SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

Política de seguridad de la información.

Versión	**1.0**
Fecha	**22 de marzo de 2022**
Identificador	**SGSI02**
Estado	**Aprobado**

info@istecdigital.es
Polígono Pista de Ademuz, S/N.
46100 Burjassot (Valencia)

www.istecdigital.es

CSV:EM2M2DZV:MZTHBVDF:Y19C4IE8 **URL de validació:**https://www.tramita.gva.es/csv-front/index.faces?cadena=EM2M2DZV:MZTHBVDF:Y19C4IE8

Sumario

info@istecdigital.es
Polígono Pista de Ademuz, S/N.
46100 Burjassot (Valencia)
www.istecdigital.es

CSV:EM2M2DZV:MZTHBVDF:Y19C4IE8 URL de validació:https://www.tramita.gva.es/csv-front/index.faces?cadena=EM2M2DZV:MZTHBVDF:Y19C4IE8

1. Aprobación y entrada en vigor

Mediante Acuerdo del Consejo de Administración de **22 de marzo de 2022**, se aprueba la Política de Seguridad de la Información de Infraestructures i Serveis de Telecomunicacions i Certificació, SAU, (en adelante Istec).

Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva versión de esta.

2. Introducción

Istec 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 con presteza 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 Istec y todo su personal deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad (en adelante ENS) - Real Decreto 3/2010 –, el estándar UNE - ISO/IEC 27001:2013 dentro de su alcance, y resto de normativa de aplicación, 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.

Istec debe cerciorarse de que la seguridad TIC es una parte integral de cada etapa del

CSV:EM2M2DZV:MZTHBVDF:Y19C4IE8 URL de validació:https://www.tramita.gva.es/csv-front/index.faces?cadena=EM2M2DZV:MZTHBVDF:Y19C4IE8

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, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

La entidad debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el Artículo 7 del ENS.

2.1. Prevención

Istec debe 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 implementará las medidas mínimas de seguridad determinadas por el ENS, el estándar UNE - ISO/IEC 27001:2013 dentro de su alcance, y resto de normativa de aplicación, 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, van a estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, Istec debe:

- Autorizar los sistemas antes de entrar en operación.
- 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

CSV:EM2M2DZV:MZTHBVDF:Y19C4IE8 URL de validació:https://www.tramita.gva.es/csv-front/index.faces?cadena=EM2M2DZV:MZTHBVDF:Y19C4IE8

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

Istec:

- Establece mecanismos para responder eficazmente a los incidentes de seguridad.
- Designa punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establece 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, Istec desarrollará planes de continuidad de los sistemas TIC como parte de su plan general de continuidad del servicio y actividades de recuperación en aquellos servicios en que sea necesario.

3. Alcance

Esta política de seguridad será de obligado cumplimiento para todos los miembros de Istec, siendo aplicable a todos los activos empleados por la misma en la prestación de los servicios a los ciudadanos, a las entidades, a otras administraciones, así como para su propia gestión y funcionamiento.

CSV:EM2M2DZV:MZTHBVDF:Y19C4IE8 URL de validació:https://www.tramita.gva.es/csv-front/index.faces?cadena=EM2M2DZV:MZTHBVDF:Y19C4IE8

4. Misión

Ser instrumento de la Generalitat Valenciana (GVA) para facilitar la transformación digital de la sociedad, prestando servicios resilientes e innovadores de telecomunicaciones, tecnologías de la información y confianza electrónica.

5. Objetivos y principios de seguridad

Esta Política tiene como objetivo preservar los siguientes atributos de la información y los servicios de Istec:

- **Confidencialidad**: Garantizar que la información es accesible sólo para aquellos autorizados a tener acceso.
- **Integridad**: Garantizar la exactitud y completitud de la información y de los métodos de su procesamiento.
- **Disponibilidad**: Garantizar que los usuarios autorizados tienen acceso cuando lo requieran a la información, los servicios y sus activos asociados.
- **Autenticidad**: Garantizar la identidad del usuario que origina la información.
- **Trazabilidad**: Garantizar el conocimiento de aspectos clave de las operaciones de creación, modificación y consulta de la información.

Los siguientes ocho principios son complementarios y afectan a todo el personal de todos los niveles: gobierno, ejecución, supervisión y operación. La responsabilidad del personal es diferenciada y varía de acuerdo con los papeles que desempeñen.

Son directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de información. Estas son:

1. **Alcance estratégico**: La seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos de forma que pueda estar coordinada e integrada con el resto de las iniciativas estratégicas para conformar un todo coherente y eficaz.

CSV:EM2M2DZV:MZTHBVDF:Y19C4IE8 URL de validació:https://www.tramita.gva.es/csv-front/index.faces?cadena=EM2M2DZV:MZTHBVDF:Y19C4IE8

2. **Concienciación y responsabilidad**: El personal debe ser consciente de la necesidad de contar con sistemas de información y redes seguros, y qué es lo que pueden hacer para promover y fortalecer la seguridad. Todo el personal es responsable de la seguridad de la información y redes.
3. **Respuesta**: El personal debe actuar de manera oportuna y cooperativa para prevenir, detectar y responder a incidentes que afecten a la seguridad.
4. **Gestión de riesgos**: El análisis y gestión de riesgos será parte esencial del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales.
5. **Proporcionalidad**: El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.
6. **Seguridad por defecto**: El personal debe incorporar la seguridad desde el inicio como un elemento esencial de los sistemas de información y redes, que deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.
7. **Seguridad integral**: La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los
8. **Mejora continua**: El personal debe revisar y reevaluar la seguridad de sus sistemas de información y redes y hacer las modificaciones pertinentes a sus políticas, prácticas, medidas y procedimientos de seguridad.

CSV:EM2M2DZV:MZTHBVDF:Y19C4IE8 URL de validació:https://www.tramita.gva.es/csv-front/index.faces?cadena=EM2M2DZV:MZTHBVDF:Y19C4IE8

6. Marco normativo

El marco normativo en materia de seguridad de la información en el que Istec desarrolla su actividad, esencialmente, es el siguiente:

- De ámbito europeo:
  - Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas del mercado interior (ReIDAS) y normas de ejecución.
  - 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 (RGPD).
  - Directiva (UE) 2016/1148 del Parlamento Europeo y el Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión.
  - Directiva (UE) 2016/2102 del Parlamento Europeo y del Consejo, de 26 de octubre de 2016, sobre accesibilidad de los sitios web y aplicaciones para dispositivos móviles de los organismos del sector público.
- De ámbito estatal:
  - Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD-GDD).
  - Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
  - Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI).
  - Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS).
  - 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 (ENI).

CSV:EM2M2DZV:MZTHBVDF:Y19C4IE8 URL de validació:https://www.tramita.gva.es/csv-front/index.faces?cadena=EM2M2DZV:MZTHBVDF:Y19C4IE8

- Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la información pública y Buen gobierno.
- Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas (LPAC).
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSC).
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Resolución de 7 de octubre de 2016 de la Secretaría de estado de Administraciones Públicas, por el que se aprueba la Instrucción Técnica de Seguridad de Informe de Estado de Seguridad.
- Resolución de 13 de octubre de 2016 de la Secretaría de estado de Administraciones Públicas, por el que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- 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.
- 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.
- Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.

- De ámbito autonómico:
  - ORDEN 1/2021, de 20 de abril, de la consellera de Participación, Transparencia, Cooperación y Calidad Democrática, por la que se desarrolla el Decreto 179/2020, de 30 de octubre, del Consell, por el cual se aprueba el Reglamento orgánico y funcional de la Conselleria de Participación, Transparencia,

CSV:EM2M2DZV:MZTHBVDF:Y19C4IE8 URL de validació:https://www.tramita.gva.es/csv-front/index.faces?cadena=EM2M2DZV:MZTHBVDF:Y19C4IE8

Cooperación y Calidad Democrática. [2021/4126]

- De ámbito interno:
  - UNE - ISO/IEC 27001:2013 Especificaciones para los Sistemas de Gestión de la Seguridad de la Información.
  - UNE - ISO/IEC 27002:2013 Código de buenas prácticas para la Gestión de la Seguridad de la información.
  - WebTrust Principles and Criteria for Certification Authorities.
  - WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security.

7. Organización de la seguridad

La implantación de la Política de Seguridad de la Información en Istec requiere que todos los miembros de la organización entiendan sus obligaciones y responsabilidades en función del puesto desempeñado. Como parte de la Política de Seguridad de la Información, cada rol especifico, personalizado en usuarias y usuarios concretos, debe entender las implicaciones de sus acciones y las responsabilidades que tiene atribuidas, quedando identificadas y detalladas en esta sección, y que se agrupan del modo siguiente:

a) Comité de Seguridad de la Información

b) Responsable de la Información y del Servicio

c) Responsable de Seguridad de la Información y delegado

d) Responsable del Sistema

e) Delegado de Protección de Datos

En los siguientes apartados se especifican las funciones atribuidas a cada uno de estos roles.

CSV:EM2M2DZV:MZTHBVDF:Y19C4IE8 URL de validació:https://www.tramita.gva.es/csv-front/index.faces?cadena=EM2M2DZV:MZTHBVDF:Y19C4IE8

7.1. Comité de Seguridad de la Información

El Comité de Seguridad de la Información es el órgano de gestión interna de Istec al que compete la Seguridad de la Información. Dicho Comité está compuesto por:

- Presidente: Gerente.
- Vicepresidente: Vicegerente.
- Secretaria o secretario: Responsable de Seguridad de la Información.
- Vocales: Responsables del Sistema, y Responsable de la Información y del Servicio cuando su figura no recaiga en la persona del Gerente.
- Asesora o asesor: Delegado de Protección de Datos.

El Comité de Seguridad de la Información recabará regularmente del personal propio o externo, la información pertinente para la toma de decisiones. La gerencia y todas las subdirecciones y departamentos de Istec están obligadas a informar y prestar apoyo al Comité de Seguridad de la Información cuando éste lo requiera.

El Comité de Seguridad de la Información es el responsable del mantenimiento, la revisión y la mejora continua del sistema de gestión de seguridad de la información de Istec, y tiene las siguientes funciones y responsabilidades:

- Elaborar la estrategia de evolución de Istec en lo que respecta a la seguridad de la información. Identificar, revisar y proponer objetivos estratégicos en materia de seguridad de la información.
- Informar del estado de la seguridad de la información.
- Proponer al Consejo de Administración la aprobación de la política de seguridad de la información.
- Proponer al Gerente la aprobación de las modificaciones sobre la política de seguridad.
- Proponer al Gerente la aprobación de las normativas y reglamentos de seguridad relacionados con la aplicación del ENS, el estándar UNE - ISO/IEC 27001:2013 dentro de su alcance, y resto de normas de aplicación en materia de seguridad de la información.

CSV:EM2M2DZV:MZTHBVDF:Y19C4IE8 URL de validació:https://www.tramita.gva.es/csv-front/index.faces?cadena=EM2M2DZV:MZTHBVDF:Y19C4IE8

- Proponer las iniciativas principales para mejorar la gestión de la seguridad de la información, incluyendo la divulgación de la política y normativas de seguridad.
- Coordinar la adopción de acciones y medidas encaminadas a la adaptación de Istec al ENS, al estándar UNE - ISO/IEC 27001:2013 dentro de su alcance, y resto de normas de aplicación en materia de seguridad de la información.
- Asegurar la disponibilidad de los recursos necesarios para llevar a cabo los planes de acción relacionados con la seguridad de la información o priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Proponer la designación de los responsables encargados de la aplicación y supervisión de las medidas de seguridad.
- Aprobación de los procedimientos de seguridad de Istec cuando así lo solicite el Responsable de Seguridad.
- Realizar una revisión anual del contenido de la Política de Seguridad y una propuesta de actualización cuando sea necesario.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la entidad, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Supervisión y aprobación de las tareas de seguimiento del ENS, el estándar UNE - ISO/IEC 27001:2013 dentro de su alcance, y resto de normas de aplicación en materia de seguridad de la información.

La secretaria o secretario del Comité de Seguridad de la Información será la persona con el rol de Responsable de Seguridad y tendrá como funciones:

- Convocar las reuniones del Comité de Seguridad de la Información.
- Preparar los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elaborar el acta de las reuniones.
- Es responsable de la ejecución directa o delegada de las decisiones del Comité.

Corresponde a los vocales:

CSV:EM2M2DZV:MZTHBVDF:Y19C4IE8 URL de validació:https://www.tramita.gva.es/csv-front/index.faces?cadena=EM2M2DZV:MZTHBVDF:Y19C4IE8

- Participar en las reuniones, contribuyendo con ideas y sugerencias para el buen desarrollo de estas.

Corresponde a los asesores:

- Participar en las reuniones, emitiendo su parecer en aquellos aspectos relacionados con las funciones específicas de su rol.

Todos los miembros del Comité, a excepción de los asesores, actuarán con voz y voto y sus acuerdos requerirán, como mínimo, el voto de la **mayoría simple** de sus miembros.

7.2. Responsable de la Información y del Servicio

El ENS se refiere al concepto de servicio público entendido como el servicio en sí, junto a la información por él tratada. Todo ello soportado por los sistemas de información que son requeridos para que pueda prestarse ese servicio.

El Responsable de la información tiene la potestad de determinar los niveles de seguridad de la información, pues tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección. Cualquier error o negligencia que conlleve un incidente de confidencialidad o de integridad (en materia de protección de datos) y de disponibilidad (en materia de seguridad de la información) recae sobre su persona.

El Responsable del servicio tiene la potestad de determinar los niveles de seguridad de los servicios.

La estructura de Istec refleja el hecho habitual de que un servicio hereda los requisitos de la información que maneja, sin perjuicio de las exigencias en materia de disponibilidad que convenga añadir. Circunstancia que justifica la decisión de la entidad de unificar ambas responsabilidades en una misma figura, con las siguientes funciones y responsabilidades:

- Establecer los requisitos de seguridad que deban ser garantizados en el tratamiento de la información de la que es responsable.
- Establecer los requisitos de los servicios en materia de seguridad que deban ser garantizados en el tratamiento de la información.
- Valorar para cada información y cada servicio contemplados en el análisis de

CSV:EM2M2DZV:MZTHBVDF:Y19C4IE8 URL de validació:https://www.tramita.gva.es/csv-front/index.faces?cadena=EM2M2DZV:MZTHBVDF:Y19C4IE8

riesgos las diferentes dimensiones de la seguridad (disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad).

- Trabajar en colaboración con el Responsable de Seguridad y el del Sistema en el mantenimiento de los sistemas catalogados según el Anexo I del ENS.
- Velar por la inclusión de cláusulas sobre seguridad en los contratos con terceras partes y por su cumplimiento.

7.3. Responsable de Seguridad de la Información y delegado

La complejidad, distribución y separación física de los elementos que componen los sistemas de información de Istec requiere de la definición de un Responsable de Seguridad de la Información y un Responsable de Seguridad de la Información Delegado.

Las funciones del Responsable de Seguridad de la Información son las siguientes:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas TIC, tanto en el ámbito de cumplimiento del ENS, el estándar UNE - ISO/IEC 27001:2013 dentro de su alcance, y la normativa de aplicación en materia de **protección de datos**, como en el resto de normas de aplicación en materia de seguridad de la información.
- Instar y asesorar en la valoración de los requisitos de seguridad que deban ser garantizados en el tratamiento de la información por parte de los nuevos servicios electrónicos prestados por Istec atendiendo al criterio de valoración establecido por el artículo 43 del ENS.
- Realizar o instar la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones de Istec en materia de seguridad.
- Supervisar el estado de seguridad del sistema o sistemas.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.
- Elaborar un informe periódico de seguridad, que incluya los incidentes más relevantes del periodo.
- Elaborar la normativa de seguridad.

CSV:EM2M2DZV:MZTHBVDF:Y19C4IE8 URL de validació:https://www.tramita.gva.es/csv-front/index.faces?cadena=EM2M2DZV:MZTHBVDF:Y19C4IE8

- Llevar a cabo el preceptivo proceso de análisis y gestión de riesgos.
- Promover la formación y concienciación del personal de Istec y en especial, del personal involucrado en las labores de gestión de los sistemas de información que dan soporte a los procesos de Istec.
- Verificar que las medidas de seguridad establecidas son adecuadas para la protección de la información manejada y los servicios prestados.

El Responsable de Seguridad de la Información Delegado tendrá una dependencia funcional directa del Responsable de Seguridad de la Información, que es a quien reporta. Su ámbito de actuación será el de los servicios de Istec, y la información por ellos tratada, a excepción de los propios de las competencias de la entidad en materia de certificación y confianza electrónica, que quedan exclusivamente bajo el amparo del Responsable de Seguridad de la Información. Entre sus funciones delegadas:

- Mantener en su ámbito la seguridad de la información manejada y de los servicios prestados por los sistemas TIC, en cumplimiento del ENS, la normativa vigente de **protección de datos personales** y resto de normas de aplicación en materia de seguridad de la información.
- Colaborar en la supervisión del estado de seguridad del sistema o sistemas bajo su responsabilidad.
- Servir de apoyo en la investigación de los incidentes de seguridad de su ámbito.
- Presentar al Responsable de Seguridad de la Información periódicamente informes de seguridad en su ámbito.
- Participar de la elaboración de la normativa de seguridad de su ámbito.
- Llevar a cabo el preceptivo proceso de análisis y gestión de riesgos en su ámbito.
- Promover la formación y concienciación del personal de Istec en su ámbito.
- Verificar que las medidas de seguridad establecidas son adecuadas para la protección de la información manejada y los servicios prestados en su ámbito.

El Responsable de Seguridad de la Información podrá delegar otras funciones, si bien la responsabilidad última de todas ellas recaerá siempre en su persona.

CSV:EM2M2DZV:MZTHBVDF:Y19C4IE8 URL de validació:https://www.tramita.gva.es/csv-front/index.faces?cadena=EM2M2DZV:MZTHBVDF:Y19C4IE8

7.4. Responsable del Sistema

En el marco del ENS se define sistema de información como conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.

Atendiendo los criterios de complejidad, distribución y separación física ya mencionados, Istec cuenta con dos sistemas diferenciados: uno propio de las actividades de la entidad en el ejercicio de sus competencias en materia de certificación y confianza electrónica (SISTEMA1); y otro que da soporte al resto de actividades de Istec (SISTEMA2).

La entidad define un Responsable del Sistema para cada uno de ellos, con las siguientes funciones sobre el sistema bajo su responsabilidad:

- Desarrollar, operar y mantener el Sistema durante todo su ciclo de vida, incluyendo las especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la tipología y los procedimientos de gestión del Sistema estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Definir la política de conexión o desconexión de equipos y usuarios nuevos en el Sistema.
- Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.
- Decidir las medidas de seguridad que aplicarán los suministradores de componentes del Sistema durante las etapas de desarrollo, instalación y prueba de este.
- Implantar y controlar las medidas específicas de seguridad del Sistema y cerciorarse de que éstas se integren adecuadamente dentro del marco general de seguridad.
- Establecer planes de contingencia y participar de los procesos de análisis y gestión de riesgos en el Sistema.
- Determinar la configuración autorizada de hardware y software a utilizar en el Sistema.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento

CSV:EM2M2DZV:MZTHBVDF:Y19C4IE8 URL de validació:https://www.tramita.gva.es/csv-front/index.faces?cadena=EM2M2DZV:MZTHBVDF:Y19C4IE8

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.
- Elaborar la documentación de seguridad del Sistema.
- Delimitar las responsabilidades de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del Sistema.
- Investigar los incidentes de seguridad que afecten al Sistema, y en su caso, efectuar la comunicación al Responsable de Seguridad o a quién éste determine.

7.5. Delegado de Protección de Datos (DPD)

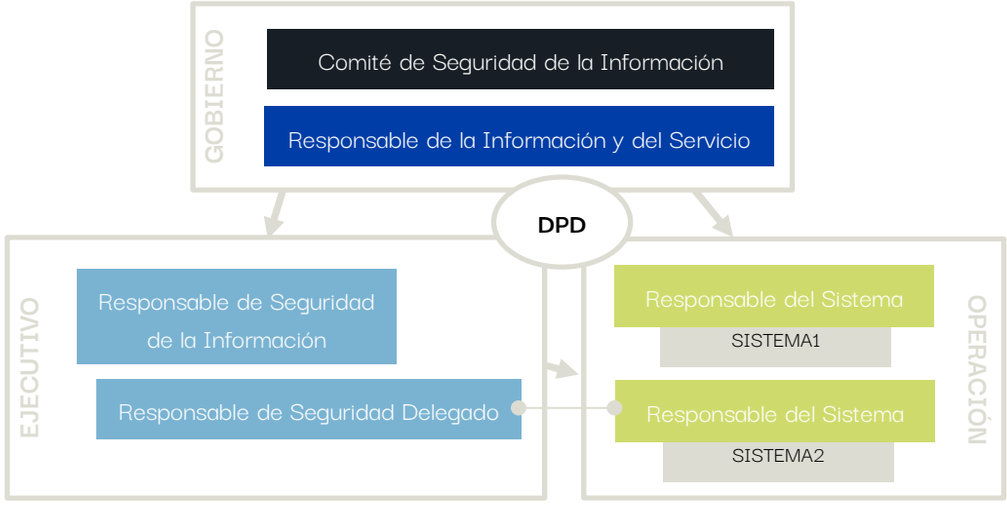
De acuerdo con lo previsto en el artículo 39 del RGPD, las funciones del Delegado de Protección de Datos son las siguientes:

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del RGPD y de otras disposiciones de protección de datos de la Unión o de los Estados miembros.
- Supervisar el cumplimiento de lo dispuesto en el RGPD, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de 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.
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.
- Cooperar con la autoridad de control.
- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, y realizar consultas, en su caso, sobre cualquier otro asunto.

CSV:EM2M2DZV:MZTHBVDF:Y19C4IE8 URL de validació:https://www.tramita.gva.es/csv-front/index.faces?cadena=EM2M2DZV:MZTHBVDF:Y19C4IE8

- 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.

7.6. Resumen



8. Incompatibilidades y procedimientos de designación

La ostentación de uno de los roles descritos inhabilita a la persona designada para la ocupación de cualquier otro de estos. La designación de los roles atiende a esta máxima y es la siguiente:

- Responsable de la Información y del Servicio: Estas funciones serán asumidas por el **Gerente**, que entiende la misión de Istec, determina los objetivos que se propone alcanzar y responde que se alcancen.
- Responsable del Sistema: Istec administra su actividad y competencias a través de subdirecciones, las cuales son las encargadas de implementar, prestar y mantener los diferentes servicios de la entidad.

  Estas funciones serán asumidas por la persona al frente de cada una de las **Subdirecciones**, del siguiente modo: para el SISTEMA1 por la persona al frente

CSV:EM2M2DZV:MZTHBVDF:Y19C4IE8 URL de validació:https://www.tramita.gva.es/csv-front/index.faces?cadena=EM2M2DZV:MZTHBVDF:Y19C4IE8

de la Subdirección con las competencias en materia de certificación y confianza electrónica; y para el SISTEMA2 serán compartidas por las personas al frente del resto de Subdirecciones.

- Responsable de Seguridad de la Información: designado por el Gerente a propuesta del resto de miembros del Comité de Seguridad de la Información, entre el personal de la Subdirección con las competencias en materia de certificación y confianza electrónica (SISTEMA1).
- El Responsable de Seguridad de la Información delegado: designado por el Gerente a propuesta del Responsable de Seguridad de la Información, entre el personal del resto de Subdirecciones (SISTEMA2).
- Delegado de Protección de Datos: Recae en la Conselleria de Participación, Transparencia, Cooperación y Calidad Democrática de la GVA según se especifica la ORDEN 1/2021, de 20 de abril, de la consellera de Participación, Transparencia, Cooperación y Calidad Democrática.

Los nombramientos se revisarán cada **2 años** o cuando alguno de los puestos quede vacante.

9. Revisión de la política de seguridad de la información

Será misión del Comité de Seguridad de la Información la revisión **anual** de esta Política de Seguridad de la Información y la propuesta de modificación o mantenimiento de esta. La Política será aprobada mediante Acuerdo del Consejo de Administración y difundida para que la conozcan todas las partes afectadas.

10. Datos de carácter personal

Istec trata datos de carácter personal. En aplicación del principio de responsabilidad proactiva establecido en el Reglamento General de Protección de Datos (RGPD), las actividades de tratamiento de datos de carácter personal se integrarán en la categorización de sistemas del ENS, considerando las amenazas y riesgos asociados a este tipo de tratamientos. Se aplicará, asimismo, cualquier otra normativa vigente en materia de protección de datos de carácter personal.

CSV:EM2M2DZV:MZTHBVDF:Y19C4IE8 URL de validació:https://www.tramita.gva.es/csv-front/index.faces?cadena=EM2M2DZV:MZTHBVDF:Y19C4IE8

11. Clasificación de la información

Istec establece los siguientes niveles de información manejada por sus sistemas TIC en función de sus exigencias de seguridad, que derivan de las consecuencias que tendría para la entidad su conocimiento por personas que no deben tener acceso a ella.

Nivel	Características
confidencial	Su revelación supondría un grave daño: ■ Ventaja comercial desproporcionada para la competencia. ■ Grave quebranto económico. ■ Quebrar la capacidad de operar de Istec. ■ Serio daño de imagen para Istec y/o la GVA. ■ Serio incumplimiento de obligaciones de confidencialidad adquiridas por Istec con respecto a terceros. ■ Serio incumplimiento de obligaciones legales.
difusión limitada	Su revelación supondría daños indeseables: ■ Ventaja comercial para la competencia. ■ Quebranto económico. ■ Dañar significativamente la capacidad de operar de Istec. ■ Cierto daño de imagen para Istec y/o la GVA. ■ Incumplimiento de obligaciones de confidencialidad adquiridas por Istec con respecto a terceros. ■ Incumplimiento de obligaciones legales.
sin clasificar	Su revelación no supondría un gran perjuicio, aunque pudiera ser embarazosa. Se corresponde con la información interna que no es pública, y a la que pueden acceder todos los miembros de Istec.

Istec desarrolla procedimientos específicos para la clasificación de su información, así como para el correcto tratamiento, mantenimiento, control y supresión de la información clasificada en base a su nivel.

CSV:EM2M2DZV:MZTHBVDF:Y19C4IE8 URL de validació:https://www.tramita.gva.es/csv-front/index.faces?cadena=EM2M2DZV:MZTHBVDF:Y19C4IE8

12. Gestión 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 Seguridad de la Información establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de 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.

La gestión de riesgos quedará documentada en el informe de Análisis y gestión de riesgos.

13. Desarrollo de la política de seguridad de la información

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. 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 Política de seguridad estará disponible en las URLs:

https://www.istecdigital.es/politica-de-seguridad/
https://www.accv.es/politica-de-seguridad/

CSV:EM2M2DZV:MZTHBVDF:Y19C4IE8 URL de validació:https://www.tramita.gva.es/csv-front/index.faces?cadena=EM2M2DZV:MZTHBVDF:Y19C4IE8

14. Obligaciones del personal

Todos y cada uno de los usuarios de los sistemas de información de Istec son responsables de la seguridad de los activos de información mediante un uso correcto de los mismos, siempre de acuerdo con sus atribuciones profesionales y académicas.

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

Los miembros de Istec recibirán formación en seguridad de la información. Se establecerá un programa de concienciación continua para atender a todos los miembros de Istec, 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.

El incumplimiento de la presente Política de Seguridad de la Información podrá acarrear el inicio de las medidas disciplinarias que procedan, sin perjuicio de las responsabilidades legales correspondientes.

15. Terceras partes

Cuando Istec preste servicios a otros organismos o manejen 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 de Seguridad y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando Istec utilice servicios de terceros o cedan 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

CSV:EM2M2DZV:MZTHBVDF:Y19C4IE8 URL de validació:https://www.tramita.gva.es/csv-front/index.faces?cadena=EM2M2DZV:MZTHBVDF:Y19C4IE8

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 el Responsable de la Información y del Servicio antes de seguir adelante.

CSV:EM2M2DZV:MZTHBVDF:Y19C4IE8 URL de validació:https://www.tramita.gva.es/csv-front/index.faces?cadena=EM2M2DZV:MZTHBVDF:Y19C4IE8

Firmas

Firmat per Juan Alegre Sanahuja el 16/06/2022 08:56:55

Control de versiones

Ver.	Autor	Descripción	Aprobación
1.0	COMSEG	Versión inicial.	22.03.2022

Responsabilidades

Acción	Nombre	Fecha
Realizado por:	COMSEG	22.03.2022
Revisado por:	Gerente	22.03.2022
Aprobado por:	Consejo de Administración	22.03.2022

* COMSEG - Comité de Seguridad de la información

CSV:EM2M2DZV:MZTHBVDF:Y19C4IE8 URL de validació:https://www.tramita.gva.es/csv-front/index.faces?cadena=EM2M2DZV:MZTHBVDF:Y19C4IE8