POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE DASS

1 Introducción

1.1. DASS es una empresa que presta SERVICIOS DE COMERCIALIZACIÓN, INSTALACIÓN, MANTENIMIENTO INTEGRAL DE EQUIPOS DE IMPRESIÓN E INFORMÁTICOS Y GESTIÓN DE SOLUCIONES DE IT. a organismos públicos.

1.2. DASS tiene personalidad jurídica propia y plena capacidad de obrar para administrar, adquirir, contratar, asumir obligaciones, así como renunciar y ejercer libremente toda clase de derechos y acciones ante las Administraciones públicas.

1.3. En el nuevo marco de la administración electrónica, y para su correcto desarrollo, DASS presta servicios a las propias administraciones y organismos públicos con los que colabora, y para ello, proporciona las mayores garantías para el correcto uso de las tecnologías por parte de las Administraciones Públicas.

DASS establece objetivos de seguridad de la información encaminados a proteger con las mayores garantías, la integridad, la confidencialidad, la disponibilidad, la trazabilidad y la autenticidad de la información objeto de tratamiento dentro de sus competencias.

1.5. Para garantizar una apropiada seguridad de la información, DASS aplicará las más adecuadas medidas de seguridad, en todos los Departamentos reforzando la prevención, detección y respuesta de incidentes de seguridad.

Los sistemas de información y comunicación de DASS deben estar protegidos contra potenciales amenazas que puedan poner en peligro la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información. A tal fin, adoptarán una estrategia de seguridad de la información que permita cumplir con los requisitos establecidos por el Esquema Nacional de Seguridad; aplicar un sistema de mejora continua, supervisar y garantizar unos adecuados niveles de servicios; seguir y analizar las vulnerabilidades reportadas y preparar una respuesta efectiva a los incidentes de seguridad con el fin de garantizar la continuidad de los servicios.

1.6. Dentro del enfoque de la seguridad de la información como parte integral de los servicios prestados por DASS y de su funcionamiento interno, tiene una especial importancia la protección de datos personales, por lo que muchas de las medidas implantadas estarán encaminadas a proteger proactivamente dichos datos, velando por el cumplimiento de lo dispuesto en la legislación vigente en materia de protección de datos personales dentro del marco normativo europeo y español.

2 Alcance

Esta política es aplicable, dentro del marco del alcance del ENS, sin excepciones a:

1. Todos los sistemas de información y comunicación
2. Todos los Departamentos y a todas las sedes.
3. Todo el personal de DASS
4. Todo el personal externo que preste servicios al DASS
5. Todo el personal, electo o profesional perteneciente a las entidades delegantes que puedan acceder a los sistemas de información del DASS.

3 Misión

Los objetivos de servicio DASS son los siguientes:

1. Colaborar con las entidades locales y demás entidades públicas en la aplicación de sus tributos y demás ingresos de derecho público.
2. Ofrecer los mejores servicios de información y asistencia a los ciudadanos para el cumplimento de sus obligaciones y el ejercicio de sus derechos
3. Integrar el sistema de gestión de protección de datos adaptado al RGPD en el ENS.
4. Reforzar la cultura de la organización en materia de seguridad de la información y protección de datos.
5. Situar al DASS en el cuadrante de las entidades públicas más avanzadas en materia de seguridad de la información en el ámbito de los servicios prestados a las Administraciones Públicas.
6. Garantizar la disponibilidad de los servicios.
7. Velar por los derechos y libertades de los ciudadanos y demás interesados en materia de protección de datos personales.

4 Marco Legal y Regulatorio Aplicable

La legislación aplicable a DASS en el marco de la seguridad de la información es la siguiente:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

- ITS - [BOE-A-2018-4573] Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información; en todo lo que no se contradiga con el Real Decreto 311/2022.
- ITS - [BOE-A-2016-10109] Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad; en todo lo que no se contradiga con el Real Decreto 311/2022.
- ITS - [BOE-A-2016-10108] Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad; en todo lo que no se contradiga con el Real Decreto 311/2022.
- ITS - [BOE-A-2018-5370] Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad; en todo lo que no se contradiga con el Real Decreto 311/2022.
- UNE-ISO/IEC 27001 “Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI). Requisitos”.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, vigente en aquellos artículos que no contradigan, se opongan o resulten incompatibles con lo dispuesto en el RGPD y en la Ley Orgánica 3/2018, de 5 de diciembre.

- 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.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

5 Organización de la Seguridad

5.1 Comité de Seguridad

5.1.1. El Comité de Seguridad de DASS está compuesto por el subdirector, la Responsable de Protección de Datos, y el Responsable de Seguridad.

5.1.2. El Comité tiene las siguientes funciones:

a) Promover la seguridad de los activos de información de DASS

b) Validar, la documentación de seguridad elaborada por el Responsable de Seguridad,

c) Proponer la aprobación de la clasificación de la información, conforme a lo que se indica más adelante

d) Valorar y proponer la aprobación de toda la documentación de seguridad

e) Diseñar la estructura de la documentación de seguridad

f) Vigilar el cumplimiento de las obligaciones del Responsable del Registro de actividades, conforme las regula la normativa de protección de datos de carácter personal.

g) Difundir entre el personal al que se refiere el ítem 2 del presente documento, el conocimiento de las obligaciones que le atañen y las consecuencias en que pudiera incurrir en caso de incumplimiento.

5.2 Responsable de la información

El Responsable de la Información (información owner) es habitualmente una persona que ocupa un alto cargo en la dirección de la organización. Este cargo

tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección. El Responsable de la Información es el responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.

5.2.1. El/la Responsable de la información será designado/a por el Director de DASS y tiene como responsabilidad la ejecución de todas las medidas de seguridad adecuadas para DASS, incluida la elaboración de la documentación de seguridad. Este cargo se irá renovando automáticamente hasta que la Dirección General anuncie la sustitución de la persona que ocupa el cargo.

5.2.2 El/la Responsable de la información dispone de la potestad de establecer los requisitos de la información en materia de seguridad. O, en terminología del ENS, la potestad de determinar los niveles de seguridad de la información.

5.2.3 Determinar los niveles de seguridad de los servicios.

5.2.4. La Dirección de DASS garantizará que el/la Responsable de la información participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la seguridad de la información y a la protección de datos personales.

5.2.5. La Dirección de DASS respaldará al/a Responsable de la información en el desempeño de las funciones mencionadas en el artículo 39 del RGPD, facilitando los recursos necesarios para el desempeño de dichas funciones y el acceso a los datos personales y a las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados.

5.2.6. La Dirección de DASS garantizará que el/la Responsable de la información no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones. El/la Responsable de la información rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado.

5.2.7. Las personas interesadas podrán ponerse en contacto con el/la Responsable de la información por lo que respecta a todas las cuestiones relativas a la seguridad de la información y a la protección de datos personales.

5.2.8. E/la Responsable de la información estará obligado/a a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones, de conformidad con el Derecho de la Unión o de los Estados miembros.

5.2.9. El/la Responsable de la información podrá desempeñar otras funciones y cometidos. La Dirección General garantizará que dichas funciones y cometidos no den lugar a conflicto de intereses.

5.3.0 La prestación de un servicio siempre debe atender a los requisitos de seguridad de la información que maneja (a veces se dice que ‘se heredan los requisitos’), y suele añadir requisitos de disponibilidad, así como otros como accesibilidad, interoperabilidad, etc.

El/la Responsable de la información tendrá como mínimo las siguientes funciones:

a) Informar y asesorar al Director General y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del ENS y de otras disposiciones aplicables en materia de seguridad de la información y de protección de datos, vigentes en España o en la Unión o de los Estados miembros;

b) Supervisar el cumplimiento de lo dispuesto en el ENS, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable en materia de seguridad de la información y protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;

c) Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la seguridad de la información y supervisar su aplicación de conformidad con lo dispuesto en el ENS;

d) Cooperar con las autoridades de control y los CERT.

e) Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento de datos personales, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

El/la Responsable de la información desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

Aunque la aprobación formal de los niveles corresponde al Responsable de la Información, se puede recabar una propuesta al Responsable de la Seguridad, así como también se escuchará la opinión del Responsable del Sistema.

5.3 Responsable del sistema

Persona designada por la Dirección. La persona designada figurará en la documentación de seguridad del sistema de información. Este cargo se renovará automáticamente, salvo que se la persona designada cause baja en la organización o cambie de puesto de trabajo dentro de la propia organización.

Responsabilidades:

a. Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.

b. Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.

c. Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

d. El Responsable del Sistema puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los responsables de la información afectada, del servicio afectado y el Responsable de la Seguridad, antes de ser ejecutada.

5.4 Responsable de seguridad y del servicio

5.3.1. El/la responsable de seguridad será designado/a por el Director de DASS y tiene como responsabilidad la ejecución de todas las medidas de seguridad adecuadas para DASS, incluida la elaboración de la documentación de seguridad. Este cargo, se irá renovando automáticamente hasta que la Dirección General anuncie la sustitución de la persona que ocupa el cargo.

5.3.2. Con independencia de la obligación genérica referida a la implantación, coordinación y control de las medidas de seguridad, se enumeran a continuación, a título enunciativo, las funciones concretas del responsable de seguridad:

a) Adoptar, con la mayor inmediatez, las medidas oportunas para subsanar cualquier anomalía que haya producido una incidencia e importar al Comité los impresos en que se hayan registrado las incidencias.

b) Cuando las incidencias hayan afectado a Datos personales, el Responsable de Seguridad deberá comunicar inmediatamente la incidencia a la Responsablede Protección de Datos.

c) Colaborar con el Director y el/la Responsable de Protección de Datos, en la comprobación de la correcta aplicación de los procedimientos de realización de copias de seguridad y recuperación de datos.

d) Verificar que, en todo procedimiento de recuperación de datos que sea realizado por personal externo, se mantiene la más estricta confidencialidad sobre los datos de carácter personal objeto de tratamiento.

e) Verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

f) Custodiar y actualizar la relación de usuarios con acceso a los sistemas de información o que intervienen en los tratamientos de datos de carácter personal.

g) Supervisar con la Responsable de Protección de Datos, el nivel de intervención, por los usuarios dados de alta, en las diferentes fases del ciclo de vida de los tratamientos de datos de carácter personal.

h) Asignar a los nuevos usuarios el correspondiente código de usuario y una contraseña, dándoles las instrucciones para que cambien la contraseña asignada en un plazo no superior a veinticuatro horas, de tal forma que la contraseña pase a ser del exclusivo conocimiento del usuario.

i) Borrar los identificadores de usuario y contraseñas cuando un usuario sea dado de baja.

j) Autorizar expresamente a la persona que entregue para su salida, o reciba de terceros, soportes informáticos que contengan datos de carácter personal. La autorización la realizará de forma específica para cada recepción o entrega, mediante firma en el impreso correspondiente, o de forma genérica, también mediante autorización escrita.

k) Conservar los impresos cumplimentados de entradas y salidas de soportes.

l) Realizar los controles de verificación periódica determinados en el Anexo X de este Documento.

m) Controlar los mecanismos establecidos para el registro de accesos, los cuales no podrán ser desactivados en ningún caso.

n) Establecer y comprobar todos los procedimientos y estándares necesarios para la correcta aplicación de la normativa de seguridad.

El Responsable del servicio determinará los requisitos que deben ser tenidos en cuenta a la hora de prestar servicios a las administraciones y organismos públicos.

El Responsable del servicio estará en contacto con el responsable por parte del cliente contratado porla administración u organismo público con el fin de consensuar los requisitos del servicio.

El responsable del servicio comunicará los requisitos del servicio a todo el personal de la organización implicado en la prestación del servicio.

El responsable del servicio velará por el cumplimiento de los requisitos del servicio y realizará un seguimiento exhaustivo de su cumplimiento por parte de la organización.

5.5 Administradores de sistema

Los administradores del sistema son designados por el responsable de seguridad y realizan tareas específicas de administración de servidores, de la red interna y distintas VPNs del proyecto. Este cargo se irá renovando automáticamente hasta que el responsable de seguridad anuncie la sustitución de la persona que ocupa el cargo.

5.6 Usuarios

Los usuarios / personal técnico, acceden a las aplicaciones con el perfil suficiente para desempeñar sus funciones profesionales, debido a la función asignada o del puesto de trabajo que despeñan y de la unidad administrativa en la que se encuadra.

5.7 Personal de campo

Los usuarios finales de los dispositivos portátiles solo disponen de los permisos necesarios para la captura de información y gestión de visitas.

6 Concienciación y Formación

Se desarrollarán actuaciones de concienciación y formación. El objetivo es lograr la plena conciencia respecto a que la seguridad de la información afecta a todos los miembros de la organización y a todas las actividades, de acuerdo con el principio de Seguridad Integral recogido en el Artículo 5 del ENS, así como la articulación de los medios necesarios para que todas las personas que intervienen en el proceso y sus responsables jerárquicos tengan una sensibilidad hacia los riesgos que se corren.

Se va a incluir en el Plan de Formación, los cursos gratuitos publicados por el CCN-CERT en su plataforma ÁNGELES (ÁNGELES - Cursos STIC (cni.es) relacionados con la seguridad de la información.

7 Herramientas de seguridad.

7.1 Clasificación de la documentación

7.1.1. La documentación de seguridad se clasifica en cuanto a su contenido del siguiente modo:

a) Política de seguridad: El presente documento, que establece las directrices generales de la seguridad en DASS al más alto nivel.

b) Normativa de seguridad: El documento que establece la obligatoriedad de la documentación de seguridad.

c) Políticas particulares: Documentación que establece directrices de actuación en áreas determinadas.

d) Procedimientos: Documentos que establecen maneras concretas de actuación.

e) Registros: Documentos que reflejan los resultados de los procedimientos.

f) Inventarios: Relación de ítems en un momento determinado.

g) Documentos para la gestión de riesgos: Análisis de impacto y plan de continuidad.

h) Otra documentación: Cualquier otra documentación relevante a la seguridad de la información procesada por DASS.

7.1.2. La documentación de seguridad se clasifica en cuanto a su naturaleza del siguiente modo:

a) Documentación para administradores.

b) Documentación para usuarios.

7.1.3. Dentro de esta documentación se incluye el Documento de seguridad y toda la documentación relevante al cumplimiento de la Legislación vigente en materia de protección de datos personales y seguridad de la información.

7.2 Procedimiento para la clasificación

La clasificación la realiza el Responsable de Seguridad, bajo la supervisión del Comité del DASS. Se ha aprobado la categorización de los servicios y sistemas de información de DASS en el marco del alcance del ENS como NIVEL MEDIO.

7.3 Generación y aprobación de la documentación.

La documentación la genera el Responsable de Seguridad, o personal bajo su dirección, la propuesta la realiza el Comité y la aprueba la Dirección de DASS.

El procedimiento de control de la documentación se encuentra incluido en el documento denominado "*FP02 Control Información Documentada.docx*".

7.4 Acceso a la documentación

El acceso a esta documentación se autoriza por el Responsable de seguridad, previa deliberación en el Comité. A cada usuario sólo se le conceden los privilegios mínimos para cumplir con estas obligaciones.

La difusión de determinada documentación está regulada en los correspondientes procedimientos de difusión.

7.5 Política de clasificación, distribución, etiquetado, almacenamiento y copia

- Deberá establecerse un **procedimiento de clasificación de datos de carácter personal**, en cuanto a los tratamientos de datos de empleados, clientes, contactos y proveedores. Esta clasificación deberá ser acorde a inventarios de tratamientos y sistemas de información, así como la información registrada en la Agencia Española de Protección de datos. Dicho procedimiento deberá ser liderado por la Dirección de Seguridad de la Información con la colaboración de responsables internos según el modelo organizativo de actuación de la normativa de privacidad y protección de datos personales.

- Deberán establecerse **procedimientos e información detallada sobre la política de distribución de información, etiquetado, impresión, almacenamiento y copia** según la clasificación descrita en esta política de manera que el personal conozca de una manera comprensible las normas de seguridad que afecten al desarrollo de sus funciones, así como las consecuencias en que pudiera afectar en caso de incumplimiento.

- Deberá establecerse un **procedimiento de inventario de intercambio de información entre departamentos** como base de la identificación y mejora de la clasificación de información para definir medidas de seguridad y directrices de salvaguarda de las mismas.

7.6 Revisión de la documentación de seguridad

La revisión de la documentación de seguridad se realiza conforme a los procedimientos que se establezcan.

7.7 Protección de las instalaciones

La protección de las instalaciones se encuentra descrita en el documento denominado ”DASS_Documentacion-instalaciones“

7.8 Adquisición de Productos

Antes de la adquisición de cualquier producto o servicios de seguridad de la información aplicable al alcance incluido dentro del ENS, se comprobará que el producto o servicios se encuentra certificado o homologado por la Guía 105 del CCN-STIC y, en su defecto, se comprobará si los productos o servicios se encuentran certificados y homologados según los common criteria, que se puede comprobar en la página web: Certified Products : CC Portal (commoncriteriaportal.org)

En caso de no estar homologados por el CCN o por COMMON CRITERIA, se procederá a realizar un análisis de riesgos previo a la adquisición de los productos o servicios, con el fin de identificar los riesgos para los que debe estar preparado el producto o servicio y proceder a denegar la adquisición del producto o a subsanar los puntos débiles detectados en los productos para mitigar los niveles de riesgos.

Cuando la organización contrate los servicios de desarrollo de software a un proveedor externo, se deberán identificar los requisitos de seguridad de la información que el producto o servicio debe abordar de forma eficiente.

La adquisición de los productos o servicios de seguridad de la información debe ser aprobada por el Director de IT y el Director Financiero.

Las peticiones de adquisición de nuevos productos se gestionan como peticiones de servicio o cambio a través de la herramienta de ticketing. En estos casos, se sigue el procedimiento de gestión de cambios descrito en el documento denominado “*DASS_ GESTION DE CAMBIOS.docx*”.

7.9 Proceso de autorización

Se ha establecido un proceso formal de autorizaciones que cubre todos los elementos del sistema de información la organización en el marco del alcance del ENS. Se requiere autorización de la Dirección para los Jefes de Área y se les

da potestad, a su vez, para autorizar a los empleados que se encuentren bajo su responsabilidad. La autorización se requerirá previamente al acceso y uso de información y medios del sistema de información. Las peticiones de autorización se gestionarán de igual forma que las peticiones de servicio.

La autorización será requerida para los siguientes elementos del sistema de información:

a) Utilización de instalaciones, habituales y alternativas.

b) Entrada de equipos en producción, en particular, equipos que involucren criptografía.

c) Entrada de aplicaciones en producción.

d) Establecimiento de enlaces de comunicaciones con otros sistemas.

e) Utilización de medios de comunicación, habituales y alternativos.

f) Utilización de soportes extraíbles de información.

g) Utilización de equipos móviles. Se entenderá por equipos móviles ordenadores, portátiles, smartphones, tablets, u otros de naturaleza análoga.

h) Utilización de servicios de terceros, bajo contrato o Convenio.

El proceso formal de autorizaciones se resume en la siguiente Matriz:

Actividad para autorizar	Responsable de Autorización
Utilización de instalaciones habituales	Responsable de Seguridad
Utilización de instalaciones alternativas	Responsable de Seguridad
Entrada de equipos en producción	Responsable de Sistemas
Entrada de equipos en producción que involucren criptografía	Responsable de Seguridad
Entrada de aplicaciones en producción	Responsable del Sistema
Enlaces de comunicación con otros Sistemas - Interconexiones	Responsable de Seguridad
Utilización de medios de comunicación habituales	Responsable del Sistema
Utilización de medios de comunicación alternativos	Responsable del Sistema
Utilización de soportes de información	Responsable del Sistema

Utilización de equipos móviles: ordenadores portátiles, tabletas, teléfonos móviles, etc.	Responsable del Sistema
Utilización de servicios de terceros	Dirección.
Adquisición de nuevos componentes	Responsable de Seguridad
Actualizaciones y parcheados del Sistema	Responsable de Seguridad

7.10 Seguridad por defecto

Antes de realizar ningún tipo de modificación de políticas, procedimientos o usos de nuevas herramientas aplicables a los servicios que se prestan a las Administraciones y organismos públicos en el marco del alcance del ENS, se tendrán en cuenta todos los aspectos de seguridad de la información requeridos por el ENS, y por cualquier otra legislación aplicable que resulte de aplicación, así como cualquier otro requisito de seguridad de la información requerido por cualquier Administración u organismo público que contrate cualquiera de los servicios enmarcados dentro del alcance del ENS.

7.11 Política de autenticación y acceso al sistema

7.11.1 Formación de las contraseñas

7.9.1.1. Las contraseñas deben cumplir las siguientes características:

a) Más de 10 caracteres.

b) Contengan caracteres alfabéticos y numéricos.

c) No repitan caracteres consecutivamente.

d) No sean de fácil conjetura (fechas significativas, números de teléfono, matrículas de coche, nombres de familiares o amigos, etc.).

e) No reutilizar contraseñas de servicios personales.

7.9.1.2. El mecanismo de gestión de autenticadores no permite utilizar contraseñas que no cumplan esta política.

7.11.2 Validez de las contraseñas y otros métodos de autenticación

7.9.2.1. La cuenta del usuario no se habilita hasta que éste haya confirmado la recepción del modo de autenticación, tal y como se describe en el Procedimiento de creación de usuarios.

7.9.2.2. Las contraseñas deben cambiarse una vez al año, como se acredita en el Registro de cambio de autenticadores.

7.9.2.3. Existe un procedimiento para la revisión de autenticadores cuyos resultados se recogerán en un breve informe o ticket.

7.9.2.4 Existe una política de acceso criptográfico donde se especifica el tiempo de cifrado de la red y acceso.

7.11.3 Mensajes previos al acceso y mensajes de error en el acceso

7.9.3.1. Los sistemas, deben ser configurados de forma que no revelen información del sistema antes de un acceso autorizado.

En particular, los diálogos de acceso no deben revelar información sobre el sistema al que se está accediendo.

7.9.3.2. Del mismo modo, los mensajes de error en el acceso deben revelar la información mínima necesaria.

7.11.4 Reacción del sistema ante intentos repetidos de acceso sin éxito

7.9.4.1. El número máximo de intentos fallidos de acceso es de cinco. Tras el quinto acceso sin éxito al sistema o a una aplicación determinado, el usuario queda bloqueado.

7.9.4.2. Un bloqueo de usuario es una incidencia que debe gestionarse conforme al procedimiento de gestión de incidencias.

7.9.4.3. El sistema almacena un registro con los accesos exitosos y los fallidos, tal y como se establece en la política de retención de registros de actividad.

7.11.5 Acceso exitoso al sistema

El sistema, después del acceso con éxito, debe informar al usuario de sus obligaciones inmediatamente, así como de la fecha y hora del último acceso con su identidad con éxito.

7.11.6 Control de accesos

En el Registro de Privilegios de usuarios se establecen el horario, fechas y lugar desde donde está autorizado el acceso para categoría de usuario o usuario particular. El sistema denegará el acceso a los usuarios fuera de las horas y lugares habilitados.

7.11.7 Política de renovación de la autenticación del usuario

El Procedimiento para los Mecanismos de Acceso establece los puntos en los que el sistema requerirá una renovación de la autenticación del usuario.

7.11.8 Política de accesos remotos

Los accesos desde fuera de las propias instalaciones de DASS deben cumplir los requisitos establecidos en el Proceso para accesos remotos autorizados.

Existen unas GPO´s que definen la política de accesos a la red, que se encuentran definidas a nivel de firewall.

8 Procedimiento de coordinación y resolución de conflictos y reclamaciones

En caso de conflicto entre los distintos perfiles de puesto integrados en el Comité de Seguridad, prevalecerán las instrucciones facilitadas por la Dirección General y, en su defecto por el Responsable de Seguridad de la Información.

9 Integridad y actualización del sistema

Cualquier elemento físico o lógico requiere la autorización del Responsable de Seguridad de la Información para poder proceder a su instalación en los sistemas de información de DASS.

Se realizan test periódicos de vulnerabilidades técnicas para comprobar el estado de la seguridad de los sistemas de información de DASS.

10 Prevención ante otros sistemas de interconexión interconectados

DASS no cuenta con sistemas de interconexión interconectados en los servicios que presta a los Organismos y Administraciones Públicas en el marco del alcance del ENS.

Independientemente, todos los intercambios de información y prestación de servicios con otros sistemas serán objeto de una autorización previa. Todo flujo de información estará prohibido salvo autorización expresa.

Y 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, siguiendo la Guía de Seguridad CCN-STIC 811.

1 Entrada en vigor y publicación

Esta Política se Seguridad de la Información es efectiva desde el día siguiente de su aprobación y hasta que no sea reemplazada por otra versión posterior, siendo de acceso público a través de la web de DASS.