DATADEC

DATADEC

Política de Seguridad

Referencia	**Política de Seguridad de DATADEC.pdf**
Autor	**Departamento de Seguridad**
Fecha de creación	**07/02/2022**
Última actualización	**05/07/2023**
Versión	**V2.2**
Clasificación	**Uso interno**

Contenido

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 02/05/2023 por la Dirección. Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

2. INTRODUCCIÓN

DATADEC S.A. (DATADEC) depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando de forma rápida y eficiente frente a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los diferentes departamentos deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación y en la solicitud de ofertas.

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes de acuerdo al Artículo 7 del ENS.

2.1. PREVENCIÓN

Los departamentos deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello

los departamentos deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, los departamentos deben

- Autorizar los sistemas antes de entrar en producción.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

2.2. DETECCIÓN

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

2.3. RESPUESTA

Los departamentos deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

2.4. RECUPERACIÓN

Para garantizar la disponibilidad de los servicios críticos, los departamentos deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

3. ALCANCE

El alcance que aplica a DATADEC es: el Sistema de información que da soporte a la actividad de: **desarrollo, mantenimiento, soporte de la plataforma Expert Suite**.

Esta política se aplica a todos los sistemas TIC de y a todos los miembros de la organización, sin excepciones.

4. MISIÓN Y VISIÓN

Misión: Buscamos una relación a largo plazo y de confianza absoluta con nuestros clientes, desarrollando e innovando productos y servicios que les aporte un valor diferencial con respecto a la competencia y sea el motor de nuevas oportunidades de negocio. El objetivo es que nuestros clientes aprovechen las nuevas tecnologías para mejorar en competitividad y asegurar un crecimiento sostenido en el tiempo.

Visión: En un mundo en continua transformación, nuestra visión es aportar a nuestros clientes herramientas y conocimientos que les ayude a adaptarse a los cambios actuales y futuros, proponiéndoles y ayudando a aplicar nuevas soluciones con alto retorno de inversión, que mejoren la productividad y les ayude a ser sostenibles en el tiempo.

Valores: Los siguientes valores son los que hacen a Datadec una empresa que apuesta por la innovación:

- Innovación.
- Compromiso con la calidad del servicio.
- Confianza.
- Trabajo en equipo.

5. MARCO NORMATIVO

DATADEC se encuentra sujeto a la una normativa en la provisión de los servicios prestados a sus clientes. Esta normativa se describe de forma detallada en la **Normativa de Uso de los sistemas**.

6. ORGANIZACIÓN DE LA SEGURIDAD

6.1. COMITÉ: FUNCIONES Y RESPONSABILIDADES

El Comité de Gestión de la Seguridad de la Información estará formado por el Director de la información y Seguridad de la Información, Responsable de TI, Responsable del Sistema de Gestión y Responsable de Desarrollo.

El Comité tendrá las siguientes funciones:

- **Representar a todas las partes implicadas dentro del alcance del ENS**.
- **Supervisar el desempeño de los procesos de gestión de incidentes de seguridad** y recomienda posibles actuaciones respecto de ellos.
- **Promover la realización de las auditorías periódicas** que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- **Aprobará planes de mejora de la seguridad de la información**. En particular, velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.
- **Velar para que la seguridad de la información tenga en cuenta todos los proyectos TIC** desde su especificación inicial hasta la puerta en operación. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- **Resolver los conflictos de responsabilidad** que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la Organización, elevando aquellos casos en que no tenga suficiente autoridad para decidir.
- **Obtener la información pertinente para tomar decisiones**, ya sea de personal técnico propio o externo y de forma regular.
- **Se asesorará de los temas que tenga que decidir** o emitir una opinión. Este asesoramiento se determinará en cada caso, pudiendo materializarse de diferentes formas y maneras:
    - Grupos de trabajo especializados internos, externos o mixtos.
    - Asesoría interna y/o externa.
    - Asistencia de sus miembros a cursos, seminarios, jornadas u otro tipo de entornos formativos o de intercambio de experiencias.
- **Aprobará el Plan de Mejora de la Seguridad**, con su dotación presupuestaria correspondiente.

6.2. ROLES: FUNCIONES Y RESPONSABILIDADES

Los diferentes roles junto con sus respectivas funciones y responsabilidades vienen reflejados a continuación:

La composición del Comité de Seguridad estará formada por los siguientes miembros:

Nombre	Cargo
Responsable de Información	Vicente Serrano Ortiz
Responsable del Sistema de Gestión de Seguridad de la Información	Jose Vicente Serrano
Responsable de Seguridad	Jesús Abellán
Responsable de Servicio Desarrollo Conselleria	Santos Moreno
Responsable de Servicio Desarrollo y Preproducción	Jose Luis Giménez
Responsable del Servicio Consultoría Consellería	Jesús París

Responsable de la Información. Máximo responsable en materia de cumplimiento normativo en la organización.

FUNCIONES

- Velar por el buen uso de la información y, por tanto, de su protección.
- Ser responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.
- Establecer los requisitos de la información en materia de seguridad.
- Determinar los niveles de seguridad de la información.
- Aprobar formalmente el nivel de seguridad de la información.
- Promover que el tratamiento de los datos personales efectuados por DATADEC, se efectúe de forma respetuosa con la normativa
- Desde el punto de vista de la seguridad y teniendo en cuenta el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables deberá velar por que se garantice una seguridad adecuada de los datos personales y determinar las medidas de seguridad concretas que tendrá que proponer al responsable del tratamiento.

Responsable del Sistema de Gestión: Responsable de la gestión del SGSI.

FUNCIONES

- Gestionar el Sistema de Información durante todo su ciclo de vida, desde la especificación, instalación hasta el seguimiento de su funcionamiento.

- Definir los criterios de uso y los servicios disponibles en el Sistema.
- Definir las políticas de acceso de usuarios al Sistema.
- Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.
- Determinar la configuración autorizada de hardware y software a utilizar en el Sistema y aprobar las modificaciones importantes de dicha configuración.
- Realizar el análisis y gestión de riesgos en el Sistema.
- Elaborar y aprobar la documentación de seguridad del Sistema.
- Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y determinar las medidas de seguridad que deben aplicarse según se describe en el Anexo II del ENS.
- Implantar y controlar las medidas específicas de seguridad del Sistema.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
- Suspensión del manejo de cierta información o la prestación de un cierto servicio si detecta deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.

Responsable de Seguridad: Responsable de la gestión de la Seguridad.

FUNCIONES

- Adoptar las medidas necesarias para que el personal conozca las normas en materia de seguridad que afectan al desarrollo de sus funciones y de las consecuencias en que pudieran incurrir en caso de incumplimiento.
- Asegurarse que se establezcan las medidas de seguridad que se hayan documentado en el SGSI.
- Coordinar y controlar las medidas definidas en la documentación de gestión del SGSI.
- Analizar los informes de auditoría.
- Controlar y gestionar los mecanismos de seguridad del SGSI.
- Establecer los criterios para la definición de los derechos de acceso de los usuarios.

- Actualizar la documentación del SGSI.
- Conocer las consecuencias que se pudieran derivar y las responsabilidades en que se pudiera incurrir en caso de incumplimiento de la normativa.
- Elevar a la Gerencia las conclusiones del análisis del informe de auditoría.
- Revisar la información de controles registrada.
- Elaborar informes de las revisiones efectuadas.

Responsable del Servicio. Responsable de la gestión del Servicio.

FUNCIONES

- Establecer los requisitos del servicio en materia de seguridad, incluyendo los requisitos de interoperabilidad, accesibilidad y disponibilidad.
- Determinar los niveles de seguridad de los servicios.
- Aprobar formalmente el nivel de seguridad del servicio.

6.3. PROCEDIMIENTOS DE DESIGNACIÓN

Los distintos cargos del Comité serán nombrados por la Dirección a propuesta del Comité de Gestión de la Seguridad de la Información. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

6.4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del Comité de Gestión de la Seguridad de la Información la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por el mismo comité y difundida para que la conozcan todas las partes afectadas.

7. DATOS DE CARÁCTER PERSONAL

DATADEC trata datos de carácter personal. El documento de seguridad, al que tendrán acceso sólo las personas autorizadas, recoge los ficheros afectados y los responsables correspondientes. Todos los sistemas de información de DATADEC se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de Seguridad.

8. GESTION DE RIESGOS

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez al año.
- Cuando cambie la información manejada,
- Cuando cambien los servicios prestados.
- Cuando ocurra un incidente grave de seguridad
- Cuando se reporten vulnerabilidades graves

Para la armonización de los análisis de riesgos, el Comité de Gestión de la Seguridad de la Información establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Gestión de la Seguridad de la Información dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

9. GESTIÓN DOCUMENTAL

Las directrices para la estructuración de la documentación del sistema, su gestión y acceso se encuentran documentadas en el **Procedimiento Elaboración y Control de Documentos**.

10. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información complementa las políticas de seguridad de DATADEC en diferentes materias:

- Aspectos organizativos de la seguridad de la información, que establece un marco de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.
- Seguridad física y ambiental, que establece las directrices para prevenir el acceso físico no autorizado, los daños e interferencia a la información de la organización y a los recursos de tratamiento de la información.

- Gestión de comunicaciones y operaciones, que define las pautas a seguir para asegurar el funcionamiento correcto y seguro de las instalaciones de tratamiento de la información, así como de las redes.
- Control de acceso, que define cómo limitar el acceso a los recursos de tratamiento para prevenir el acceso no autorizado, garantiza el acceso de usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios. Adquisición, desarrollo y mantenimiento de los SSII, para garantizar que la seguridad de la información sea parte integral de los sistemas de información a través de todo el ciclo de vida.
- Cumplimiento legal, para evitar incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales relativas a la seguridad de la información o de los requisitos de seguridad.
- Seguridad de los RRHH y Terceros, que asegura que los empleados y contratistas entiendan sus responsabilidades y sean adecuados para desempeñar sus funciones.
- Cifrado, para garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.
- Gestión de activos, que define como identificar los activos de la organización y definir las responsabilidades de protección adecuadas.

La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

La normativa de seguridad estará disponible en una carpeta compartida proporcionada por parte de la organización y accesible por parte de todos los usuarios.

11.OBLIGACIONES DEL PERSONAL

Todos los miembros de DATADEC tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Gestión de la Seguridad de la Información disponer de los medios necesarios para que la información llegue a los afectados.

Todos los miembros de DATADEC asistirán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año. Se establecerá un programa de

concienciación continua para atender a todos los miembros de DATADEC, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

12.TERCERAS PARTES

Cuando preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando DATADEC utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

13.SANCIONES

Cualquier violación premeditada o negligente de las políticas y normas de seguridad y que suponga un potencial daño, consumado o no a DATADEC, S.A., será sancionada de acuerdo a los mecanismos habilitados en el convenia del la Empresa y en la normativa legal, contractual y corporativa vigentes.

Todas las acciones en las que se comprometa la seguridad de DATADEC, S.A. y que no estén previstas en esta política, deberá ser revisadas por la Dirección General y por el Responsable de Seguridad para dictar una resolución sujetándose al criterio de la empresa y la legislación prevista.

Las acciones disciplinarias en respuesta a los incumplimientos de la Política de Seguridad son atribución de los Responsables de Departamento en conjunción con Administración y la Dirección General.

14.PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

Como respuesta a un nuevo entorno tecnológico donde la convergencia entre la informática y las comunicaciones están facilitando un nuevo paradigma de productividad para las empresas, DATADEC está altamente comprometida con mantener un servicio competitivo a través de ofrecer un modelo de negocio responsable, basado en la búsqueda permanente del equilibrio económico, social y ambiental, donde el desarrollo de buenas prácticas en Seguridad de la Información es fundamental para conseguir los objetivos de confidencialidad, integridad, disponibilidad y legalidad de toda la información gestionada.

En consecuencia, DATADEC define los siguientes principios en el marco del Sistema de Gestión de Seguridad de la Información (SGSI):

- **Confidencialidad**: la información tratada por DATADEC será conocida exclusivamente por las personas autorizadas, previa identificación, en el momento y por los medios habilitados.
- **Integridad**: la información tratada por DATADEC será completa, exacta y válida, siendo su contenido el facilitado por los afectados sin ningún tipo de manipulación.
- **Disponibilidad**: la información tratada por DATADEC estará accesible y utilizable por los usuarios autorizados e identificados en todo momento, quedando garantizada su propia persistencia ante cualquier eventualidad prevista.
- **Legalidad**: DATADEC garantizará el cumplimiento de toda legislación o requisito contractual que sea de aplicación. Y en concreto, la normativa en vigor relacionada con el tratamiento de datos de carácter personal.

DATADEC para el correcto desempeño de sus funciones de negocio se basa y ayuda del tratamiento de diferentes tipos de datos e información, sustentados por los sistemas, programas, infraestructuras de comunicaciones, ficheros, bases de datos, archivos, etc., constituyendo estos, uno de los activos principales de DATADEC. De tal manera que el daño o pérdida de los mismos inciden en la realización de sus servicios y pueden poner en peligro la continuidad de la organización. Para que esto no suceda, se ha diseñado una Política de Seguridad de la Información cuyos fines principales son:

- Proteger, mediante controles/medidas, los activos frente a amenazas que puedan derivar en incidentes de seguridad.
- Paliar los efectos de los incidentes de seguridad.
- Establecer un sistema de clasificación de la información y los datos con el fin de proteger los activos críticos de información.
- Definir las responsabilidades en materia de seguridad de la información generando la estructura organizativa correspondiente.
- Elaborar un conjunto de reglas, estándares y procedimientos aplicables a los órganos de dirección, empleados, socios, proveedores de servicios externos, etc.
- Especificar los efectos que conlleva el incumplimiento de la Política de Seguridad en el ámbito laboral.
- Evaluar los riesgos que afectan a los activos con el objeto de adoptar las medidas/controles de seguridad oportunos.
- Verificar el funcionamiento de las medidas/controles de seguridad mediante auditorías de seguridad internas realizadas por auditores independientes.
- Formar a los usuarios en la gestión de la seguridad y en tecnologías de la información y las comunicaciones de cara a disponer de una profesionalidad en proceso de mejora continua en todos sus empleados.
- Controlar el tráfico de información y de datos a través de infraestructuras de comunicaciones o mediante el envío de soportes de datos ópticos, magnéticos, en papel, etc.
- Observar y cumplir la legislación en materia de protección de datos, propiedad intelectual, laboral, de servicios de la sociedad de la información, penal, etc., que afecte a los activos de DATADEC.

- Proteger el capital intelectual de la organización para que no se divulgue ni se utilice ilícitamente.
- Reducir las posibilidades de indisponibilidad a través del uso adecuado de los activos de la organización.
- Defender los activos ante ataques internos o externos para que no se transformen en incidentes de seguridad.
- Realizar una eficiente autorización y control de los accesos de la organización.
- Proteger adecuadamente las instalaciones.
- En el proceso de adquisición de productos aplicar controles de seguridad de la información, en función de la gestión del riesgo de la entidad.
- Aplicar el principio de seguridad por defecto
- Realizar una gestión adecuada al riesgo de la entidad en función de la integridad y actualización del sistema
- Realizar una eficiente protección de la información almacenada y en tránsito.
- Aplicar medidas de prevención ante otros sistemas de información interconectados.
- Realizar un adecuado registro de la actividad de los Sistemas de Información.
- Llevar a cabo acciones para garantizar la continuidad de la actividad de la organización ante posibles contingencias.
- Controlar el funcionamiento de las medidas de seguridad averiguando el número de incidencias, su naturaleza y efectos.

La Dirección de DATADEC asume la responsabilidad de apoyar y promover el establecimiento de las medidas organizativas, técnicas de control necesarias para el cumplimiento de la presente Política de Seguridad de la Información. Así como, de proveer aquellos recursos que sean necesarios para resolver con la mayor rapidez y eficacia posible, las no conformidades e incidentes de seguridad de la información que pudiesen surgir, y la puesta en funcionamiento de las medidas necesarias para que estas no vuelvan a ocurrir.

Esta Política será mantenida, actualizada y adecuada a los fines de la organización, alineándose con el contexto de gestión de riesgos de la organización. A este efecto se revisará de forma planificada o siempre que se produzcan cambios significativos, a fin

de asegurar que se mantenga su idoneidad, adecuación y eficacia de tal forma que se aplique mejora continua en todo el proceso de seguridad de la información.

De igual forma, para **gestionar los riesgos** que afronta DATADEC se establece un **procedimiento de evaluación de riesgos formalmente definido**.

Por su parte, todas las políticas y procedimientos incluidos en el SGSI serán revisados, aprobados e impulsados por la Dirección de DATADEC.