración.

Refuerzo R2-Segmentación lógica avanzada.

- [mp.com.4.r2.1] Los segmentos de red se implementarán por medio de redes privadas virtuales (*Virtual Private Network, VPN*).

Refuerzo R3-Segmentación física.

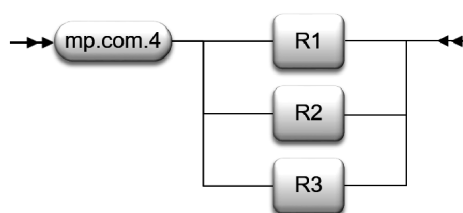
- [mp.com.4.r3.1] Los segmentos de red se implementarán con medios físicos separados.

Refuerzo R4-Puntos de interconexión.

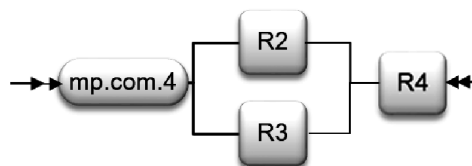
- [mp.com.4.r4.1] Control de entrada de los usuarios que llegan a cada segmento y control de entrada y salida de la información disponible en cada segmento.
- [mp.com.4.r4.2] El punto de interconexión estará particularmente asegurado, mantenido y monitorizado, (como en [mp.com.1]).

Aplicación de la medida.

- Categoría BÁSICA: no aplica.
- Categoría MEDIA: mp.com.4+ [R1o R2 o R3].



- Categoría ALTA: mp.com.4+[R2 o R3] + R4.



5.5 Protección de los soportes de información [mp.si].

5.5.1 Marcado de soportes [mp.si.1].

§ 18 Esquema Nacional de Seguridad

dimensiones	C		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	aplica

Requisitos.

– [mp.si.1.1] Los soportes de información (papel impreso, documentos electrónicos, contenidos multimedia -vídeos, cursos, presentaciones- etc.) que contengan información que según [mp.info.2] deba protegerse con medidas de seguridad específicas, llevarán las marcas o metadatos correspondientes que indiquen el nivel de seguridad de la información contenida de mayor calificación.

Refuerzo R1-Marca de agua digital.

– [mp.si.1.r1.1] La política de seguridad de la organización definirá marcas de agua para asegurar el uso adecuado de la información que se maneja.

– [mp.si.1.r1.2] Los soportes de información digital (documentos electrónicos, material multimedia, etc.) podrán incluir una marca de agua según la política de seguridad.

– [mp.si.1.r1.3] Los equipos o dispositivos a través de los que se accede a aplicaciones, escritorios remotos o virtuales, datos, etc., presentarán una marca de agua en pantalla según la política de seguridad.

Aplicación de la medida (por confidencialidad).

– Nivel BAJO: no aplica.

– Nivel MEDIO: mp.si.1.

– Nivel ALTO: mp.si.1.

5.5.2 Criptografía [mp.si.2].

dimensiones	C I		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	+ R1 + R2

Esta medida se aplica, en particular, a todos los dispositivos removibles cuando salen de un área controlada. Se entenderán por dispositivos removibles, los CD, DVD, discos extraíbles, *pendrives*, memorias USB u otros de naturaleza análoga.

Requisitos.

– [mp.si.2.1] Se usarán mecanismos criptográficos que garanticen la confidencialidad y la integridad de la información contenida.

– [mp.si.2.2] Se emplearán algoritmos y parámetros autorizados por el CCN.

Refuerzo R1– Productos certificados.

– [mp.si.2.r1.1] Se emplearán productos certificados conforme a lo establecido en [op.pl.5].

Refuerzo R2-Copias de seguridad.

– [mp.si.2.r2.1] Las copias de seguridad se cifrarán utilizando algoritmos y parámetros autorizados por el CCN.

Aplicación de la medida (por confidencialidad e integridad).

– Nivel BAJO: no aplica.

– Nivel MEDIO: mp.si.2.

– Nivel ALTO: mp.si.2 + R1 + R2.

5.5.3 Custodia [mp.si.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA

§ 18 Esquema Nacional de Seguridad

	aplica	aplica	aplica
--	--------	--------	--------

Requisitos.

- [mp.si.3.1] Se aplicará la debida diligencia y control a los soportes de información que permanecen bajo la responsabilidad de la organización, garantizando el control de acceso con medidas físicas ([mp.if.1] y [mp.if.7]) o lógicas ([mp.si.2]).
- [mp.si.3.2] Se respetarán las exigencias de mantenimiento del fabricante, en especial, en lo referente a temperatura, humedad y otros agentes medioambientales.

Aplicación de la medida.

- Categoría BÁSICA: mp.si.3.
- Categoría MEDIA: mp.si.3.
- Categoría ALTA: mp.si.3.

5.5.4 Transporte [mp.si.4].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

El responsable del sistema garantizará que los dispositivos permanecen bajo control y que satisfacen sus requisitos de seguridad mientras están siendo desplazados de un lugar a otro, fuera de las zonas controladas por la organización.

Requisitos.

- [mp.si.4.1] Se dispondrá de un registro de entrada/salida que identifique al transportista que entrega/recibe el soporte.
- [mp.si.4.2] Se dispondrá de un procedimiento rutinario que coteje las salidas con las llegadas y levante las alarmas pertinentes cuando se detecte algún incidente.
- [mp.si.4.3] Se utilizarán los medios de protección criptográfica ([mp.si.2]) correspondientes al mayor nivel de seguridad de la información contenida.
- [mp.si.4.4] Se gestionarán las claves según [op.exp.10].

Aplicación de la medida.

- Categoría BÁSICA: mp.si.4.
- Categoría MEDIA: mp.si.4.
- Categoría ALTA: mp.si.4.

5.5.5 Borrado y destrucción [mp.si.5].

dimensiones	C		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1	+ R1

La medida de borrado y destrucción de soportes de información se aplicará a todo tipo de equipos y soportes susceptibles de almacenar información, incluyendo medios electrónicos y no electrónicos.

Requisitos.

- [mp.si.5.1] Los soportes que vayan a ser reutilizados para otra información o liberados a otra organización serán objeto del borrado seguro de su contenido que no permita su recuperación. Cuando la naturaleza del soporte no permita un borrado seguro, el soporte no podrá ser reutilizado en ningún otro sistema.

Las guías CCN-STIC del CCN precisarán los criterios para definir como seguro un mecanismo de borrado o de destrucción, en función de la sensibilidad de la información almacenada en el dispositivo.

§ 18 Esquema Nacional de Seguridad

Refuerzo R1-Productos certificados.

- [mp.si.5.r1.1] Se usarán productos o servicios que cumplan lo establecido en [op.pl.5].

Refuerzo R2 - Destrucción de soportes.

- [mp.si.5.r2.1] Una vez finalizado el ciclo de vida del soporte de información, deberá ser destruido de forma segura conforme a los criterios establecidos por el CCN.

Aplicación de la medida (por confidencialidad).

- Nivel BAJO: mp.si.5.
- Nivel MEDIO: mp.si.5 + R1.
- Nivel ALTO: mp.si.5 + R1.

5.6 Protección de las aplicaciones informáticas [mp.sw].

5.6.1 Desarrollo de aplicaciones [mp.sw.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	+R1+R2+R3+R4	+R1+R2+R3+R4

Requisitos.

- [mp.sw.1.1] 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, ni datos de producción en el de desarrollo.

Refuerzo R1-Mínimo privilegio.

- [mp.sw.1.r1.1] Las aplicaciones se desarrollarán respetando el principio de mínimo privilegio, accediendo únicamente a los recursos imprescindibles para su función, y con los privilegios que sean indispensables.

Refuerzo R2-Metodología de desarrollo seguro.

- [mp.sw.1.r2.1] Se aplicará una metodología de desarrollo seguro reconocida que:
 - a) Tendrá en consideración los aspectos de seguridad a lo largo de todo el ciclo de vida.
 - b) Incluirá normas de programación segura, especialmente: control de asignación y liberación de memoria, desbordamiento de memoria (*overflow*).
 - c) Tratará específicamente los datos usados en pruebas.
 - d) Permitirá la inspección del código fuente.

Refuerzo R3-Seguridad desde el diseño.

- [mp.sw.1.r3.1] Los siguientes elementos serán parte integral del diseño del sistema:

- a) Los mecanismos de identificación y autenticación.
- b) Los mecanismos de protección de la información tratada.
- c) La generación y tratamiento de pistas de auditoría.

Refuerzo R4-Datos de pruebas.

- [mp.sw.1.r4.1] Preferiblemente, las pruebas previas a la implantación o modificación de los sistemas de información no se realizarán con datos reales. En caso de que fuese necesario recurrir a datos reales se garantizará el nivel de seguridad correspondiente.

Refuerzo R5-Lista de componentes software.

- [mp.sw.1.r5.1] El desarrollador elaborará y mantendrá actualizada una relación formal de los componentes software de terceros empleados en la aplicación o producto. Se mantendrá un histórico de los componentes utilizados en las diferentes versiones del software. El contenido mínimo de la lista de componentes, que contendrá, al menos, la identificación del componente, el fabricante y la versión empleada, se concretará en una guía CCN-STIC del CCN.

§ 18 Esquema Nacional de Seguridad

Aplicación de la medida.

- Categoría BÁSICA: no aplica.
- Categoría MEDIA: mp.sw.1 + R1 + R2 + R3 + R4.
- Categoría ALTA: mp.sw.1 + R1 + R2 + R3 + R4.

5.6.2 Aceptación y puesta en servicio [mp.sw.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+ R1

Requisitos.

Antes de pasar a producción se comprobará el correcto funcionamiento de la aplicación.

- [mp.sw.2.1] Se comprobará que:
 - a) Se cumplen los criterios de aceptación en materia de seguridad.
 - b) No se deteriora la seguridad de otros componentes del servicio.

Refuerzo R1- Pruebas.

- [mp.sw.2.r1.1] Las pruebas se realizarán en un entorno aislado (pre-producción).

Refuerzo R2-Inspección de código fuente.

- [mp.sw.2.r2.1] Se realizará una auditoría de código fuente.

Aplicación de la medida.

- Categoría BÁSICA: mp.sw.2.
- Categoría MEDIA: mp.sw.2 + R1.
- Categoría ALTA: mp.sw.2 + R1.

5.7 Protección de la información [mp.info].

5.7.1 Datos personales [mp.info.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

- [mp.info.1.1] Cuando el sistema trate datos personales, el responsable de seguridad recogerá los requisitos de protección de datos que sean fijados por el responsable o por el encargado del tratamiento, contando con el asesoramiento del DPD, y que sean necesarios implementar en los sistemas de acuerdo a la naturaleza, alcance, contexto y fines del mismo, así como de los riesgos para los derechos y libertades de acuerdo a lo establecido en los artículos 24 y 32 del RGPD, y de acuerdo a la evaluación de impacto en la protección de datos, si se ha llevado a cabo.

Aplicación de la medida.

- Categoría BÁSICA: mp.info.1.
- Categoría MEDIA: mp.info.1.
- Categoría ALTA: mp.info.1.

5.7.2 Calificación de la información [mp.info.2].

dimensiones	C		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	aplica

§ 18 Esquema Nacional de Seguridad

Requisitos.

- [mp.info.2.1] Para calificar la información se estará a lo establecido legalmente por las leyes y tratados internacionales de los que España es miembro y su normativa de aplicación cuando se trate de materias clasificadas. El valor a emplear en el caso de información de materias no clasificadas sería USO OFICIAL para información con algún tipo de restricción en su manejo por su sensibilidad y confidencialidad.
- [mp.info.2.2] La política de seguridad establecerá quién es el responsable de cada información manejada por el sistema.
- [mp.info.2.3] La política de seguridad recogerá, directa o indirectamente, los criterios que, en cada organización, determinarán el nivel de seguridad requerido, dentro del marco establecido en el artículo 40 y los criterios generales señalados en el anexo I.
- [mp.info.2.4] El responsable de cada información seguirá los criterios determinados en el apartado anterior para asignar a cada información el nivel de seguridad requerido, y será responsable de su documentación y aprobación formal.
- [mp.info.2.5] El responsable de cada información en cada momento tendrá en exclusiva la potestad de modificar el nivel de seguridad requerido, de acuerdo a los apartados anteriores.

Aplicación de la medida (por confidencialidad).

- Nivel BAJO: no aplica.
- Nivel MEDIO: mp.info.2.
- Nivel ALTO: mp.info.2.

5.7.3 Firma electrónica [mp.info.3].

dimensiones	I A		
nivel	BAJO	MEDIO	ALTO
	aplica	+R1+R2+R3	+ R1+R2+R3+R4

Requisitos.

- [mp.info.3.1] Se empleará cualquier tipo de firma electrónica de los previstos en el vigente ordenamiento jurídico, entre ellos, los sistemas de código seguro de verificación vinculados a la Administración Pública, órgano, organismo público o entidad de derecho público, en los términos y condiciones establecidos en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y en la Ley 40/2015, de 1 de octubre.

Refuerzo R1-Certificados cualificados.

- [mp.info.3.r1.1] Cuando se empleen sistemas de firma electrónica avanzada basados en certificados, estos serán cualificados.

Refuerzo R2-Algoritmos y parámetros autorizados.

- [mp.info.3.r2.1] Se emplearán algoritmos y parámetros autorizados por el CCN o por un esquema nacional o europeo que resulte de aplicación.

El CCN determinará los algoritmos criptográficos que hayan sido autorizados nominalmente para su uso en el Esquema Nacional de Seguridad conforme a la Instrucción Técnica de Seguridad Criptología de empleo en el ENS.

Refuerzo R3-Verificación y validación de firma.

- [mp.info.3.r3.1] Cuando proceda, se garantizará la verificación y validación de la firma electrónica durante el tiempo requerido por la actividad administrativa que aquella 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 se adjuntará a la firma, o se referenciará, toda la información pertinente para su verificación y validación, incluyendo certificados o datos de verificación y validación.

Refuerzo R4-Firma electrónica avanzada basada en certificados cualificados.

§ 18 Esquema Nacional de Seguridad

– [mp.info.3.r4.1] Se usará firma electrónica avanzada basada en certificados cualificados complementada por un segundo factor del tipo «algo que se sabe» o «algo que se es».

Refuerzo R5-Firma electrónica cualificada.

– [mp.info.3.r5.1] Se usará firma electrónica cualificada, empleando productos certificados conforme a lo establecido en [op.pl.5].

Aplicación de la medida (por integridad y autenticidad).

- Nivel BAJO: mp.info.3.
- Nivel MEDIO: mp.info.3 + R1 + R2 + R3.
- Nivel ALTO: mp.info.3 + R1 + R2 + R3 + R4.

5.7.4 Sellos de tiempo [mp.info.4].

dimensiones	T		
nivel	BAJO	MEDIO	ALTO
	n.a.	n.a.	aplica

Requisitos.

La utilización de sellos de tiempo exigirá adoptar las siguientes cautelas:

- [mp.info.4.1] Los sellos de tiempo se aplicarán a aquella información que sea susceptible de ser utilizada como evidencia electrónica en el futuro.
- [mp.info.4.2] Los datos pertinentes para la verificación posterior de la fecha serán tratados con la misma seguridad que la información fechada a efectos de disponibilidad, integridad y confidencialidad.
- [mp.info.4.3] Se renovarán regularmente los sellos de tiempo hasta que la información protegida ya no sea requerida por el proceso administrativo al que da soporte, en su caso.
- [mp.info.4.4] Se emplearán "sellos cualificados de tiempo electrónicos" atendiendo a lo dispuesto en el Reglamento (UE) n.º 910/2014 y normativa de desarrollo.

Refuerzo R1-Productos certificados.

- [mp.info.4.r1.1.] Se utilizarán productos certificados según [op.pl.5].
- [mp.info.4.r1.2] Se asignará una fecha y hora a un documento electrónico, conforme a lo establecido en la guía CCN-STIC Criptología de empleo en el ENS.

Aplicación de la medida (por trazabilidad).

- Nivel BAJO: no aplica.
- Nivel MEDIO: no aplica.
- Nivel ALTO: mp.info.4.

5.7.5 Limpieza de documentos [mp.info.5].

dimensiones	C		
nivel	BAJO	MEDIO	ALTO
	aplica	aplica	aplica

Requisitos.

- [mp.info.5.1] En el proceso de limpieza de documentos, se retirará de estos toda la información adicional contenida en campos ocultos, metadatos, comentarios o revisiones anteriores, salvo cuando dicha información sea pertinente para el receptor del documento.

Esta medida es especialmente relevante cuando el documento se difunde ampliamente, como ocurre cuando se ofrece al público en un servidor web u otro tipo de repositorio de información.

Aplicación de la medida (por confidencialidad).

§ 18 Esquema Nacional de Seguridad

- Nivel BAJO: mp.info.5.
- Nivel MEDIO: mp.info.5.
- Nivel ALTO: mp.info.5.

5.7.6 Copias de seguridad [mp.info.6].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1	+ R1 + R2

Requisitos.

– [mp.info.6.1] Se realizarán copias de seguridad que permitan recuperar datos perdidos, accidental o intencionadamente. La periodicidad y los plazos de retención de estas copias de seguridad se determinarán en la normativa interna de la organización relativa a copias de seguridad.

– [mp.info.6.2] Los procedimientos de respaldo establecidos indicarán:

- Frecuencia de las copias.
- Requisitos de almacenamiento en el propio lugar.
- Requisitos de almacenamiento en otros lugares.
- Controles para el acceso autorizado a las copias de respaldo.

Refuerzo R1-Pruebas de recuperación.

– [mp.info.6.r1.1] Los procedimientos de copia de seguridad y restauración deben probarse regularmente. Su frecuencia dependerá de la criticidad de los datos y del impacto que cause la falta de disponibilidad.

Refuerzo R2-Protección de las copias de seguridad.

– [mp.info.6.r2.1] Al menos, una de las copias de seguridad se almacenará de forma separada en lugar diferente, de tal manera que un incidente no pueda afectar tanto al repositorio original como a la copia simultáneamente.

- Nivel BAJO: mp.info.6.
- Nivel MEDIO: mp.info.6+ R1.
- Nivel ALTO: mp.info.6+ R1 + R2.

5.8 Protección de los servicios [mp.s].

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

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

El correo electrónico se protegerá frente a las amenazas que le son propias, actuando del siguiente modo:

- [mp.s.1.1] La información distribuida por medio de correo electrónico se protegerá, tanto en el cuerpo de los mensajes como en los anexos.
- [mp.s.1.2] Se protegerá la información de encaminamiento de mensajes y establecimiento de conexiones.

Se protegerá a la organización frente a problemas que se materializan por medio del correo electrónico, en concreto:

- [mp.s.1.3] Correo no solicitado, en su expresión inglesa «spam».
- [mp.s.1.4] Código dañino, constituidos por virus, gusanos, troyanos, espías, u otros de naturaleza análoga.
- [mp.s.1.5] Código móvil de tipo micro-aplicación, en su expresión inglesa «applet».

§ 18 Esquema Nacional de Seguridad

Se establecerán normas de uso del correo electrónico para el personal. (Ver [org.2]). Estas normas de uso contendrán:

- [mp.s.1.6] Limitaciones al uso como soporte de comunicaciones privadas.
- [mp.s.1.7] Actividades de concienciación y formación relativas al uso del correo electrónico.

Aplicación de la medida.

- Categoría BÁSICA: mp.s.1.
- Categoría MEDIA: mp.s.1.
- Categoría ALTA: mp.s.1.

5.8.2 Protección de servicios y aplicaciones web [mp.s.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	+R1oR2	+R1oR2	+R2+R3

Requisitos.

Los sistemas que prestan servicios web deberán ser protegidos frente a las siguientes amenazas:

- [mp.s.2.1] Cuando la información requiera control de acceso se garantizará la imposibilidad de acceder a la información obviando la autenticación, en particular, tomando medidas en los siguientes aspectos:

a) Se evitará que el servidor ofrezca acceso a los documentos por vías alternativas al protocolo determinado.

b) Se prevendrán ataques de manipulación del localizador uniforme de recursos (*Uniform Resource Locator, URL*).

c) Se prevendrán ataques de manipulación de fragmentos de información que se almacena en el disco duro del visitante de una página web a través de su navegador, a petición del servidor de la página, conocido en terminología inglesa como *cookies*.

d) Se prevendrán ataques de inyección de código.

- [mp.s.2.2] Se prevendrán intentos de escalado de privilegios.

- [mp.s.2.3] Se prevendrán ataques de *cross site scripting*.

Refuerzo R1-Auditorías de seguridad.

- [mp.s.2.r1.1] Se realizarán auditorías continuas de seguridad de «caja negra» sobre las aplicaciones web durante la fase de desarrollo y antes de la fase de producción.

- [mp.s.2.r1.2] La frecuencia de estas auditorías de seguridad quedará definida en el procedimiento de auditoría.

Refuerzo R2-Auditorías de seguridad avanzada.

- [mp.s.2.r2.1] Se realizarán auditorías de seguridad de «caja blanca» sobre las aplicaciones web durante la fase de desarrollo.

- [mp.s.2.r2.2] Se emplearán metodologías definidas y herramientas automáticas de detección de vulnerabilidades en la realización de las auditorías de seguridad sobre las aplicaciones web.

- [mp.s.2.r2.3] Una vez finalizada una auditoría de seguridad, se analizarán los resultados y se solventarán las vulnerabilidades encontradas mediante los procedimientos definidos [op.exp.5].

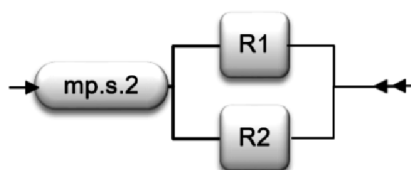
Refuerzo R3-Protección de las cachés.

- [mp.s.2.r3.1] Se prevendrán ataques de manipulación de programas o dispositivos que realizan una acción en representación de otros, conocidos en terminología inglesa como "*proxies*" y, sistemas especiales de almacenamiento de alta velocidad, conocidos en terminología inglesa como "*cachés*".

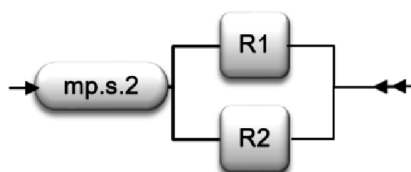
§ 18 Esquema Nacional de Seguridad

Aplicación de la medida.

- Categoría BÁSICA: mp.s.2 + [R1 o R2].



- Categoría MEDIA: mp.s.2 + [R1 o R2].



- Categoría ALTA: mp.s.2 + R2 + R3.

5.8.3 Protección de la navegación web [mp.s.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	+ R1

Requisitos.

El acceso de los usuarios internos a la navegación por internet se protegerá frente a las amenazas que le son propias, actuando del siguiente modo:

- [mp.s.3.1] Se establecerá una normativa de utilización, definiendo el uso que se autoriza y las limitaciones de uso personal. En particular, se concretará el uso permitido de conexiones cifradas.
- [mp.s.3.2] Se llevarán a cabo regularmente actividades de concienciación sobre higiene en la navegación web, fomentando el uso seguro y alertando de usos incorrectos.
- [mp.s.3.3] Se formará al personal encargado de la administración del sistema en monitorización del servicio y respuesta a incidentes.
- [mp.s.3.4] Se protegerá la información de resolución de direcciones web y de establecimiento de conexiones.
- [mp.s.3.5] Se protegerá a la organización en general y al puesto de trabajo en particular frente a problemas que se materializan vía navegación web.
- [mp.s.3.6] Se protegerá contra la actuación de programas dañinos tales como páginas activas, descargas de código ejecutable, etc., previniendo la exposición del sistema a vectores de ataque del tipo *spyware*, *ransomware*, etc.
- [mp.s.3.7] Se establecerá una política ejecutiva de control de cookies, en particular, para evitar la contaminación entre uso personal y uso organizativo.

Refuerzo R1 - Monitorización.

- [mp.s.3.r1.1] Se registrará el uso de la navegación web, estableciendo los elementos que se registran, el periodo de retención de estos registros y el uso que el organismo prevé hacer de ellos.
- [mp.s.3.r1.2] Se establecerá una función para la ruptura de canales cifrados a fin de inspeccionar su contenido, indicando qué se analiza, qué se registra, durante cuánto tiempo se retienen los registros y qué uso prevé hacer el organismo de estas inspecciones. Todo

§ 18 Esquema Nacional de Seguridad

ello sin perjuicio de que se puedan autorizar accesos cifrados singulares a destinos de confianza.

- [mp.s.3.r1.3] Se establecerá una lista negra de destinos vetados.

Refuerzo R2-Destinos autorizados.

- [mp.s.3.r2.1] Se establecerá una lista blanca de destinos accesibles. Todo acceso fuera de los lugares señalados en la lista blanca estará vetado, salvo autorización singular expresa.

Aplicación de la medida.

- Categoría BÁSICA: mp.s.3.
- Categoría MEDIA: mp.s.3.
- Categoría ALTA: mp.s.3 + R1.

5.8.4 Protección frente a la denegación de servicio [mp.s.4].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	+ R1

Requisitos.

Se establecerán medidas preventivas frente a ataques de denegación de servicio y denegación de servicio distribuido (*Denial of Service, DoS y Distributed Denial of Service, DDoS*). Para ello:

- [mp.s.4.1] Se planificará y dotará al sistema de capacidad suficiente para atender con holgura a la carga prevista.
- [mp.s.4.2] Se desplegarán tecnologías para prevenir los ataques conocidos.

Refuerzo R1-Detección y reacción.

- [mp.s.4.r1.1] Se establecerá un sistema de detección y tratamiento de ataques de denegación de servicio (DoS y DDoS).
- [mp.s.4.r1.2] Se establecerán procedimientos de reacción a los ataques, incluyendo la comunicación con el proveedor de comunicaciones.

Refuerzo R2-Ataques propios.

- [mp.s.4.r2.1] Se detectará y se evitará el lanzamiento de ataques desde las propias instalaciones perjudicando a terceros.

Aplicación de la medida (por disponibilidad).

- Nivel BAJO: no aplica.
- Nivel MEDIO: mp.s.4.
- Nivel ALTO: mp.s.4+ R1.

6. Valoración de la implantación de las medidas de seguridad

Es habitual el empleo de niveles de madurez para caracterizar la implementación de un proceso. El modelo de madurez de capacidad (*Capability Maturity Model, CMM*) permite describir las características que hacen un proceso efectivo, midiendo el grado o nivel de profesionalización de la actividad.

Un proceso es una colección de actividades o tareas relacionadas y estructuradas que, en una secuencia específica, proporciona un servicio para la organización.

Para la valoración de la implantación de las medidas de seguridad, éstas se analizarán como procesos y se estimará su nivel de madurez usando el modelo de madurez de capacidad (CMM).

Se identifican cinco "niveles de madurez", de modo que una organización que tenga institucionalizadas todas las prácticas incluidas en un nivel y sus inferiores, se considera que ha alcanzado ese nivel de madurez:

a) L0-Inexistente.

No existe un proceso que soporte el servicio requerido.

b) L1 - Inicial. Ad hoc.

Las organizaciones en este nivel no disponen de un ambiente estable para la prestación del servicio requerido. Aunque se utilicen técnicas correctas de ingeniería, los esfuerzos se ven minados por falta de planificación. El éxito de los proyectos se basa la mayoría de las veces en el esfuerzo personal, aunque a menudo se producen fracasos y casi siempre retrasos y sobrecostos. El resultado es impredecible. A menudo las soluciones se implementan de forma reactiva a los incidentes.

Los procedimientos de trabajo, cuando existen, son informales, incompletos y no se aplican de forma sistemática.

c) L2-Reproducible, pero intuitivo.

En este nivel las organizaciones disponen de unas prácticas institucionalizadas de gestión, existen unas métricas básicas y un razonable seguimiento de la calidad.

Existen procedimientos de trabajo, pero no están suficientemente documentados o no cubren todos los aspectos requeridos.

d) L3-Proceso definido.

Además de una buena gestión, a este nivel las organizaciones disponen de normativa y procedimientos detallados y documentados de coordinación entre grupos, formación del personal, técnicas de ingeniería, etc.

e) L4-Gestionado y medible.

Se caracteriza porque las organizaciones disponen de un conjunto de métricas de efectividad y eficiencia, que se usan de modo sistemático para la toma de decisiones y la gestión de riesgos. El servicio resultante es de alta calidad.

f) L5 - Optimizado.

La organización completa está volcada en la mejora continua de los procesos. Se hace uso intensivo de las métricas y se gestiona el proceso de innovación.

Para cada medida de seguridad que sea de aplicación al sistema de información se exigirá un determinado nivel de madurez. Los niveles mínimos de madurez requeridos por el ENS en función de la categoría del sistema son:

Categoría del sistema	Nivel mínimo de madurez requerido
BÁSICA	L2-Reproducible, pero intuitivo.
MEDIA	L3-Proceso definido.
ALTA	L4-Gestionado y medible.

7. Desarrollo y complemento de las medidas de seguridad

Las medidas de seguridad se desarrollarán y complementarán según lo establecido en la disposición final segunda.

8. Interpretación

La interpretación de este anexo se realizará según el sentido propio de sus palabras, en relación con el contexto, antecedentes históricos y legislativos, entre los que figura lo dispuesto en las instrucciones técnicas de seguridad y en las guías CCN-STIC que sean de aplicación a la implementación y a los diversos escenarios de aplicación tales como sedes electrónicas, servicios de validación de certificados electrónicos, servicios de fechado electrónico y validación de documentos fechados, atendiendo el espíritu y finalidad de aquellas.

ANEXO III

Auditoría de la seguridad

1. Objeto de la auditoría

1.1 La seguridad de los sistemas de información de una organización será auditada en los siguientes términos, al objeto de constatar:

- a) Que la política de seguridad define los roles y funciones de los responsables del sistema, la información, los servicios y la seguridad del sistema de información.
- b) Que existen procedimientos para resolución de conflictos entre dichos responsables.
- c) Que se han designado personas para dichos roles a la luz del principio de «diferenciación de responsabilidades».
- d) Que se ha realizado un análisis de riesgos, con revisión y aprobación anual.
- e) 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.
- f) Que existe un sistema de gestión de la seguridad de la información, documentado y con un proceso regular de aprobación por la dirección, tomando como base la Declaración de Aplicabilidad regulada en el artículo 28 de este real decreto.

1.2 La auditoría se basará en la existencia de evidencias que permitan sustentar objetivamente el cumplimiento de los siguientes puntos:

- a) Documentación de los procedimientos.
- b) Registro de incidentes.
- c) Examen del personal afectado: conocimiento y praxis de las medidas que le afectan.
- d) Productos certificados. Se considerará evidencia suficiente el empleo de productos que satisfagan lo establecido en artículo 19 «Adquisición de productos de seguridad y contratación de servicios de seguridad».

1.3 Se dispondrá de un programa o plan de auditorías documentado. Las actividades de auditoría que impliquen comprobaciones en los sistemas operativos deberán ser planificadas y acordadas previamente.

2. Niveles de auditoría

Los niveles de auditoría que se realizan a los sistemas de información serán los siguientes:

2.1 Auditoría a sistemas de categoría BÁSICA.

a) Los sistemas de información de categoría BÁSICA no necesitarán realizar una auditoría. Bastará una autoevaluación realizada por el mismo personal que administra el sistema de información o en quien éste delegue.

El resultado de la autoevaluación debe estar documentado, indicando si cada medida de seguridad está implantada y sujeta a revisión regular, así como las evidencias que sustentan la valoración anterior.

b) Los informes de autoevaluación serán analizados por el responsable de la seguridad competente, que elevará las conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.

2.2 Auditoría a sistemas de categoría MEDIA O ALTA.

a) El informe de auditoría dictaminará sobre el grado de cumplimiento de este real decreto e identificando los hallazgos de conformidad y no conformidad. Deberá, igualmente, incluir los criterios metodológicos de auditoría utilizados, el alcance y el objetivo de la auditoría, y los datos, hechos y observaciones en que se basen las conclusiones formuladas.

b) Los informes de auditoría serán analizados por el responsable de la seguridad competente, que presentará sus conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.

3. Interpretación

La interpretación de este anexo se realizará según el sentido propio de sus palabras, en relación con el contexto, antecedentes históricos y legislativos, entre los que figura lo dispuesto en la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los sistemas de información y en la guía CCN-STIC que sea de aplicación, atendiendo al espíritu y finalidad de aquellas.

ANEXO IV

Glosario

– Activo: componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

– Administrador del sistema/de la seguridad del sistema: persona encargada de la instalación y el mantenimiento de un sistema de información, implantando los procedimientos y la configuración de seguridad que se haya establecido en el marco de la política de seguridad del organismo.

– Análisis de riesgos: estudio de las consecuencias previsibles de un posible incidente de seguridad, considerando su impacto en la organización (en la protección de sus activos, en su misión, en su imagen o reputación, o en sus funciones) y la probabilidad de que ocurra.

– Área controlada: zona o área en la que una organización considera cumplidas las medidas de seguridad físicas y procedimentales requeridas para la protección de la información y los sistemas de información ubicados en ella.

– Arquitectura de seguridad: conjunto de elementos físicos y lógicos que forman parte de la arquitectura del sistema y cuyo objetivo es la protección de los activos dentro del sistema y en las interconexiones con otros sistemas.

– Auditoría de la seguridad: es un proceso sistemático, independiente y documentado que persigue la obtención de evidencias objetivas y su evaluación objetiva para determinar en qué medida se cumplen los criterios de auditoría en relación con la idoneidad de los controles de seguridad adoptados, el cumplimiento de la política de seguridad, las normas y los procedimientos operativos establecidos, y detectando desviaciones a los antedichos criterios.

– Autenticación: ratificación de la identidad de un usuario, proceso o dispositivo.

– Autenticación multifactor: exigencia de dos o más factores de autenticación para ratificar una autenticación como válida.

– Autenticador: algo, físico o inmaterial, que posee el usuario bajo su exclusivo control y que le distingue de otros usuarios.

– Autenticidad: propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

– Biometría (factor de autenticación): reconocimiento de los individuos en base a sus características biológicas o de comportamiento.

– Cadena de suministro: conjunto relacionado de recursos y procesos que comienza con la provisión de materias primas y se extiende a través de la entrega de productos o servicios al usuario final a través de los modos de transporte. Incluye a los proveedores (primer, segundo y tercer nivel), los almacenes de materia prima (directa o indirecta), las líneas de producción, los almacenes de productos terminados y los canales de distribución (mayoristas y minoristas), hasta llegar al cliente final.

– Categoría de seguridad de un sistema: es un grado, dentro de la escala Básica-Media-Alta, con el que se adjetiva un sistema de información a fin de seleccionar las medidas de seguridad necesarias para el mismo. La categoría de seguridad del sistema recoge la visión holística del conjunto de activos como un todo armónico, orientado a la prestación de unos servicios.

§ 18 Esquema Nacional de Seguridad

- Certificado de firma electrónica (factor de autenticación): una declaración electrónica que vincula los datos de validación de una firma con una persona física o jurídica y confirma, al menos, el nombre o el seudónimo de esa persona.
- Certificado cualificado de firma electrónica: un certificado de firma electrónica que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo I del Reglamento (UE) 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.
- Ciberamenaza: amenaza a los sistemas y servicios presentes en el ciberespacio o alcanzables a través de éste.
- Ciberataque: cualquier conducta dolosa de individuos u organizaciones, conocidos o no, desarrollada a través del ciberespacio contra sistemas de información, con el propósito de sustraer, alterar, abusar, desestabilizar, inutilizar, destruir o eliminar activos.
- Ciberespacio: dominio global y dinámico compuesto por infraestructuras de tecnología de la información -incluyendo internet-, redes de telecomunicaciones y sistemas de información que configura un ámbito virtual.
- Ciberincidente: Incidente relacionado con la seguridad de las tecnologías de la información y las comunicaciones que se produce en el ciberespacio.
- Ciberseguridad (seguridad de los sistemas de información): la capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos.
- Compromiso de la seguridad: incidente de seguridad en el que, debido a una violación de las medidas técnicas u organizativas de seguridad, una información o un servicio quedan expuestos, o potencialmente expuestos, a un acceso no autorizado.
- Confidencialidad: propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.
- Contraseña: un secreto memorizado por el usuario, compuesto por varios caracteres según unas reglas de complejidad frente a ataques de adivinación o fuerza bruta.
- Contraseña de un solo uso (OTP - *One-Time Password*): contraseña generada dinámicamente y que solamente se puede usar una vez y durante un periodo limitado.
- Disponibilidad: propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.
- Dispositivo de autenticación (*token*): autenticador físico.
- Distintivo de Certificación de Conformidad con el ENS: documento electrónico, en formato PDF-A, firmado electrónicamente por la Entidad de Certificación responsable de la evaluación de los sistemas de información concernidos, incluyendo un enlace a la Certificación de Conformidad con el ENS que, mientras se mantenga su vigencia, permanecerá accesible a través de la sede electrónica o página web de la entidad pública o privada, respectivamente, de que se trate.
- Distintivo de Declaración de Conformidad con el ENS: documento electrónico, en formato PDF-A, firmado o sellado electrónicamente por la entidad bajo cuya responsabilidad se encuentre el sistema de información en cuestión, incluyendo un enlace a la Declaración de Conformidad con el ENS que, mientras se mantenga su vigencia, permanecerá accesible a través de la sede electrónica o página web de la entidad pública o privada de que se trate.
- Dominio de seguridad: colección de activos uniformemente protegidos, típicamente bajo una única autoridad. Los dominios de seguridad se utilizan para diferenciar entre zonas en el sistema de información. Por ejemplo:
 - a) Instalaciones centrales, sucursales, comerciales trabajando con portátiles.
 - b) Servidor central (host), frontal Unix y equipos administrativos.
 - c) Seguridad física, seguridad lógica.
- Evento de seguridad: ocurrencia identificada de un sistema, servicio o estado de red que indica un posible incumplimiento de la política de seguridad de la información, una falla de los controles o una situación desconocida que puede ser relevante para la seguridad.

§ 18 Esquema Nacional de Seguridad

- Factor de autenticación: hay 3 tipos de factores de autenticación: (1) algo que se sabe, un secreto; (2) algo que se tiene, un autenticador; y (3) algo que se es, biometría.
- Firma electrónica: los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar.
- Firma electrónica avanzada: la firma electrónica que cumple los requisitos contemplados en el artículo 26 del Reglamento (UE) 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.
- Firma electrónica cualificada: una firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica.
- Gestión de incidentes: procedimientos seguidos para detectar, analizar y limitar un incidente y responder ante éste.
- Gestión de riesgos: actividades coordinadas para dirigir y controlar a una organización con respecto a los riesgos.
- Incidente de seguridad (ciberincidente o incidente): suceso inesperado o no deseado con consecuencias en detrimento de la seguridad de las redes y sistemas de información.
- Integridad: propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
- Lista de componentes software: documento que detalla los componentes software utilizados para construir algo, sea una aplicación o un servicio.
- Medidas de seguridad: conjunto de disposiciones encaminadas a proteger al sistema de información de los riesgos a los que estuviere sometido, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción, o de recuperación.
- Mínimo privilegio: principio que determina que el diseño de la arquitectura de seguridad de un sistema garantiza el uso de los servicios y permisos mínimos necesarios para su correcto funcionamiento.
- Monitorización continua: proceso de gestión dinámica de la seguridad basado en el seguimiento de indicadores críticos de seguridad y parcheo de las vulnerabilidades descubiertas en los componentes del sistema de información.
- Observatorio Digital: un observatorio digital, en su propósito de conocer realidades de la información que se transmite a través de medios digitales, es un conjunto de capacidades para la toma de decisiones dedicado a la detección y seguimiento de anomalías en el origen, definición o diseminación de contenidos digitales, las cuales pudieran representar indicadores de amenaza.
- Perfil de cumplimiento específico: conjunto de medidas de seguridad, comprendidas o no en el anexo II de este real decreto, que, como consecuencia del preceptivo análisis de riesgos, resulten de aplicación a una entidad o sector de actividad concreta y para una determinada categoría de seguridad, y que haya sido habilitado por el CCN.
- PIN: un secreto memorizado por el usuario, compuesto por unos pocos caracteres, siguiendo unas ciertas reglas frente a ataques de adivinación.
- Política de firma electrónica, sello electrónico y certificados: conjunto de normas de seguridad, de organización, técnicas y legales para determinar cómo se generan, verifican y gestionan firmas electrónicas y sellos electrónicos, incluyendo las características exigibles a los certificados de firma o sello electrónicos.
- Política de seguridad (Política de seguridad de la información): conjunto de directrices plasmadas en un documento, que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta.
- Principios básicos de seguridad: fundamentos que deben regir toda acción orientada a asegurar la información y los servicios.
- Proceso: conjunto organizado de actividades que se llevan a cabo para producir un producto o prestar un servicio, que tiene un principio y fin delimitados, que implica recursos y da lugar a un resultado.
- Proceso de seguridad: método que se sigue para alcanzar los objetivos de seguridad de la organización. El proceso se diseña para identificar, medir, gestionar y mantener bajo control los riesgos a que se enfrenta el sistema en materia de seguridad.

§ 18 Esquema Nacional de Seguridad

- Proceso TIC: conjunto de actividades llevadas a cabo para la concepción, elaboración, suministro y mantenimiento de un producto o servicio TIC.
- Producto TIC: elemento o grupo de elementos de las redes o los sistemas de información.
- Requisitos mínimos de seguridad: exigencias mínimas necesarias para asegurar la información tratada y los servicios prestados.
- Secreto memorizado (factor de autenticación): algo que solamente sabe el usuario autorizado. Típicamente, se concreta en una contraseña o un PIN.
- Sistema de información: cualquiera de los elementos siguientes:
 - 1.º Las redes de comunicaciones electrónicas que utilice la entidad del ámbito de aplicación de este real decreto sobre las que posea capacidad de gestión.
 - 2.º Todo dispositivo o grupo de dispositivos interconectados o relacionados entre sí, en el que uno o varios de ellos realicen, mediante un programa, el tratamiento automático de datos digitales.
 - 3.º Los datos digitales almacenados, tratados, recuperados o transmitidos mediante los elementos contemplados en los números 1.º y 2.º anteriores, incluidos los necesarios para el funcionamiento, utilización, protección y mantenimiento de dichos elementos.
- TEMPEST: término que hace referencia a las investigaciones y estudios de emanaciones comprometedoras (emisiones electromagnéticas no intencionadas, producidas por equipos eléctricos y electrónicos que, detectadas y analizadas, puedan llevar a la obtención de información) y a las medidas aplicadas a la protección contra dichas emanaciones.
- Trazabilidad: propiedad o característica consistente en que las actuaciones de una entidad (persona o proceso) pueden ser trazadas de forma indiscutible hasta dicha entidad.
- USO OFICIAL: designa información con algún tipo de restricción en su manejo por su sensibilidad y confidencialidad.
- Usuarios de la organización: personal del organismo, propio o contratado, estable o circunstancial, que acceden al sistema para desarrollar las funciones o actividades que les han sido encomendadas por la organización.
- Usuarios externos: usuarios con acceso al sistema que no entran en el conjunto de usuarios de la organización. En particular, los ciudadanos administrados.

NORMATIVA PARA INGRESO EN EL CUERPO GENERAL ADMINISTRATIVO DE LA ADMINISTRACIÓN DEL ESTADO

§ 19

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

Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática
«BOE» núm. 77, de 31 de marzo de 2021
Última modificación: 2 de abril de 2025
Referencia: BOE-A-2021-5032

La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, consagran el derecho de las personas a relacionarse por medios electrónicos con las administraciones públicas, simplificando el acceso a los mismos, y refuerzan el empleo de las tecnologías de la información y las comunicaciones (TIC) en las administraciones públicas, tanto para mejorar la eficiencia de su gestión como para potenciar y favorecer las relaciones de colaboración y cooperación entre ellas.

Ambas leyes recogen los elementos que conforman el marco jurídico para el funcionamiento electrónico de las Administraciones Públicas introduciendo un nuevo paradigma que supera la concepción que inspiró la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y su desarrollo reglamentario parcial en la Administración General del Estado y sus organismos públicos vinculados o dependientes a través del Real Decreto 1671/2009, de 6 de noviembre, según la cual la tramitación electrónica no era sino una forma de gestión de los procedimientos.

En este sentido, la Ley 11/2007, de 22 de junio, respondiendo a las nuevas realidades, exigencias y experiencias que se habían puesto de manifiesto, al propio desarrollo de la sociedad de la información y al cambio de circunstancias tecnológicas y sociales, entre otros factores, reconocía el derecho de la ciudadanía a relacionarse electrónicamente con las Administraciones Públicas, y no solo la posibilidad como se preveía en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. La Ley 11/2007, de 22 de junio admitía incluso que, por vía reglamentaria, se estableciese la obligatoriedad de comunicarse con las Administraciones Públicas por medios electrónicos cuando las personas interesadas fuesen personas jurídicas o colectivos de personas físicas que por razón de su capacidad económica o técnica, dedicación profesional u otros motivos acreditados tuviesen garantizado el acceso y disponibilidad de los medios tecnológicos precisos.

En este contexto, la Ley 39/2015, de 1 de octubre, y la Ley 40/2015, de 1 de octubre, han dado respuesta a la demanda actual en el sentido de que la tramitación electrónica de los procedimientos debe constituir la actuación habitual de las Administraciones Públicas, y no solamente ser una forma especial de gestión de los mismos. En consecuencia, se prevé que las relaciones de las Administraciones entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes se realizará a través de medios electrónicos, y se

§ 19 Reglamento de actuación y funcionamiento del sector público por medios electrónicos

establece la obligatoriedad de relacionarse electrónicamente con la Administración para las personas jurídicas, entes sin personalidad y, en algunos supuestos, para las personas físicas, y ello sin perjuicio de la posibilidad de extender esta obligación a otros colectivos, por vía reglamentaria.

Con estos antecedentes, era necesario desarrollar y concretar las previsiones legales con el fin, entre otros aspectos, de facilitar a los agentes involucrados en el uso de medios tecnológicos su utilización efectiva, aclarando y precisando, al mismo tiempo, aquellas materias reguladas en estas leyes que permiten un margen de actuación reglamentaria.

La satisfacción del interesado, por tanto, en el uso de los servicios públicos digitales es fundamental para garantizar adecuadamente sus derechos y el cumplimiento de sus obligaciones en su relación con las Administraciones Públicas. Por ello, es prioritario disponer de servicios digitales fácilmente utilizables y accesibles, de modo que se pueda conseguir que la relación del interesado con la Administración a través del canal electrónico sea fácil, intuitiva, efectiva, eficiente y no discriminatoria.

Por otra parte, a lo largo de las dos últimas décadas, los sucesivos Gobiernos de España han ido adoptando programas para el avance digital alineados con las agendas digitales europeas, en todos los cuales ha estado presente el eje de mejora de la Administración electrónica. Fruto de estos programas, España cuenta con una posición muy favorable para abordar la siguiente fase del proceso de Transformación digital de nuestro país y, en lo que concierne a la Administración electrónica, está situada entre los países más avanzados de la Unión Europea, lo que se ha logrado gracias al esfuerzo continuado de las Administraciones Públicas en la adaptación de sus servicios electrónicos para ofrecer cada vez mejores servicios, más adaptados a las demandas de la ciudadanía y las empresas, y más eficientes. En este esfuerzo, la estrategia de España se ha basado en el impulso de los fundamentos que permiten una tramitación electrónica completa, y en el desarrollo de servicios que pueden ser utilizados libremente por todas las Administraciones Públicas, y que están alineados con los esquemas de interoperabilidad europeos.

Los cambios que se están produciendo con la maduración de tecnologías disruptivas y su aplicación a la gestión de la información y la ejecución de políticas públicas, los nuevos modelos de relación de la ciudadanía y empresas con las Administraciones y la reutilización eficiente de la información son grandes desafíos que para ser afrontados con éxito y para que coadyuven a la Transformación digital exigen como presupuesto contar con un marco regulatorio adecuado, tanto con rango de ley como con rango reglamentario, que garantizando la seguridad jurídica para todos los intervinientes sirva a los objetivos de mejorar la eficiencia administrativa para hacer efectiva una Administración totalmente electrónica e interconectada, incrementar la transparencia de la actuación administrativa y la participación de las personas en la Administración Electrónica y garantizar servicios digitales fácilmente utilizables.

En este sentido, la Agenda España Digital 2025 contiene un eje estratégico específico sobre la Transformación Digital del Sector Público, cuya plasmación se concreta en el cumplimiento de un conjunto de medidas entre las que se encuentra la mejora del marco regulatorio de la Administración digital y específicamente en la aprobación de este real decreto. Por su parte, el Plan de Recuperación, Transformación y Resiliencia (España Puede) incluye entre sus diez políticas palanca de reforma estructural para un crecimiento sostenible e inclusivo, lograr una Administración modernizada a través de su digitalización, tanto a nivel transversal como en ámbitos estratégicos, que actúe como tractor de los cambios tecnológicos. El último hito en estrategia transformadora lo constituye el Plan de Digitalización de las Administraciones Públicas 2021 -2025, que supone un salto decisivo en la mejora de la eficacia y eficiencia de la Administración Pública, en la transparencia y eliminación de trabas administrativas a través de la automatización de la gestión, en una mayor orientación a la personalización de servicios y a la experiencia de usuario, actuando todo ello de elemento catalizador de la innovación tecnológica de nuestro país desde el ámbito público.

En definitiva, el Reglamento que aprueba este real decreto persigue los cuatro grandes objetivos mencionados: mejorar la eficiencia administrativa, incrementar la transparencia y la participación, garantizar servicios digitales fácilmente utilizables y mejorar la seguridad jurídica.

§ 19 Reglamento de actuación y funcionamiento del sector público por medios electrónicos

En primer lugar, persigue mejorar la eficiencia administrativa para hacer efectiva una Administración totalmente electrónica e interconectada. Así, se desarrolla y concreta el empleo de los medios electrónicos establecidos en las leyes 39/2015, de 1 de octubre, y 40/2015, de 1 de octubre, para garantizar, por una parte, que los procedimientos administrativos se tramiten electrónicamente por la Administración y, por otra, que la ciudadanía se relacione con ella por estos medios en los supuestos en que sea establecido con carácter obligatorio o aquellos lo decidan voluntariamente.

Un segundo objetivo consiste en incrementar la transparencia de la actuación administrativa y la participación de las personas en la Administración Electrónica. Así, se desarrolla el funcionamiento del Punto de Acceso General electrónico (PAGE), y la Carpeta ciudadana en el Sector Público Estatal. Se regula el contenido y los servicios mínimos a prestar por las sedes electrónicas y sedes electrónicas asociadas y el funcionamiento de los registros electrónicos.

En tercer lugar, el Reglamento persigue garantizar servicios digitales fácilmente utilizables de modo que se pueda conseguir que la relación del interesado con la Administración sea fácil, intuitiva y efectiva cuando use el canal electrónico.

Por último, busca mejorar la seguridad jurídica. Así, se elimina la superposición de regímenes jurídicos distintos, se adapta e integra en el Reglamento que aprueba este real decreto la regulación que aún permanecía vigente del Real Decreto 1671/2009, de 6 de noviembre, procediendo, por ello, a su derogación definitiva y se adecua la regulación al nuevo marco de la Ley 39/2015, de 1 de octubre y la Ley 40/2015, de 1 de octubre.

El real decreto consta de un artículo único que aprueba el Reglamento de actuación y funcionamiento del Sector Público por medios electrónicos, dos disposiciones transitorias, una disposición derogatoria y cinco disposiciones finales.

Entre las cinco disposiciones finales hay dos que modifican normas vigentes y las tres restantes regulan el título competencial, la habilitación reglamentaria para el desarrollo y ejecución del real decreto y la entrada en vigor. Respecto de las disposiciones modificativas, estas afectan al Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica y al Real Decreto 931/2017, de 27 de octubre, por el que se regula la Memoria del Análisis de Impacto Normativo. Así, en primer lugar, con relación al Real Decreto 4/2010, de 8 de enero, su artículo 29 establece que el Esquema Nacional de Interoperabilidad se desarrollará y perfeccionará a lo largo del tiempo en paralelo al progreso de los servicios de Administración electrónica, la evolución tecnológica y a medida que vayan consolidándose las infraestructuras que lo apoyan. Por ello, la rápida evolución de las tecnologías, la experiencia derivada de la aplicación del Esquema Nacional de Interoperabilidad desde su aprobación hace 10 años, las previsiones de la Ley 39/2015, de 1 de octubre, y de la Ley 40/2015, de 1 de octubre, relativas a la interoperabilidad entre las Administraciones Públicas y sus órganos, organismos públicos y entidades de derecho público vinculados o dependientes, más la necesidad de adecuarse a lo previsto en el Reglamento n.º 1025/2012 del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre la normalización europea, por el que se modifican las Directivas 89/686/CEE y 93/15/CEE del Consejo y las Directivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE y 2009/105/CE del Parlamento Europeo y del Consejo y por el que se deroga la Decisión 87/95/CEE del Consejo y la Decisión no 1673/2006/CE del Parlamento Europeo y del Consejo, determinan la necesidad de proceder a modificar ciertos aspectos de su redacción actual. En consecuencia, se modifican los artículos, 9, 11, 14, 16, 17, y 18, así como la disposición adicional primera y el anexo de glosario, a la vez que se suprimen el artículo 19 y las disposiciones adicionales tercera y cuarta.

En segundo lugar, se modifica el Real Decreto 931/2017, de 27 de octubre, para incorporar en la Memoria del Análisis de Impacto Normativo el análisis de la incidencia en los gastos en medios o servicios de la Administración digital dentro del impacto presupuestario de los proyectos y, por otra parte, para incluir dentro del apartado de «Otros impactos» el que tendrá para las personas destinatarias de la norma y para la organización y funcionamiento de la Administración el desarrollo o uso de los medios y servicios de la Administración digital que conlleve la aplicación de la normativa proyectada.

§ 19 Reglamento de actuación y funcionamiento del sector público por medios electrónicos

Por su parte, el Reglamento de actuación y funcionamiento del Sector Público por medios electrónicos que aprueba el real decreto consta de 65 artículos distribuidos en cuatro títulos, diez disposiciones adicionales y un anexo de definiciones.

El título preliminar del Reglamento comprende las disposiciones generales regulando el objeto y ámbito de aplicación de la norma (que se remite al ámbito del artículo 2 tanto de la Ley 39/2015, de 1 de octubre, como de la Ley 40/2015, de 1 de octubre) y los principios generales que debe respetar el sector público en sus actuaciones y relaciones electrónicas. Entre estos principios se incluyen el de neutralidad tecnológica y de adaptabilidad al progreso de las tecnologías y sistemas de comunicaciones electrónicas, para garantizar tanto la independencia en la elección de las alternativas tecnológicas necesarias para relacionarse con las Administraciones Públicas por parte de las personas interesadas y por el propio sector público, como la libertad para desarrollar e implantar los avances tecnológicos en un ámbito de libre mercado; el principio de accesibilidad, para promover que el diseño de los servicios electrónicos garantice la igualdad y no discriminación en el acceso de las personas usuarias, en particular, de las personas discapacitadas y de las personas mayores; el principio de facilidad de uso, que determina que el diseño de los servicios electrónicos esté centrado en las personas usuarias para minimizar el grado de conocimiento tecnológico necesario para el uso del servicio, el principio de interoperabilidad, entendido como la capacidad de los sistemas de información y, por ende, de los procedimientos a los que estos dan soporte, de compartir datos y posibilitar el intercambio de información entre ellos; el principio de proporcionalidad, para que las medidas de seguridad y garantías que se exijan sean adecuadas a la naturaleza y circunstancias de los distintos trámites y actuaciones electrónicas y, por último, el principio de personalización y proactividad, entendido como la capacidad de las Administraciones Públicas para que, partiendo del conocimiento adquirido del usuario final del servicio, proporcione servicios precumplimentados y se anticipe a las posibles necesidades de los mismos.

Asimismo el título preliminar regula el derecho y obligación de relacionarse electrónicamente con las Administraciones Públicas, en aplicación del artículo 14 de la Ley 39/2015, de 1 de octubre, y los canales a través de los cuales las Administraciones Públicas prestarán la asistencia necesaria para facilitar el acceso de las personas interesadas a los servicios electrónicos proporcionados en su ámbito.

El título I regula los portales de internet, el PAgE, las sedes electrónicas y sedes electrónicas asociadas (características, creación y supresión, contenido y servicios, y responsabilidad) y el área personalizada a través de la cual cada interesado podrá acceder a su información, al seguimiento de los trámites administrativos que le afecten y a las notificaciones y comunicaciones en el ámbito de la Administración Pública competente, que en el ámbito estatal se denomina «Carpeta Ciudadana».

El título II se subdivide en tres capítulos y regula el procedimiento administrativo por medios electrónicos. Así, el capítulo I, sobre «Disposiciones generales» aborda la tramitación administrativa automatizada y el régimen de subsanaciones. Por su parte el capítulo II regula la identificación y autenticación de las Administraciones Públicas y de las personas interesadas y se subdivide en cuatro Secciones: la 1ª aborda las disposiciones comunes a la identificación y autenticación y condiciones de interoperabilidad (incluyendo la plataforma de verificación de certificados electrónicos y otros sistemas de identificación), la 2ª regula la «Identificación electrónica de las Administraciones Públicas y la autenticación del ejercicio de su competencia», que comprende la identificación de las sedes electrónicas y sedes asociadas, la identificación mediante sello electrónico basado en certificado electrónico cualificado, los sistemas de firma electrónica para la actuación administrativa automatizada, la identificación y firma del personal al servicio de las Administraciones Públicas (incluidos los certificados de empleado público con número de identificación profesional) y la autenticación e identificación de las Administraciones emisoras y receptoras en intercambio de datos a través de entornos cerrados de comunicación. La sección 3ª desarrolla la regulación de la identificación y firma de las personas interesadas y, por último, la sección 4ª regula la acreditación de la representación de las personas interesadas (regulando, entre otros extremos, el registro electrónico de apoderamientos).

El título II se cierra con el capítulo III, que en sus dos secciones regula los Registros electrónicos, las notificaciones electrónicas y los otros actos de comunicación electrónicos.

§ 19 Reglamento de actuación y funcionamiento del sector público por medios electrónicos

Así, la sección 1ª regula los registros electrónicos (entre otros aspectos, el Registro Electrónico General de cada Administración y la presentación y tratamiento de documentos en registro o las competencias de las Oficinas de asistencia en materia de registros de la Administración General del Estado) y la sección 2ª regula las comunicaciones administrativas a las personas interesadas por medios electrónicos (actos de comunicación electrónica a las personas interesadas distintos de las notificaciones o publicaciones) y las notificaciones electrónicas (incluyendo las reglas generales de la práctica de las notificaciones electrónicas, el aviso de puesta a disposición de la notificación, la notificación a través de la Dirección Electrónica Habilitada única (DEHu) y la notificación electrónica en sede electrónica o sede electrónica asociada).

El título III regula el expediente electrónico y se divide en dos capítulos. El capítulo I regula el documento administrativo electrónico y los requisitos y la emisión de copias auténticas de documentos públicos administrativos o documentos privados, que sean originales o copias auténticas de originales; la formación del expediente administrativo electrónico y el ejercicio de acceso al mismo y a la obtención de copias y la destrucción de documentos. Por su parte, el capítulo II regula la conservación de documentos electrónicos y la definición de archivo electrónico único.

Por último, el título IV se divide en dos capítulos y regula las relaciones y colaboración entre Administraciones Públicas para el funcionamiento electrónico del sector público. Así, el capítulo I aborda la colaboración entre las Administraciones Públicas para la actuación administrativa por medios electrónicos e incluye las obligadas relaciones interadministrativas e interorgánicas por medios electrónicos en el ejercicio de sus competencias, las comunicaciones en la Administración General del Estado, la posibilidad de adhesión a sedes electrónicas y sedes electrónicas asociadas y la regulación del Sistema de Interconexión de Registros (SIR), a través del cual deberán realizarse las interconexiones entre Registros de las Administraciones Públicas, que deberán ser interoperables entre sí y, en el caso de la Administración General del Estado, lo que supone una novedad, también con los sistemas de gestión de expedientes.

El capítulo I del título IV regula también las transmisiones de datos a las que se refiere el artículo 155 de la Ley 40/2015 de 1 de octubre, las plataformas de intermediación de datos (con mención especial a la de ámbito estatal), la remisión electrónica de expedientes administrativos en el ámbito de las Administraciones públicas mediante puesta a disposición, a través de un nodo de interoperabilidad, de la dirección electrónica o localizador que dé acceso al expediente electrónico completo y, por último, las previsiones el intercambio automático de datos o documentos a nivel europeo previstos en el Reglamento (UE) n.º 2018/1724 del Parlamento Europeo y del Consejo, de 2 de octubre de 2018, relativo a la creación de una pasarela digital única de acceso a información, procedimientos y servicios de asistencia y resolución de problemas y por el que se modifica el Reglamento (UE) n.º 1024/2012.

El título IV finaliza con el capítulo II, que regula la transferencia y uso compartido de tecnologías entre Administraciones Públicas, abordando, por una parte, la reutilización de sistemas y aplicaciones de las Administraciones Públicas y, por otra, la adhesión a las plataformas, registros o servicios electrónicos de la Administración General del Estado

La parte final del Reglamento consta de diez disposiciones adicionales y un anexo de definiciones. Las primeras regulan la obligatoriedad de uso de medios electrónicos en los procesos selectivos para el acceso al empleo público en el ámbito de la Administración General del Estado; la promoción de la formación del personal al servicio de la Administración General del Estado para garantizar el derecho de las personas interesadas a ser asistidas en el uso de medios electrónicos en sus relaciones con la Administración Pública; la creación del nodo de interoperabilidad para la identificación electrónica del Reino de España para el reconocimiento mutuo de identidades electrónicas entre Estados miembros de la Unión Europea; la adhesión de las entidades de derecho privado vinculadas o dependientes de la Administración General del Estado, en el ejercicio de potestades administrativas, a las sedes electrónicas y sedes electrónicas asociadas y sistema de firma y notificaciones electrónicas aplicables; la adhesión de los órganos constitucionales al uso de las plataformas, registros o servicios electrónicos de la Administración General del Estado; la situación de las sedes electrónicas y subsedes electrónicas en el ámbito estatal existentes a

§ 19 Reglamento de actuación y funcionamiento del sector público por medios electrónicos

la entrada en vigor de este real decreto; la interoperabilidad de los registros electrónicos de apoderamientos; supletoriedad en Registro Civil; la autorización de los sistemas de identificación previstos en el artículo 9.2.c) y de los sistemas de firma previstos en el artículo 10.2.c) de la Ley 39/2015, de 1 de octubre y, por último, las especialidades por razón de materia.

El Reglamento concluye con un Anexo terminológico que retoma la buena praxis que incluía la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, en una materia de especial complejidad por la imbricación de categorías jurídicas y conceptos tecnológicos en permanente evolución.

El real decreto se ajusta a los principios de buena regulación contenidos en el artículo 129 de la Ley 39/2015, de 1 de octubre (principios de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia), en tanto que persigue un interés general al concretar determinados aspectos de la Ley 39/2015, de 1 de octubre y de la Ley 40/2015, de 1 de octubre, que van a facilitar el uso efectivo de los medios electrónicos de la Administración, y el desarrollo necesario de las citadas leyes. La norma es acorde con el principio de proporcionalidad al contener la regulación imprescindible para la consecución de los objetivos previamente mencionados. Igualmente, se ajusta al principio de seguridad jurídica, siendo coherente con el resto del ordenamiento jurídico, estableciéndose un marco normativo estable, integrado y claro. Asimismo, durante el procedimiento de elaboración de la norma, se han formalizado los trámites de consulta pública previa e información pública, que establece la Ley en cumplimiento del principio de transparencia, quedando además justificados en el preámbulo los objetivos que persigue este real decreto. Por último, en virtud del principio de eficiencia la norma no introduce ninguna variación, en materia de cargas administrativas, respecto de las leyes que con esta norma se desarrollan.

Asimismo, el proyecto ha sido informado por la Agencia Española de Protección de Datos y se ha sometido a consulta a las comunidades autónomas y a la Federación Española de Municipios y Provincias a través de la Comisión Sectorial de Administración Electrónica y a informe de los diferentes ministerios.

El real decreto se dicta en ejercicio de la habilitación normativa contenida en la disposición final sexta de la Ley 39/2015, de 1 de octubre, y en la disposición final decimoquinta de la Ley 40/2015, de 1 de octubre, para llevar a cabo su desarrollo reglamentario en lo referido a la gestión electrónica de los procedimientos y el funcionamiento electrónico del sector público y garantizar, así, la efectiva aplicación e implantación de las previsiones que ambas leyes establecen, todo ello al amparo de lo dispuesto en el artículo 149.1.18.^a de la Constitución. Los artículos 15,16, 23, 26, 28.2, 28.3 y 29.4 y la disposición adicional tercera del Reglamento, en cuanto a su relación con la ciberseguridad y su impacto en la seguridad de las redes y sistemas de información se dictan, además, de acuerdo con lo dispuesto en los artículos 149.1.21.^a y 149.1.29.^a de la Constitución, que atribuyen al Estado la competencia exclusiva en materia de telecomunicaciones y en materia de seguridad pública, respectivamente.

En su virtud, a propuesta de la Ministra de Asuntos Económicos y Transformación Digital y del Ministro de Política Territorial y Función Pública, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 30 de marzo de 2021,

DISPONGO:

Artículo único. *Aprobación del Reglamento de actuación y funcionamiento del sector público por medios electrónicos.*

Se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos, cuyo texto se incluye a continuación.

Disposición transitoria primera. *Destrucción de documentos en soporte no electrónico.*

(Anulada)

Disposición transitoria segunda. *Portales de internet existentes y aplicaciones específicas en el ámbito estatal.*

1. La supresión de los portales de internet creados en el ámbito estatal antes de la entrada en vigor de este real decreto se regirá por las reglas aplicables en el momento de su creación.

2. En el plazo de seis meses desde la entrada en vigor de este real decreto, en el ámbito de cada ministerio se analizará la oportunidad del mantenimiento de sus portales de internet existentes y los de sus organismos públicos o entidades de derecho público vinculados o dependientes respectivos, así como de las páginas web promocionales («microsites»). Para ese análisis se aplicarán los mismos criterios previstos en el artículo 6 para la creación de nuevos portales y se decidirá acerca de su mantenimiento o su supresión.

En caso de que se decida la supresión, se valorará si es pertinente o no incorporar en el PAgE de la Administración General del Estado la información que se ha contenido en dichos portales hasta la supresión.

3. Realizado el proceso previsto en el apartado anterior, en el plazo máximo de un año desde la entrada en vigor de este real decreto se publicará en el PAgE de la Administración General del Estado una Resolución del Secretario General de Función Pública, en la que figurará el listado de portales de internet activos de la Administración General del Estado y de los organismos públicos o entidades de derecho público vinculados o dependientes de esta.

4. En el plazo máximo de un año desde la entrada en vigor de este real decreto, y a partir de la información facilitada por los ministerios, la Secretaría General de Administración Digital realizará el censo de aplicaciones específicas diseñadas para dispositivos móviles («app») para su utilización en los procedimientos de la Administración General del Estado.

5. En el ámbito de la Administración General del Estado, los portales de internet muy reconocidos e identificables por los usuarios, creados antes de la entrada en vigor de este real decreto se regirán por las reglas aplicables en el momento de su creación en cuanto a nomenclatura, sin necesidad de que modifiquen el nombre del dominio de segundo nivel.

Disposición derogatoria única. *Derogación normativa.*

Quedan derogadas las disposiciones de igual o inferior rango que se opongan a lo dispuesto en este real decreto y, en concreto, el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

Disposición final primera. *Títulos competenciales.*

1. Este real decreto se dicta al amparo de lo dispuesto en el artículo 149.1.18.^a de la Constitución Española, que atribuye al Estado la competencia exclusiva en materia de procedimiento administrativo común y para dictar las bases del régimen jurídico de las Administraciones Públicas.

2. Los artículos 15, 16, 23, 26, 28.2, 28.3 y 29.4 y la disposición adicional tercera del Reglamento que aprueba este real decreto, en cuanto a su relación con la ciberseguridad y su impacto en la seguridad de las redes y sistemas de información se dictan, además, de acuerdo con lo dispuesto en los artículos 149.1.21.^a y 149.1.29.^a de la Constitución, que atribuyen al Estado la competencia exclusiva en materia de telecomunicaciones y en materia de seguridad pública, respectivamente.

3. No tiene carácter básico y será de aplicación únicamente en el ámbito estatal lo dispuesto en:

a) La disposición transitoria segunda y la disposición final tercera de este real decreto.

b) El segundo párrafo del apartado 3 del artículo 3, los artículos 6, 7.4, 8, 10.3, 10.4, 13.2, 17, 18.2, 19.3, 19.4, 21.4, 23.2, 24, 25.4, 28.3, 30.2, 31, 33, 36, 38.1, el segundo párrafo del apartado 4 del artículo 39, los artículos 40, 42.5, 48, 53.5, 55.2, 57, 60.3, 62.2 y las disposiciones adicionales primera, segunda, cuarta, quinta, sexta, el segundo apartado de la disposición adicional séptima del Reglamento que aprueba este real decreto.

Disposición final segunda. *Modificación del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.*

El Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica queda modificado como sigue:

Uno. El artículo 9 queda redactado del siguiente modo:

«Artículo 9. *Inventarios de información administrativa.*

1. Cada Administración Pública mantendrá actualizado el conjunto de sus inventarios de información administrativa que incluirá, al menos:

a) La relación de los procedimientos administrativos y servicios prestados de forma clasificada y estructurada. Las Administraciones Públicas conectarán electrónicamente sus inventarios con el Sistema de Información Administrativa gestionado por el Ministerio de Política Territorial y Función Pública en colaboración con el Ministerio de Asuntos Económicos y Transformación Digital.

b) La relación de sus órganos administrativos y oficinas orientadas al público y sus relaciones entre ellos. Dicho inventario se conectará electrónicamente con el Directorio Común de Unidades Orgánicas y Oficinas, gestionado por el Ministerio de Asuntos Económicos y Transformación Digital, en colaboración con el Ministerio de Política Territorial y Función Pública, que proveerá una codificación unívoca.

2. Cada Administración Pública regulará la creación y mantenimiento de estos dos inventarios, en las condiciones que se determinen, con carácter general, por las normas técnicas de interoperabilidad correspondientes; en su caso, las Administraciones Públicas podrán hacer uso de los citados Sistema de Información Administrativa y Directorio Común de Unidades Orgánicas y Oficinas para la creación y mantenimiento de sus propios inventarios. Para la descripción y modelización de los procedimientos administrativos y de los procesos que los soportan será de aplicación lo previsto sobre estándares en el artículo 11.»

Dos. El párrafo a) del artículo 11.3, queda redactado como sigue:

«a) El uso de las especificaciones técnicas de las TIC en la contratación pública junto con las definiciones de norma y especificación técnica establecidos en el Reglamento n.º 1025/2012, del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre normalización europea.»

Tres. Se modifica el artículo 14, que queda redactado como sigue:

«Artículo 14. *Plan de direccionamiento de la Administración.*

Las Administraciones Públicas aplicarán el Plan de direccionamiento e interconexión de redes en la Administración, desarrollado en la norma técnica de interoperabilidad correspondiente, para su interconexión a través de las redes de comunicaciones.»

Cuatro. Se modifica el artículo 16, que queda redactado como sigue:

«Artículo 16. *Condiciones de licenciamiento aplicables.*

1. Las condiciones de licenciamiento de las aplicaciones informáticas, documentación asociada, y cualquier otro objeto de información cuya titularidad de los derechos de la propiedad intelectual sea de una Administración Pública y permita su puesta a disposición de otra Administración y de los ciudadanos tendrán en cuenta los siguientes aspectos:

a) El fin perseguido es el aprovechamiento y la reutilización de recursos públicos.

b) La completa protección contra su apropiación exclusiva o parcial por parte de terceros.

c) La exención de responsabilidad del cedente por el posible mal uso por parte del cesionario.

d) La no obligación de asistencia técnica o de mantenimiento por parte del cedente.

e) La ausencia total de responsabilidad por parte del cedente con respecto al cesionario en caso de errores o mal funcionamiento de la aplicación.

f) El licenciamiento se realizará por defecto sin contraprestación y sin necesidad de establecer convenio alguno. Sólo se podrá acordar la repercusión parcial del coste de adquisición o desarrollo de las aplicaciones cedidas en aquellos casos en los que este pago repercuta directamente en el incremento de funcionalidades del activo cedido, incluya adaptaciones concretas para su uso en el organismo cesionario, o impliquen el suministro de servicios de asistencia o soporte para su reutilización en el organismo cesionario.

2. Las Administraciones Públicas utilizarán para las aplicaciones informáticas, documentación asociada, y cualquier otro objeto de información declarados como de fuentes abiertas aquellas licencias que aseguren que los programas, datos o información cumplen los siguientes requisitos:

a) Pueden ejecutarse para cualquier propósito.

b) Permiten conocer su código fuente.

c) Pueden modificarse o mejorarse.

d) Pueden redistribuirse a otros usuarios con o sin cambios siempre que la obra derivada mantenga estas cuatro garantías.

3. Para este fin se procurará la aplicación de la Licencia Pública de la Unión Europea, sin perjuicio de otras licencias que garanticen los mismos derechos expuestos en los apartados 1 y 2.

4. A efectos de facilitar el establecimiento de las condiciones de licenciamiento, las Administraciones Públicas incluirán en los pliegos de cláusulas técnicas de aquellos contratos que tengan por finalidad el desarrollo de nuevas aplicaciones informáticas, los siguientes aspectos:

a) Que la Administración contratante adquiera los derechos completos de propiedad intelectual de las aplicaciones y cualquier otro objeto de información que se desarrollen como objeto de ese contrato.

b) Que en el caso de reutilizar activos previamente existentes, la Administración contratante reciba un producto que pueda ofrecer para su reutilización posterior a otras Administraciones Públicas. Además, en el caso de partir de productos de fuentes abiertas, que sea posible declarar como de fuentes abiertas la futura aplicación desarrollada.»

Cinco. Se modifica el artículo 17, que queda redactado como sigue:

«Artículo 17. Directorios de aplicaciones reutilizables.

1. La Administración General del Estado mantendrá el Directorio general de aplicaciones para su libre reutilización, de acuerdo al artículo 158 de la Ley 40/2015, de 1 octubre, a través del Centro de Transferencia de Tecnología. Este directorio podrá ser utilizado por otras Administraciones Públicas. En el caso de disponer de un directorio propio, deberá garantizar que las aplicaciones disponibles en ese directorio propio se pueden consultar también a través del Centro de Transferencia de Tecnología.

2. Las Administraciones Públicas conectarán los directorios de aplicaciones para su libre reutilización entre sí; y con instrumentos equivalentes del ámbito de la Unión Europea.

3. Las Administraciones Públicas publicarán las aplicaciones reutilizables, en modo producto o en modo servicio, en los directorios de aplicaciones para su libre reutilización, con al menos el siguiente contenido:

a) Código fuente de las aplicaciones finalizadas, en el caso de ser reutilizables en modo producto y haber sido declaradas de fuentes abiertas.

b) Documentación asociada.

c) Condiciones de licenciamiento de todos los activos, en el caso de ser reutilizables en modo producto, o nivel de servicio ofrecido, en el caso de ser reutilizables en modo servicio.

d) Los costes asociados a su reutilización, en el caso de que existieran.

4. Las Administraciones procurarán la incorporación a la aplicación original de aquellas modificaciones o adaptaciones realizadas sobre cualquier aplicación que se haya obtenido desde un directorio de aplicaciones reutilizables.»

Seis. Se modifica el artículo 18, que queda redactado como sigue:

«Artículo 18. Interoperabilidad en la política de firma electrónica y de certificados.

1. La Administración General del Estado definirá una política de firma electrónica y de certificados que servirá de marco general de interoperabilidad para el reconocimiento mutuo de las firmas electrónicas basadas en certificados de documentos administrativos en las Administraciones Públicas.

Todos los organismos y entidades de derecho público de la Administración General del Estado aplicarán la política de firma electrónica y de certificados a que se refiere el párrafo anterior. La no aplicación de dicha política deberá ser justificada por el órgano u organismo competente y autorizada por la Secretaría General de Administración Digital.

2. Las restantes Administraciones Públicas podrán acogerse a la política de firma electrónica y de certificados a que hace referencia el apartado anterior.

3. Sin perjuicio de lo expuesto en el apartado anterior, las Administraciones Públicas podrán aprobar otras políticas de firma electrónica dentro de sus respectivos ámbitos competenciales.

Las políticas de firma electrónica que aprueben las Administraciones Públicas partirán de la norma técnica establecida a tal efecto en la disposición adicional primera, de los estándares técnicos existentes, y deberán ser interoperables con la política marco de firma electrónica mencionada en el apartado 1, en particular, con sus ficheros de implementación. La Administración Pública proponente de una política de firma electrónica particular garantizará su interoperabilidad con la citada política marco de firma electrónica y con sus correspondientes ficheros de implementación según las condiciones establecidas en la norma técnica de interoperabilidad recogida a tal efecto en la disposición adicional primera.

4. Al objeto de garantizar la interoperabilidad de las firmas electrónicas emitidas conforme a las políticas establecidas, las políticas de firma electrónica que las Administraciones Públicas aprueben deberán ser comunicadas, junto con sus correspondientes ficheros de implementación, a la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital.

5. Las Administraciones Públicas receptoras de documentos electrónicos firmados, siempre que hayan admitido con anterioridad la política de firma del emisor, permitirán la validación de las firmas electrónicas según la política de firma indicada en la firma del documento electrónico.

6. Los perfiles comunes de los campos de los certificados definidos por la política de firma electrónica y de certificados posibilitarán la interoperabilidad entre las aplicaciones usuarias, de manera que tanto la identificación como la firma electrónica generada a partir de estos perfiles comunes puedan ser reconocidos por las aplicaciones de las distintas Administraciones Públicas sin ningún tipo de restricción técnica, semántica u organizativa.

7. Los procedimientos en los que se utilicen certificados de firma electrónica deberán atenerse a la política de firma electrónica y de certificados aplicable en su ámbito, particularmente en la aplicación de los datos obligatorios y opcionales, las

§ 19 Reglamento de actuación y funcionamiento del sector público por medios electrónicos

reglas de creación y validación de firma electrónica, los algoritmos a utilizar y longitudes de clave mínimas aplicables.»

Siete. Se elimina el artículo 19.

Ocho. Se modifica la disposición adicional primera, que queda redactada como sigue:

«Disposición adicional primera. *Desarrollo del Esquema Nacional de Interoperabilidad.*

1. Se desarrollarán las siguientes normas técnicas de interoperabilidad que serán de obligado cumplimiento por parte de las Administraciones Públicas:

a) Norma Técnica de Catálogo de estándares: establecerá un conjunto de estándares que satisfagan lo previsto en el artículo 11 de forma estructurada y con indicación de los criterios de selección y ciclo de vida aplicados.

b) Norma Técnica de Documento electrónico: tratará los metadatos mínimos obligatorios, la asociación de los datos y metadatos de firma o de sellado de tiempo, así como otros metadatos complementarios asociados; y los formatos de documento.

c) Norma Técnica de Digitalización de documentos: tratará los formatos y estándares aplicables, los niveles de calidad, las condiciones técnicas y los metadatos asociados al proceso de digitalización.

d) Norma Técnica de Expediente electrónico: tratará de su estructura y formato, así como de las especificaciones de los servicios de remisión y puesta a disposición.

e) Norma Técnica de Política de firma electrónica y de certificados de la Administración: Tratará, entre otras cuestiones recogidas en su definición en el anexo, aquellas que afectan a la interoperabilidad incluyendo los formatos de firma, los algoritmos a utilizar y longitudes mínimas de las claves, las reglas de creación y validación de la firma electrónica, la gestión de las políticas de firma, el uso de las referencias temporales y de sello de tiempo, así como la normalización de la representación de la firma electrónica en pantalla y en papel para el ciudadano y en las relaciones entre las Administraciones Públicas.

f) Norma Técnica de Protocolos de intermediación de datos: tratará las especificaciones de los protocolos de intermediación de datos que faciliten la integración y reutilización de servicios en las Administraciones Públicas y que serán de aplicación para los prestadores y consumidores de tales servicios.

g) Norma Técnica de Relación de modelos de datos que tengan el carácter de comunes en la Administración y aquellos que se refieran a materias sujetas a intercambio de información con los ciudadanos y otras Administraciones.

h) Norma Técnica de Política de gestión de documentos electrónicos: incluirá directrices para la asignación de responsabilidades, tanto directivas como profesionales, y la definición de los programas, procesos y controles de gestión de documentos y administración de los repositorios electrónicos, y la documentación de los mismos, a desarrollar por las Administraciones Públicas y por los organismos públicos y entidades de derecho público vinculados o dependientes de aquellas.

i) Norma Técnica de Requisitos de conexión a la Red de comunicaciones de las Administraciones Públicas españolas.

j) Norma Técnica de Procedimientos de copiado auténtico y conversión entre documentos electrónicos, así como desde papel u otros medios físicos a formatos electrónicos.

k) Norma Técnica de Modelo de Datos para el intercambio de asientos entre las Entidades Registrales: tratará de aspectos funcionales y técnicos para el intercambio de asientos registrales, gestión de errores y excepciones, gestión de anexos, requerimientos tecnológicos y transformaciones de formatos.

l) Norma Técnica de Reutilización de recursos de información: tratará de las normas comunes sobre la localización, descripción e identificación unívoca de los recursos de información puestos a disposición del público por medios electrónicos para su reutilización.

m) Norma Técnica de interoperabilidad de inventario y codificación de objetos administrativos: tratará las reglas relativas a la codificación de objetos

administrativos, así como la conexión entre los inventarios correspondientes, incluyendo, por un lado, las unidades orgánicas y oficinas de la Administración, y, por otro lado, la información administrativa de procedimientos y servicios.

n) Norma Técnica de Interoperabilidad de Transferencia e Ingreso de documentos y expedientes electrónicos: tratará los requisitos y condiciones relativos a la transferencia de agrupaciones documentales en formato electrónico, documentos y expedientes electrónicos, junto con los metadatos asociados, entre sistemas de gestión de documentos electrónicos y sistemas de archivo electrónico.

ñ) Norma Técnica de Interoperabilidad de Valoración y Eliminación de documentos y expedientes electrónicos: tratará las condiciones y requisitos relativos a la valoración de los documentos y expedientes electrónicos para establecimiento de plazos de conservación, transferencia y acceso o, en su caso, eliminación total o parcial.

o) Norma Técnica de Interoperabilidad de preservación de documentación electrónica: tratará las condiciones y requisitos relativos a la conservación de los documentos electrónicos para garantizar su autenticidad, integridad, confidencialidad, disponibilidad y trazabilidad, así como la protección, recuperación y conservación física y lógica de los documentos y su contexto.

p) Norma Técnica de Interoperabilidad de tratamiento y preservación de bases de datos: tratará las condiciones y requisitos relativos a la conservación de las bases de datos para garantizar su autenticidad, integridad, confidencialidad, disponibilidad y trazabilidad, y permitiendo la protección, recuperación y conservación física y lógica de los datos y su contexto.

q) Norma Técnica de Interoperabilidad de Plan de Direccionamiento: tratará reglas aplicables a la asignación y requisitos de direccionamiento IP para garantizar la correcta administración de la Red de comunicaciones de las Administraciones Públicas españolas y evitar el uso de direcciones duplicadas.

r) Norma Técnica de Interoperabilidad de reutilización de activos en modo producto y en modo servicio: tratará los requisitos y condiciones para facilitar la reutilización de activos tanto en modo producto como en modo servicio por las Administraciones Públicas españolas.

s) Norma Técnica de Interoperabilidad del modelo de datos y condiciones de interoperabilidad de los registros de funcionarios habilitados: tratará los aspectos funcionales y técnicos para la plena interoperabilidad de los registros electrónicos de funcionarios habilitados pertenecientes a las Administraciones, así como la interconexión de estos a las sedes electrónicas.

t) Norma Técnica de Interoperabilidad del modelo de datos y condiciones de interoperabilidad de los registros electrónicos de apoderamientos: tratará los aspectos funcionales y técnicos para la plena interoperabilidad de los registros electrónicos de apoderamientos pertenecientes a las Administraciones, así como la interconexión de estos a las sedes electrónicas, A los registros mercantiles, de la propiedad, y a los protocolos notariales.

u) Norma Técnica de Interoperabilidad de Sistema de Referencia de documentos y repositorios de confianza: tratará los requisitos técnicos que deberán cumplir las referencias a documentos al ser intercambiadas, de forma que se evite trasladar documentación de forma innecesaria.

v) Norma Técnica de Política de firma electrónica y de certificados en el ámbito estatal: tratará las directrices y normas técnicas aplicables a la utilización de certificados y firma electrónica dentro de su ámbito de aplicación, organizadas alrededor de los conceptos de generación y validación de firma e incluirá los perfiles interoperables de los medios de identificación de las Administraciones Públicas previstos en Ley 40/2015, de 1 de octubre.

2. El Ministerio de Asuntos Económicos y Transformación Digital, a propuesta de la Comisión Sectorial de Administración Electrónica prevista en la disposición adicional novena de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, aprobará las normas técnicas de interoperabilidad y las publicará mediante Resolución de la Secretaría de Estado de Digitalización e Inteligencia Artificial.

3. Para la redacción y actualización de las normas técnicas de interoperabilidad indicadas en el apartado 1 y las futuras que pueda aprobar el Ministerio de Asuntos Económicos y Transformación Digital que sean necesarias para garantizar el adecuado nivel de interoperabilidad como consecuencia del nivel de desarrollo tecnológico, los compromisos internacionales o el marco normativo aplicable, se constituirán los correspondientes grupos de trabajo en los órganos colegiados con competencias en materia de Administración electrónica.

Para garantizar la debida interoperabilidad en materia de ciberseguridad y criptografía, en relación con la aplicación del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la administración electrónica, el órgano competente será el Centro Criptológico Nacional, adscrito al Centro Nacional de Inteligencia.

4. Se desarrollarán los siguientes instrumentos para la interoperabilidad:

a) Sistema de Información Administrativa: Inventario de procedimientos administrativos, servicios prestados y otras actuaciones administrativas que generen documentación pública, conteniendo información de los mismos clasificada por funciones y con indicación de su nivel de informatización, así como información acerca de las interfaces al objeto de favorecer la interacción o en su caso la integración de los procesos.

b) Centro de interoperabilidad semántica de la Administración: Almacenará, publicará y difundirá los modelos de datos de los servicios de interoperabilidad entre Administraciones Públicas y de estas con los ciudadanos, tanto comunes como sectoriales, así como los relativos a infraestructuras y servicios comunes, además de las especificaciones semánticas y codificaciones relacionadas. Su propósito es facilitar la comprensión semántica de los servicios de intercambio de datos de las Administraciones y maximizar la reutilización de activos semánticos en la construcción de éstos. Se conectará con otros instrumentos equivalentes de las Administraciones Públicas y del ámbito de la Unión Europea.

c) Centro de Transferencia de Tecnología: Directorio de aplicaciones para su libre reutilización que contendrá la relación de aplicaciones para su libre reutilización, incluyendo, al menos, los datos descriptivos relativos a nombre de la aplicación, breve descripción de sus funcionalidades, uso y características, licencia, principales estándares abiertos aplicados, y estado de desarrollo.

d) Directorio Común de Unidades Orgánicas y Oficinas de las Administraciones Públicas: Instrumento que permitirá la sincronización de los sistemas que traten la información de inventariado, codificación y evolución de unidades orgánicas y oficinas en diferentes modalidades de integración para garantizar la flexibilidad tanto en el consumo como en la provisión de información relacionada.»

Nueve. Se suprime la disposición adicional tercera.

Diez. Se suprime la disposición adicional cuarta.

Once. Se modifica el anexo de la forma siguiente:

1. Se suprime el término « Familia».

2. A continuación del término «Índice electrónico» se sustituye el vigente término «Infraestructuras y servicios comunes» por el término «Infraestructura o servicio común» con la siguiente redacción:

«Infraestructura o servicio común: capacidad organizativa y técnica que satisface necesidades comunes de los usuarios en diversos ámbitos de la Administración, junto con su gobernanza operativa de apoyo, que pueden tener carácter horizontal o sectorial, con diversos modos de provisión, como servicio o como producto, o integración a modo de plataforma, que facilitan la interoperabilidad, la seguridad, las economías de escala, la racionalización y la simplificación de la actuación administrativa.»

3. A continuación del término «Estándar abierto» se introduce el término «Ficheros de implementación de las políticas de firma» con la siguiente redacción:

«Ficheros de implementación de las políticas de firma: Son la representación en lenguaje formal (XML o ASN.1) de las condiciones establecidas en la política de firma, acorde a las normas técnicas establecidas por los organismos de estandarización.»

Disposición final tercera. *Modificación del Real Decreto 931/2017, de 27 de octubre, por el que se regula la Memoria del Análisis de Impacto Normativo.*

Se modifican el párrafo segundo de la letra d) y la letra g) del apartado 1 del artículo 2 del Real Decreto 931/2017, de 27 de octubre, por el que se regula la Memoria del Análisis de Impacto Normativo, que quedan redactados como sigue:

«2.º El Impacto presupuestario comprenderá, al menos, una referencia a los efectos en los ingresos y gastos públicos e incluirá la incidencia en los gastos de personal, dotaciones o retribuciones, gastos en medios o servicios de la Administración digital o cualesquiera otros gastos al servicio del sector público.»

«g) Otros impactos: La memoria del análisis de impacto normativo incluirá cualquier otro extremo que pudiera ser relevante a criterio del órgano proponente, prestando especial atención a los impactos de carácter social y medioambiental, al impacto en materia de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad y al impacto que tendrá para la ciudadanía y para la Administración el desarrollo o uso de los medios y servicios de la Administración digital que conlleve la norma.»

Disposición final cuarta. *Habilitación normativa.*

Se faculta a la persona titular del Ministerio de Política Territorial y Función Pública y a la persona titular del Ministerio de Asuntos Económicos y Transformación Digital en el ámbito de sus competencias, para dictar las disposiciones y adoptar las medidas necesarias para el desarrollo y ejecución de este real decreto y del Reglamento que aprueba, así como para modificar el anexo del mismo.

Disposición final quinta. *Entrada en vigor.*

Este real decreto entrará en vigor el día 2 de abril de 2021.

REGLAMENTO DE ACTUACIÓN Y FUNCIONAMIENTO DEL SECTOR PÚBLICO POR MEDIOS ELECTRÓNICOS

TÍTULO PRELIMINAR

Disposiciones generales

Artículo 1. *Objeto y ámbito de aplicación.*

1. Este Reglamento tiene por objeto el desarrollo de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en lo referido a la actuación y el funcionamiento electrónico del sector público.

2. El ámbito subjetivo de aplicación es el establecido en el artículo 2 de la Ley 39/2015, de 1 de octubre, y el artículo 2 de la Ley 40/2015, de 1 de octubre.

Artículo 2. *Principios generales.*

El sector público deberá respetar los siguientes principios en sus actuaciones y relaciones electrónicas:

a) Los principios de neutralidad tecnológica y de adaptabilidad al progreso de las tecnologías y sistemas de comunicaciones electrónicas, para garantizar tanto la independencia en la elección de las alternativas tecnológicas necesarias para relacionarse

§ 19 Reglamento de actuación y funcionamiento del sector público por medios electrónicos

con las Administraciones Públicas por parte de las personas interesadas y por el propio sector público, como la libertad para desarrollar e implantar los avances tecnológicos en un ámbito de libre mercado. A estos efectos, el sector público utilizará estándares abiertos, así como, en su caso y de forma complementaria, estándares que sean de uso generalizado.

Las herramientas y dispositivos que deban utilizarse para la comunicación por medios electrónicos, así como sus características técnicas, serán no discriminatorios, estarán disponibles de forma general y serán compatibles con los productos informáticos de uso general.

b) El principio de accesibilidad, entendido como el conjunto de principios y técnicas que se deben respetar al diseñar, construir, mantener y actualizar los servicios electrónicos para garantizar la igualdad y la no discriminación en el acceso de las personas usuarias, en particular de las personas con discapacidad y de las personas mayores.

c) El principio de facilidad de uso, que determina que el diseño de los servicios electrónicos esté centrado en las personas usuarias, de forma que se minimice el grado de conocimiento necesario para el uso del servicio.

d) El principio de interoperabilidad, entendido como la capacidad de los sistemas de información y, por ende, de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información entre ellos.

e) El principio de proporcionalidad, en cuya virtud sólo se exigirán las garantías y medidas de seguridad adecuadas a la naturaleza y circunstancias de los distintos trámites y actuaciones electrónicos.

f) El principio de personalización y proactividad, entendido como la capacidad de las Administraciones Públicas para que, partiendo del conocimiento adquirido del usuario final del servicio, proporcione servicios precumplimentados y se anticipe a las posibles necesidades de los mismos.

Artículo 3. *Derecho y obligación de relacionarse electrónicamente con las Administraciones Públicas.*

1. Estarán obligados a relacionarse a través de medios electrónicos con las Administraciones Públicas para la realización de cualquier trámite de un procedimiento administrativo, al menos, los sujetos a los que se refiere el artículo 14.2 de la Ley 39/2015, de 1 de octubre.

2. Las personas físicas no obligadas a relacionarse a través de medios electrónicos con las Administraciones Públicas podrán ejercitar su derecho a relacionarse electrónicamente con la Administración Pública de que se trate al inicio del procedimiento y, a tal efecto, lo comunicarán al órgano competente para la tramitación del mismo de forma que este pueda tener constancia de dicha decisión. La voluntad de relacionarse electrónicamente o, en su caso, de dejar de hacerlo cuando ya se había optado anteriormente por ello, podrá realizarse en una fase posterior del procedimiento, si bien deberá comunicarse a dicho órgano de forma que quede constancia de la misma. En ambos casos, los efectos de la comunicación se producirán a partir del quinto día hábil siguiente a aquel en que el órgano competente para tramitar el procedimiento haya tenido constancia de la misma.

3. De acuerdo con lo previsto en el apartado 3 del artículo 14 de la Ley 39/2015, de 1 de octubre, la obligatoriedad de relacionarse electrónicamente podrá establecerse reglamentariamente por las Administraciones Públicas para determinados procedimientos y para ciertos colectivos de personas físicas que, por razón de su capacidad económica, técnica, dedicación profesional u otros motivos, quede acreditado que tienen acceso y disponibilidad de los medios electrónicos necesarios.

A tal efecto, en el ámbito estatal la mencionada obligatoriedad de relacionarse por medios electrónicos con sus órganos, organismos y entidades de derecho público podrá ser establecida por real decreto acordado en Consejo de Ministros o por orden de la persona titular del Departamento competente respecto de los procedimientos de que se trate que afecten al ámbito competencial de uno o varios Ministerios cuya regulación no requiera de norma con rango de real decreto. Asimismo, se publicará en el Punto de Acceso General electrónico (PAGe) de la Administración General del Estado y en la sede electrónica o sede asociada que corresponda.