Centro Informático Científico de Andalucía
CONSEJERÍA DE CONOCIMIENTO, INVESTIGACIÓN Y UNIVERSIDAD

JUNTA DE ANDALUCIA

POLÍTICA DE SEGURIDAD INFORMÁTICA

CENTRO INFORMÁTICO CIENTÍFICO DE ANDALUCÍA

Fecha: 22 agosto 2019

Índice de contenido

1. APROBACIÓN Y ENTRADA EN VIGOR....3
2. INTRODUCCIÓN....3
3. DEFINICIONES....5
4. ALCANCE....5
5. MISIÓN....5
6. MARCO NORMATIVO....6
7. OBJETIVOS DE LA POLÍTICA DE SEGURIDAD TIC....7
8. PRINCIPIOS DE SEGURIDAD TIC....7
9. ORGANIZACIÓN DE LA SEGURIDAD....11
9.1. RESPONSABILIDAD GENERAL....11
9.2. ESTRUCTURA ORGANIZATIVA....11
9.3. RESOLUCIÓN DE CONFLICTOS....12
9.4. COMITÉ DE SEGURIDAD TIC DEL CICA (CSTIC)....13
9.5. GRUPO DE RESPUESTA A INCIDENTES EN LOS SISTEMAS DE INFORMACIÓN....15
9.6. RESPONSABLE DE SEGURIDAD TIC....16
9.7. RESPONSABLES DE LA INFORMACIÓN....17
9.8. RESPONSABLES DE LOS SERVICIOS....18
9.9. RESPONSABLES DE LOS SISTEMAS....18
9.10. ADMINISTRADOR DE SEGURIDAD DEL SISTEMA (ASS)....20
10. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN....21
11. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN....21
12. OBLIGACIONES DEL PERSONAL....22
13. TERCERAS PARTES....23
14. GESTIÓN DE RIESGOS....23
15. CLASIFICACIÓN Y CONTROL DE ACTIVOS....24
16. AUDITORÍAS DE SEGURIDAD....24
17. NOTIFICACIONES DE VIOLACIONES DE SEGURIDAD....24
18. DATOS DE CARÁCTER PERSONAL....25
18.1. RESPONSABLES DE LOS TRATAMIENTOS DE DATOS DE CARÁCTER PERSONAL....26
18.2. ENCARGADOS DE LOS TRATAMIENTOS DE DATOS DE CARÁCTER PERSONAL....26
18.3. DELEGADO DE PROTECCIÓN DE DATOS....27

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 22 de agosto de 2019 por el Centro Informático Científico de Andalucía (CICA en adelante).

Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política. Deberá ser revisada y actualizada conforme a las exigencias del CICA o en el momento en que haya la necesidad de realizar cambios sustanciales en la infraestructura tecnológica.

2. INTRODUCCIÓN

El Centro Informático Científico de Andalucía (en adelante CICA) se creó en el año 1989 por el Decreto 43/89 de 7 de marzo, BOJA núm. 25 de 31 de marzo, como centro de la Red de Informática Científica de Andalucía, RICA. En esta disposición se atribuyen al CICA las siguientes funciones:

- Propiciar la formación de un complejo de investigación en tecnologías de la información, tecnologías de las comunicaciones y otras disciplinas relacionadas.
- Participar con sus instalaciones y personal en proyectos de investigación multidisciplinares en colaboración con otros centros de investigación y empresas andaluzas.
- Prestar servicios informáticos a las instituciones y organismos conectados a la Red Informática Científica de Andalucía (RICA).
- Organizar cursos de especialización en materias de su competencia.

El CICA aloja en sus instalaciones el nodo de Red Iris, Red de comunicaciones de la comunidad científica española, para la conexión de la RICA, red autonómica de telecomunicaciones al servicio de la enseñanza superior y la investigación, con la red nacional, a la red paneuropea GEANT y otras redes científicas internacionales.

La Ley 16/2007, de 3 de diciembre, Andaluza de la Ciencia y el Conocimiento, BOJA núm. 250 de 21 de diciembre, recoge en su artículo 49 como la Administración de la Junta de Andalucía favorecerá la existencia de infraestructuras adecuadas para las actividades de I+D+I, que comprenden las instalaciones y recursos físicos y virtuales al servicio de los agentes del Sistema, tanto en el ámbito público como en el privado, cuya utilización se guiará por el criterio de eficiencia en el uso compartido e integrado de las mismas, fomentando modelos de gestión de uso compartido de las infraestructuras y el acceso a proyectos compartidos de ámbito suprarregional.

Entre las competencias de la Dirección General de Investigación y Transferencia del Conocimiento, Centro Directivo del que depende el CICA como infraestructura al servicio del Sistema Andaluz de Ciencia y Tecnología, se encuentran la gestión de las redes científicas y tecnológicas, así como la ejecución del Plan Andaluz de Investigación, Desarrollo e Innovación, y de manera particular de las políticas de Formación de Recursos Humanos, Investigadores e Investigadoras y Tecnólogos y Tecnólogas, de infraestructura científica, de promoción general del conocimiento y de divulgación científica.

De esta forma, el CICA presta diversos servicios a los Agentes del Sistema Andaluz del Conocimiento:

- Gestión de la Red Informática Científica de Andalucía (RICA), que interconecta las Universidades y Centros de Investigación de Andalucía, proporcionándoles además acceso a la red científica a nivel nacional (RedIRIS) y a Internet.

- Sincronización horaria (NTP) de nivel Stratum 1.
- Alojamiento de equipamiento físico en su CPD: servidores, almacenamiento, comunicaciones y demás equipo TIC.
- Alojamiento de servicios de aplicaciones web, servidores y sistemas informáticos en general.
- Recursos de supercomputación y cálculo intensivo a la comunidad científica de Andalucía, en sus labores de investigación.
- Recursos para fomentar los desarrollos de software libre en la comunidad así como servir de soporte a iniciativas de interés en el entorno académico-científico relacionadas con el conocimiento libre.
- Servicios de seguridad: asesoramiento técnico en esta materia a las instituciones y centros conectados a la red RICA, además de la gestión de incidentes de seguridad (NIS).

Por todo lo arriba referido, el Centro Informático Científico de Andalucía, para llevar a cabo su cometido, precisa de Políticas de Seguridad de la Información (en adelante PSI) que establezcan las medidas de índole técnica y organizativas necesarias para garantizar la seguridad de las Tecnologías de la Información y las Comunicaciones (en adelante TIC), consistentes en sistemas de información, equipos de cómputo, redes de voz y datos, etc., de las y personas que interactúan haciendo uso de los servicios asociados a dichas TIC.

El CICA 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.

Como organismo perteneciente a la Administración de la Junta de Andalucía, al CICA se le aplica la Política de Seguridad TIC publicada en Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía (http://www.juntadeandalucia.es/boja/2011/11/d2.pdf), modificado por el Decreto 70/2017, de 6 de junio, por el que se modifica el Decreto 1/2011 (http://www.juntadeandalucia.es/boja/2017/110/1).

Según el apartado 2 del artículo 1 del citado Decreto, "*cada entidad incluida en el ámbito de aplicación del Decreto desarrollará y aprobará el documento de política de seguridad TIC de la entidad, así como las normas y procedimientos que adecuen, en su caso, las directrices comunes de la Administración de la Junta de Andalucía a sus particularidades.*". Además, el artículo 10 dice: "*Sin perjuicio de las directrices establecidas en el marco regulador de seguridad TIC de la Administración de la Junta de Andalucía, cada Consejería y entidad incluida en el ámbito de aplicación del presente Decreto deberá disponer formalmente de su propio documento de política de seguridad TIC, así como de las disposiciones de desarrollo que adecuen, en su caso, las directrices comunes de la Administración de la Junta de Andalucía a sus particularidades*".

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. La Seguridad Informática se basa en la existencia de un conjunto de directrices que brinden instrucciones claras y oportunas, soportando la gestión frente al gran dinamismo de nuevos ataques y violaciones a la seguridad e integridad de la información.

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.

El 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 (en adelante ENS), modificado parcialmente por el Real Decreto 951/2015, de 23 de octubre, tiene por objeto determinar la política de seguridad en la utilización de medios electrónicos en su ámbito de aplicación, sus principios básicos y los requisitos mínimos que permitan una protección adecuada de la información. Esto implica que los organismos deben aplicar las medidas mínimas de seguridad exigidas por el ENS, 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 organismos 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, en la solicitud de ofertas, y en los pliegos de licitación para proyectos TIC.

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

Este documento se debe entender como el compendio de reglas que permiten definir la gestión, protección y asignación de los recursos, concienciando a cada uno de los miembros del CICA acerca de la importancia y sensibilidad de los sistemas de información y de la información que se almacena en ellos.

Todas las directrices contempladas en este documento deben ser revisadas periódicamente, determinando oportunamente la creación, actualización y obsolescencia de cada una de ellas, con el fin de mitigar las vulnerabilidades identificadas y mantener altos estándares de seguridad en el CICA.

3. DEFINICIONES

A los efectos previstos en este documento, las definiciones han de ser entendidas en el sentido indicado en el Glosario de términos incluido como Anexo I.

4. ALCANCE

Las políticas y estándares contempladas en este documento se aplican a todos los sistemas TIC del CICA y a todos los miembros de la organización, sin excepciones, incluyendo a todos los empleados y contratistas del CICA, y todo el personal tercero, que hagan uso de los sistemas, plataformas y servicios tecnológicos de la Organización.

5. MISIÓN

El CICA tiene como misión responder a las necesidades e intereses de los investigadores y grupos de investigación, las Universidades y el resto de Agentes del Sistema Andaluz del Conocimiento (en adelante SAC), mediante la prestación de servicios TIC dentro del ámbito de competencias del CICA; difundir y fomentar el uso de estos servicios, atendiendo las necesidades de apoyo informático a las tareas de investigación.

6. MARCO NORMATIVO

- DIRECTIVA 95/46: Protección de personas físicas y tratamiento de datos. http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:31995L0046
- REAL DECRETO Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual. https://www.boe.es/diario_boe/txt.php?id=BOE-A-1996-8930
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. https://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750
- Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, por el que se aprueba el Reglamento General de Protección de Datos, 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. https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807. En adelante Reglamento General de Protección de Datos
- Ley 59/2003, de 19 de diciembre, de firma electrónica. https://www.boe.es/buscar/doc.php?id=BOE-A-2003-23399
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2007-12352
- 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. https://www.boe.es/buscar/act.php?id=BOE-A-2008-979
- REGLAMENTO (CE) nº 460/2004 del Parlamento Europeo y del Consejo, de 10 de marzo de 2004, (https://www.boe.es/doue/2004/077/L00001-00011.pdf) por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información, modificado por el Reglamento (CE) nº 1007/2008 del Parlamento Europeo y del Consejo, de 24 de septiembre de 2008. https://www.boe.es/buscar/doc.php?id=DOUE-L-2008-82156
- 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. https://www.boe.es/buscar/doc.php?id=BOE-A-2010-1330. BOE de 29 de enero de 2010.
- DECRETO 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía (http://www.juntadeandalucia.es/boja/2011/11/d2.pdf), modificado por el Decreto 70/2017, de 6 de junio, por el que se modifica el Decreto 1/2011 (http://www.juntadeandalucia.es/boja/2017/110/1).
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2014-4950.
- DIRECTIVA 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra sistemas de información. http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32013L0040
- Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas.

- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Orden de 10 de enero de 2017, por la que se regula la composición, atribuciones, funcionamiento y método de trabajo del Comité de Seguridad de las Tecnologías de la Información y Comunicaciones de la Consejería de Economía y Conocimiento (http://www.juntadeandalucia.es/boja/2017/11/1)
- NORMA UNE ISO/IEC 27002. http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0055190
- NORMA UNE-EN-ISO/IEC 27001:2014

  http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0053761.

7. OBJETIVOS DE LA POLÍTICA DE SEGURIDAD TIC

En consonancia con la Política de Seguridad TIC (PSTIC) de la Junta de Andalucía, los objetivos perseguidos son los siguientes:

a) Marcar las directrices, los objetivos y los principios básicos de seguridad TIC de la Consejería.

b) Establecer un modelo integral de gestión de la seguridad TIC en el Centro, que cubra en un ciclo continuo de mejora los aspectos técnicos, organizativos y procedimentales en los servicios que presta el CICA.

c) Establecer la estructura de la organización de la seguridad TIC de la Consejería.

d) Garantizar a las personas usuarias de los servicios del CICA y a los distintos agentes del SAC que sus datos serán gestionados de acuerdo a los estándares y buenas prácticas en seguridad TIC.

e) Aumentar el nivel de concienciación en materia de seguridad TIC de todas las entidades a las que es de aplicación la Política, garantizando que el personal a su servicio es consciente de sus obligaciones y responsabilidades.

f) Garantizar el cumplimiento de la legislación vigente en materia de seguridad TIC.

g) Servir de base para el desarrollo de las normas, procedimientos y procesos de gestión de la seguridad TIC.

8. PRINCIPIOS DE SEGURIDAD TIC

La PSTIC del CICA se desarrollará,con carácter general, de acuerdo a los siguientes principios, además de los establecidos en la normativa reguladora de la política de seguridad de las tecnologías de la información y las comunicaciones en la Administración de la Junta de Andalucía y en el Esquema Nacional de Seguridad en el ámbito de la administración electrónica:

a) Alcance estratégico: la seguridad TIC debe contar con el compromiso y apoyo de todos los niveles directivos de forma que pueda estar coordinada e integrada con el resto de iniciativas estratégicas del Centro, para conformar un todo coherente y eficaz.

b) Responsabilidad: todo el personal del CICA es responsable de garantizar la seguridad de los sistemas de información con diferentes grados de participación según las funciones o atribuciones asignadas debiendo, de forma general cumplir con el marco normativo en materia de seguridad y protección de datos de carácter personal que el CICA haya publicado y distribuido entre el personal. Cada persona

que de una u otra forma participe en la utilización, operación, administración o gestión de un sistema de información será informada de sus responsabilidades, que estarán determinadas de forma explícita e inequívoca.

c) Función diferenciada: la responsabilidad de la seguridad de los sistemas de tecnologías de la información y las comunicaciones estará diferenciada de la responsabilidad sobre la prestación de los servicios, tal y como aparece en el apartado 10 del ENS.

d) Confidencialidad: los activos TIC deberán ser accesibles únicamente para aquellas personas usuarias, órganos y entidades o procesos expresamente autorizados para ello, con respeto a las obligaciones de secreto y sigilo profesional.

e) Integridad y calidad: se deberá garantizar el mantenimiento de la integridad y calidad de la información, así como de los procesos de tratamiento de la misma, estableciéndose los mecanismos para asegurar que los procesos de creación, tratamiento, almacenamiento y distribución de la información contribuyen a preservar su exactitud y corrección.

f) Disponibilidad y continuidad: se garantizará un alto nivel de disponibilidad en los activos TIC y se dotarán de los planes y medidas necesarias para asegurar la continuidad de los servicios y la recuperación ante posibles contingencias graves.

g) Gestión del riesgo: se deberá articular un proceso continuo de análisis y tratamiento de riesgos como proceso esencial sobre el que debe descansar la gestión de la seguridad de los activos TIC. Las decisiones en materia de seguridad se basarán en dicho análisis y gestión de riesgos, que deberá mantenerse permanentemente actualizado. La evaluación de riesgos debe ser suficientemente amplia para abarcar los principales factores internos y externos tales como factores tecnológicos, físicos y humanos, políticos y servicios de terceros con implicaciones 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 de carácter personal.

   La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando dichos riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerán un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad.

h) Proporcionalidad: la implantación de medidas que mitiguen los riesgos de seguridad de los activos TIC deberá hacerse bajo un enfoque de proporcionalidad en los costes económicos y operativos. 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.

i) Concienciación y formación: todo el personal del CICA debe ser consciente de la necesidad de garantizar la seguridad de los sistemas de información, así como que ellos mismos son una pieza esencial para el mantenimiento y mejora de la seguridad. El conocimiento de los riesgos es la primera línea de defensa para la seguridad de los sistemas de información. Para mitigarlos, el CICA ha redactado un marco normativo en materia de seguridad y el conocimiento y cumplimiento de dichas normativas de seguridad contribuirán de modo efectivo a reducir los potenciales riesgos que pudieran afectar al buen funcionamiento de los sistemas de información. Por lo tanto, se articularán iniciativas que permitan a las personas usuarias conocer sus deberes y obligaciones en cuanto al tratamiento seguro de la información se refiere.

   El personal del CICA debe estar debidamente concienciado sobre esta materia para que pueda ser

capaz de detectar posibles incidentes que pudieran perjudicar seriamente los sistemas de información. Se fomentará la formación específica en materia de seguridad TIC de todas aquellas personas que gestionan y administran sistemas TIC.

j) Prevención, reacción y recuperación: se desarrollarán planes y líneas de trabajo específicas orientadas a prevenir fraudes, incumplimientos o incidentes relacionados con la seguridad TIC.

Las medidas de prevención deben eliminar 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 se 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, se deberá:

- 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.

Se monitorizará 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.

Se pondrá especial interés en:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otras áreas 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).

Las medidas de detección estarán acompañadas de medidas de reacción, de forma que los incidentes de seguridad se atajen en la mayor brevedad de tiempo que sea posible.

Las medidas de recuperación permitirán la restauración de la información y los servicios, de forma que se pueda hacer frente a las situaciones en las que un incidente inhabilite los medios habituales. Para garantizar la disponibilidad de los servicios críticos, se deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

k) Mejora continua: se revisará el grado de eficacia de los controles de seguridad TIC implantados, al objeto de adecuarlos a la constante evolución de los riesgos y del entorno tecnológico del CICA. La

gestión de la seguridad de la información requiere una evaluación y una auditoría continua para comprobar que los requisitos establecidos por el R.D. 3/2010 se cumplen y que las medidas de seguridad son eficaces proporcionando el nivel de seguridad deseado. Ello implica la coordinación de los aspectos técnicos, jurídicos y organizativos establecidos como medidas de seguridad en el citado R.D.

La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y dedicado. Se llevará un control de las incidencias que se producen para agilizar la reacción éstas, con el objetivo de reducir los daños que puedan producir, reaccionar de manera coordinada y obtener evidencias que permitan introducir los cambios necesarios para que las incidencias no vuelvan repetirse. Se generarán las correspondientes acciones preventivas, correctivas o de mejora que sean analizadas tras analizar los hechos.

l) 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.

   Las especificaciones de seguridad se incluirán en todas las fases del ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control. Los sistemas de información deben diseñarse y configurarse de forma que garanticen la seguridad por defecto.

   La seguridad debe ser un elemento fundamental de todos los servicios, sistemas y redes del CICA, así como una parte integrante del diseño de los sistemas de información y su arquitectura.

   En los entornos de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que no sean de interés, sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue.

m) Legalidad: las medidas de seguridad deben ser aplicadas de manera coherente con la legislación garante de la intimidad de las personas, incluida la libertad de intercambiar pensamientos e ideas, el libre flujo de información y la protección adecuada de los datos de carácter personal. La seguridad de los sistemas de información debe preservar y proteger dichos valores respecto de los datos que sean custodiados por el CICA en relación a los servicios que presta.

Las directrices fundamentales de seguridad se concretan en un conjunto de principios particulares y responsabilidades específicas, que se configuran como objetivos instrumentales que garantizan el cumplimiento de los principios básicos de la PSTIC y que inspiran las actuaciones del Centro en dicha materia. Se establecen los siguientes:

a) Protección de datos de carácter personal: Se adoptarán las medidas técnicas y organizativas que corresponda implantar para atender los riesgos generados por el tratamiento de acuerdo a lo exigido por el citado Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

b) Gestión de activos de información: Los activos de información del Centro se encontrarán inventariados y categorizados y estarán asociados a un responsable.

c) Seguridad ligada a las personas: Se implantarán los mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.

d) Seguridad física: Los activos de información serán emplazados en áreas seguras, protegidas por

controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.

e) Seguridad en la gestión de comunicaciones y operaciones: Se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las TIC. La información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.

f) Control de acceso: Se limitará el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de la organización.

g) Adquisición, desarrollo y mantenimiento de los sistemas de información: Se contemplarán los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.

h) Gestión de los incidentes de seguridad: Se implantarán los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.

i) Gestión de la continuidad: Se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus procesos de negocio, de acuerdo a las necesidades de nivel de servicio de sus usuarios.

j) Cumplimiento: Se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información.

9. ORGANIZACIÓN DE LA SEGURIDAD

9.1. RESPONSABILIDAD GENERAL

La preservación de la seguridad TIC será considerada objetivo común de todas las personas al servicio del CICA, siendo éstas responsables del uso correcto de los activos TIC puestos a su disposición.

9.2. ESTRUCTURA ORGANIZATIVA

La estructura organizativa de la gestión de la seguridad TIC del CICA, en relación con el Esquema Nacional de Seguridad en el ámbito de la administración electrónica, está compuesta por las siguientes figuras:

a) El Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones, en adelante Comité de Seguridad TIC, y el Grupo de Respuesta a Incidentes en los Sistemas de Información.

b) Responsable de Seguridad TIC.

c) Responsables de la Información.

d) Responsables del Sistema.

e) Responsables del Servicio.

Además, en el ámbito de la Consejería, las siguientes figuras ostentan atribuciones directamente relacionadas con la seguridad TIC que son las que les asigna la normativa sobre protección de datos de carácter personal:

a) Responsables de los Tratamientos de datos de carácter personal.

b) Encargados de los Tratamientos de datos de carácter personal.

c) El Delegado de Protección de Datos, en adelante DPD.

En consonancia con el ENS, concretamente con su artículo 10:

- En los sistemas de información se diferenciará el Responsable de la Información (en adelante RI), el Responsable del Servicio (en adelante RSER) y el Responsable de la Seguridad (en adelante RSEG).
- El RI determinará los requisitos de la información tratada; el RSER determinará los requisitos de los servicios prestados; y el RSEG determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.
- La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios, por lo tanto, tal y como queda expresamente prohibido por el ENS, no pueden recaer sobre la misma persona las responsabilidades de Responsable del Sistema y Resonsable de Seguridad.
- La política de seguridad de la organización detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos.

La estructura organizacional diferencia 3 grandes bloques de responsabilidad: la especificación de las necesidades o requisitos, la operación del sistema de información que se atiene a aquellos requisitos y la función de supervisión de acuerdo al principio básico del ENS "*La seguridad como función diferenciad*a".

- La especificación de requisitos de seguridad corresponde al RI y al RSER, junto con el responsable del fichero si hubiera datos de carácter personal.
- La operación corresponde al Responsable del Sistema (en adelante RSIS).
- La supervisión corresponde al RSEG.

De acuerdo con el principio arriba citado de "*La seguridad como función diferenciada*" el RSEG será independiente del RSIS

9.3. RESOLUCIÓN DE CONFLICTOS

De acuerdo con el Principio de Jerarquía que rige en las administraciones públicas españolas, en caso de conflicto éste deberá ser resuelto por el superior jerárquico común. En su defecto, prevalecerán las decisiones del Comité de Seguridad TIC adoptadas en sesión plenaria sobre las adoptadas por el Grupo de Respuesta a Incidentes de Seguridad de la Información.

En los conflictos entre las personas responsables que componen la estructura organizativa de la política de seguridad TIC y las personas responsables definidas en la normativa de protección de datos de carácter personal prevalecerá la decisión que presente un mayor nivel de exigencia respecto a la protección de los datos de carácter personal.

9.4. COMITÉ DE SEGURIDAD TIC DEL CICA (CSTIC)

La Seguridad TIC se organiza en el CICA dentro de las estructuras que a tal efecto existen en la Consejería en la que se encuentra circunscrito y en la organización de Seguridad TIC de la Junta de Andalucía definida según el DECRETO 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía.

A estos efectos, la composición, atribuciones, funcionamiento y método de trabajo del Comité de Seguridad de las Tecnologías de la Información y Comunicaciones de la Consejería de Economía y Conocimiento están regulados según Orden de 10 de enero de 2017, publicada en BOJA n.º 11 de 18/01/2017 (http://www.juntadeandalucia.es/boja/2017/11/1). Es el órgano colegiado de dirección y seguimiento en materia de seguridad de los activos TIC de titularidad de la Consejería o cuya gestión tenga encomendada.

Para una mejor coordinación entre dicho Comité de Seguridad y el CICA, así como para establecer una estructura organizacional conforme a lo indicado por el Real Decreto 3/2010 y por el Decreto 1/2011, se establece el Comité de Seguridad TIC del CICA, que estará formado por:

- Presidencia: la persona titular de la Dirección del CICA.
- Vocalías:
  - La persona titular de la Gerencia del CICA.
  - La persona titular de la Jefatura de Informática del CICA.
- Secretaría: la persona Responsable de la Seguridad TIC o persona designada por el CSTIC en su defecto.

El Comité de Seguridad TIC del CICA mantendrá una estrecha colaboración con el Comité de Seguridad TIC de la Consejería a la que se encuentra adscrito el CICA.

El CSTIC ostenta las responsabilidades de las figuras RI y RSER, además de las de RSIS y RSEG.

Podrán ser nombradas personas concretas para ejercer las responsabilidades de RI, RSER, RSIS y RSEG. El nombramiento de cada una de ellas será realizado por la persona titular de la Dirección General a la que se adscribe el CICA a propuesta del CSTIC, y será revisado cada 2 años o cuando el puesto quede vacante. En el caso de que el puesto correspondiente a RI, RSER, RSIS o RSEG quede vacante, la responsabilidad pasará automáticamente al CSTIC hasta que una nueva persona sea nombrada para ejercer el rol correspondiente. Los nombramientos atenderán siempre al principio de función diferenciada.

Se mantendrá actualizado un documento específico con la relación detallada de las personas nombradas en cada una de las responsabilidades. La última versión se incluirá como Anexo I a la presente PSTIC.

El Comité de Seguridad TIC tendrá las siguientes funciones:

a) Atender las peticiones en materia de seguridad TIC de las áreas del CICA.

b) Informar regularmente a la persona titular de la Dirección General en la que se circunscribe el CICA del estado de la seguridad de las TIC en su ámbito.

c) Promover la mejora continua del sistema de gestión de la seguridad TIC.

d) Elaborar la estrategia de evolución de la seguridad TIC del CICA, en el marco de las directrices e iniciativas estratégicas emanadas de sus instancias jerárquicas superiores dentro de la organización de la Junta de Andalucía.

e) Coordinar los esfuerzos de todo el equipo humano con responsabilidad en materia de seguridad TIC para asegurar que son consistentes y están alineados con la estrategia decidida, evitando duplicidades y racionalizando el gasto.

f) Elaborar y revisar regularmente la PSTIC del CICA y proponer su aprobación.

g) Aprobar las normas y procedimientos de seguridad TIC del CICA.

h) Elaborar y aprobar los requisitos de formación y cualificación de las personas administradoras, operadoras y usuarias desde el punto de vista de seguridad TIC.

i) Aprobar los planes de concienciación y formación propuestos por el RSEG.

j) Monitorizar los principales riesgos residuales asumidos por la Consejería y recomendar posibles actuaciones respecto a ellos.

k) Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto a ellos, velando en particular por la coordinación en la gestión de incidentes de seguridad TIC.

l) Promover la realización de las auditorias periódicas que permitan verificar el cumplimiento de las obligaciones del CICA en materia de seguridad TIC.

m) Aprobar los planes de mejora de la seguridad TIC en el CICA, junto con su dotación presupuestaria correspondiente, velando en particular por la coordinación entre diferentes planes que puedan coexistir.

n) Priorizar las actuaciones en materia de seguridad TIC cuando los recursos sean limitados.

o) Velar para que la seguridad TIC se tenga en cuenta en todos los proyectos desde su especificación inicial hasta su puesta en producción, procurando la creación y utilización de servicios horizontales que reduzcan duplicidades y permitan un funcionamiento homogéneo de todos los sistemas.

p) Aprobar y coordinar los planes de continuidad elaborados por el RSIS y validados por el RSEG.

q) Resolver los conflictos de competencia que se puedan suscitar entre los diferentes responsables de la gestión de la seguridad TIC o elevar propuesta para resolverlos, en su caso.

Funcionamiento y método de trabajo del Comité de Seguridad TIC.

1. El Comité de Seguridad TIC se reunirá con carácter ordinario, al menos, tres veces al año y, con carácter extraordinario, cuando lo decida la persona titular de la Presidencia de oficio o a propuesta de alguno de sus miembros, y siempre que:
   a) Se produzcan incidencias de seguridad graves que afecten a cualquier sistema de la Consejería.
   b) Surjan nuevas necesidades de seguridad que requieran la participación del Comité.
2. El Comité de Seguridad TIC se podrá constituir, convocar, celebrar sus sesiones, adoptar acuerdos y remitir actas, tanto de forma presencial como a distancia, salvo que su reglamento interno recoja expresa y excepcionalmente lo contrario, con las medidas adecuadas que garanticen la identidad de las personas comunicantes y la autenticidad de la información entre ellas transmitida, de conformidad con lo establecido en el artículo 91.3 de la Ley 9/2007, de 22 de octubre.
3. Los miembros del Comité de Seguridad TIC podrán proponer a la Presidencia, individual o colectivamente, la inclusión de asuntos en el orden del día. La propuesta deberá realizarse por escrito

dirigido a la Presidencia y al resto de los miembros, con una antelación mínima de 24 horas de la convocatoria.

4. A las sesiones del Comité de Seguridad TIC podrán asistir en calidad de asesoras, con voz pero sin voto, las personas que en cada caso estime pertinente la Presidencia, por iniciativa propia o a propuesta de sus miembros.
5. El Comité de Seguridad TIC podrá crear en su seno, las ponencias técnicas o grupos de trabajo que requiera el normal desarrollo de sus funciones.
6. El funcionamiento del Comité de Seguridad TIC y, en su caso, de las ponencias técnicas o grupos de trabajo, se ajustará a lo dispuesto en el presente documento y a las normas establecidas para el funcionamiento de los órganos colegiados por la Sección3.ª del Capítulo II del Título Preliminar de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, y por la Sección 1.ª del Capítulo II del Título IV de la Ley 9/2007, de 22 de octubre.
7. El Comité de Seguridad TIC se regirá por este documento, por la normativa reguladora de la política de seguridad de las tecnologías de la información y las comunicaciones en la Administración de la Junta de Andalucía, así como por el resto de normativa aplicable, como la reguladora del ENS y la normativa de protección de datos de carácter personal.

9.5. GRUPO DE RESPUESTA A INCIDENTES EN LOS SISTEMAS DE INFORMACIÓN

El Comité de Seguridad TIC nombrará un Grupo de Respuesta a Incidentes de Seguridad de la Información, cuya función será la toma urgente de decisiones en caso de contingencia grave que afecte a la seguridad de los sistemas de información críticos del CICA. Será la persona titular de la Presidencia del Comité de Seguridad TIC quien determine la existencia de tales contingencias y las califique como graves. Las decisiones adoptadas por este grupo serán ratificadas por el Comité en su conjunto cuando sea necesario.

- La composición mínima de este grupo será la siguiente:
  a) La persona titular de la Presidencia del Comité de Seguridad TIC.
  b) La persona titular de la Vicepresidencia del Comité de Seguridad TIC.
  c) La persona titular de la Jefatura de Informática del CICA
- En el ejercicio de las funciones del grupo participarán en calidad de asesores:
  a) La persona Responsable de Seguridad TIC.
  b) La persona que ostente la condición de Delegado de Protección de Datos.
- Su composición podrá ser modificada mediante acuerdo del Comité de Seguridad TIC.
- Corresponde al Grupo de Respuesta a Incidentes de Seguridad de la Información, entre sus funciones, notificar a la autoridad competente en materia de seguridad de las redes y sistemas de información, concretamente a su equipo de respuesta a incidentes de seguridad informática (CSIRT o CERT), los incidentes de seguridad TIC, en los casos y en los términos que determine la normativa aplicable.
- La notificación mencionada en el apartado anterior podrá realizarse bien directamente, bien a través de AndalucíaCERT o por el medio o procedimiento que disponga la política de seguridad de las

tecnologías de la información y comunicaciones de la Junta de Andalucía que determine la Dirección General competente en materia de coordinación y ejecución de las políticas de seguridad de los sistemas de información y telecomunicaciones de la Administración de la Junta de Andalucía o el Comité de Seguridad TIC corporativo de la Junta de Andalucía.

- La Consejería estará integrada en el grupo atendido del Centro de Seguridad TIC AndalucíaCERT

9.6. RESPONSABLE DE SEGURIDAD TIC

Sus responsabilidades son las siguientes:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en esta PSTIC, en el Real Decreto 1720/2007 de Protección de Datos de Carácter Personal y en el ENS.
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.
- Elaborar y revisar periódicamente los planes de concienciación y formación, y presentarlos al CSI para su aprobación.
- Informar al Responsable de la Información de las decisiones e incidentes en materia de seguridad que afecten a la información que le compete, en particular de la estimación de riesgo residual y de las desviaciones significativas de riesgo respecto de los márgenes aprobados.
- Informar al Responsable del Servicio de las decisiones e incidentes en materia de seguridad que afecten al servicio que le compete, en particular de la estimación de riesgo residual y de las desviaciones significativas de riesgo respecto de los márgenes aprobados.
- Reportar al Comité de Seguridad TIC (CSTIC), como secretario:
  - Resumen consolidado de actuaciones en materia de seguridad.
  - Resumen consolidado de incidentes relativos a la seguridad de la información.
  - Estado de la seguridad del sistema, en particular del riesgo residual al que el sistema está expuesto.
- Realizar los pertinentes análisis de riesgos para los Sistemas de Información
- Determinar la Declaración de Aplicabilidad, teniendo en cuenta los mínimos requeridos por el Anexo II del ENS y las medidas adicionales que se estimen oportunas.
- Proponer los indicadores de riesgo (KRI – Key Risk Indicators) para los sistemas de información de categoría alta:
  - Su definición concreta será acordada por el RSEG y el propietario del riesgo, indicando expresamente:
    - En qué medidas se basan.
    - Cuál es el algoritmo de cálculo.
    - Periodicidad de evaluación
    - Umbrales de aviso y alarma para atención urgente

- Se presentarán al responsable correspondiente:
  - Rutinariamente, con periodicidad acordada entre el RSEG y el propietario del riesgo.
  - Puntualmente, por demanda expresa del propietario del riesgo medido.
  - Extraordinariamente, cuando se supera un umbral de riesgo.
- Estarán a disposición de los auditores.

- Determinar la configuración de seguridad de los sistemas.
- Elaborar y revisar regularmente la documentación de seguridad de los sistemas.
- Elaborar y revisar regularmente las normas de seguridad.
- Aprobar los procedimientos operativos de seguridad, a propuesta del Responsable del Sistema.
- Realizar los informes del estado de seguridad de los sistemas, que reportará al CSI.
- Elaborar los planes de mejora de la seguridad junto con el RSIS.
- Validar los planes de continuidad elaborados por el RSIS, y presentarlos al CSI para su aprobación y coordinación.
- Aprobar las definiciones del ciclo de vida de los sitemas: especificación, arquitectura, desarrollo, operación y cambios, que elabora el RSIS.
- Analizar y proponer salvaguardas que prevengan incidentes de seguridad, tanto de manera proactiva como tras la aparición de un incidente de seguridad concreto.

9.7. RESPONSABLES DE LA INFORMACIÓN

Los Responsables de la Información serán los órganos directivos que decidan sobre la finalidad, contenido y uso de la información. Sus funciones son las siguientes:

- El Responsable de la Información (RI) tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.
- El RI es el responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.
- Tiene la potestad de establecer los requisitos de la información en materia de seguridad, en terminología del ENS, la potestad de determinar los niveles de seguridad de la información. De esta forma, corresponde al RI la aprobación formal de los niveles definidos para el Sistema o Sistemas, pudiendo recabar una propuesta al RSEG y escuchar al RSIS, categorizando la información mediante la valoración de los impactos de los incidentes que puedan producirse.
- Si esta información incluye datos de carácter personal, además deberán tenerse en cuenta las medidas de seguridad que corresponda implantar teniendo en cuenta los riesgos generados por el tratamiento de acuerdo a lo exigido por el citado Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.
- Proporcionar la información necesaria al RSEG para realizar los preceptivos análisis de riesgos, con la finalidad de establecer las salvaguardas a implantar. Para ello contará con la ayuda de los RSER y de los RSIS implicados.

- Es el propietario de los riesgos sobre la información, debiendo ser informado de los riesgos que afectan a su propiedad y del riesgo residual al que está sometida. Cuando un sistema de información entra en operación, los riesgos residuales deben haber sido aceptados formalmente por su correspondiente propietario.
- Es responsable de monitorizar los riesgos de los que es propietario y de verificar que los análisis de riesgos realizados se corresponden en todo momento con la información aportada para la realización de los mismos.

9.8. RESPONSABLES DE LOS SERVICIOS

Los Responsables de los Servicios serán los órganos directivos que decidan sobre las características de los servicios a prestar. Sus funciones son las siguientes:

- El Responsable del Servicio (RSER) tiene la potestad de establecer los requisitos del servicio en materia de seguridad, es decir, determinar los niveles de seguridad de los servicios. De esta forma, corresponde al RI la aprobación formal de los niveles definidos para el Servicio o Servicios, pudiendo recabar una propuesta al RSEG y escuchar al RSIS, categorizando los servicios mediante la valoración de los impactos de los incidentes que puedan producirse.
- Si este servicio incluye datos de carácter personal, además deberán tenerse en cuenta las medidas de seguridad que corresponda implantar teniendo en cuenta los riesgos generados por el tratamiento de acuerdo a lo exigido por el citado Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.
- La prestación de un servicio atenderá a los requisitos de seguridad de la información que maneja, es decir, “se heredan los requisitos”, lo que suele añadir requisitos de disponibilidad, accesibilidad, interoperabilidad, etc.
- Proporcionará la información necesaria al RSEG para realizar los preceptivos análisis de riesgos, con la finalidad de establecer las salvaguardas a implantar. Para ello contará con la ayuda de los RI y de los RSIS implicados.
- Es el propietario de los riesgos sobre los servicios, debiendo ser informado de los riesgos que afectan a su propiedad y del riesgo residual al que está sometida. Cuando un sistema de información entra en operación, los riesgos residuales deben haber sido aceptados formalmente por su correspondiente propietario.
- Es responsable de monitorizar los riesgos de los que es propietario y de verificar que los análisis de riesgos realizados se corresponden en todo momento con la información aportada para la realización de los mismos.

9.9. RESPONSABLES DE LOS SISTEMAS

Los Responsables de los Sistemas serán las personas adscritas al Responsable de Informática designadas al efecto por la persona titular de la Jefatura de Informática y figurarán en la documentación de seguridad de los sistemas de información. Para cada sistema de información deberá existir una persona Responsable del Sistema, siendo posible que una misma persona sea responsable de varios sistemas.

Las responsabilidades del Responsable del Sistema (RSIS) son las siguientes:

- Supervisar el desarrollo, operación y mantenimiento del Sistema o Sistemas de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Ser la primera persona responsable de la seguridad de los Sistemas de Información que dirija, velando porque la segudidad TIC esté presente en todas y cada una de las partes de sus ciclos de vida. Especialmente deberá velar porque el desarrollo de los sistemas siga las directrices de seguridad establecidas de manera horizontal por la Junta de Andalucía de acuerdo con los criterios y requisitos técnicos de seguridad aplicables definidos por el RSEG del CICA.
- La creación, el mantenimiento y actualización continua de la documentación de seguridad de los sistemas de información, con el asesoramiento del RSEG.
- Definir la política de conexión o desconexión de equipos y usuarios nuevos en el Sistema.
- Determinar la configuración autorizada de hardware y software a utilizar en el Sistema.
- Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.
- Implantar y controlar las medidas específicas de seguridad del Sistema y cerciorarse de que éstas se integren adecuadamente dentro del marco general de seguridad.
- Ejecutar los planes mejora de la seguridad aprobados por el Comité de Seguridad TIC.
- Asesorar en la definición de la topología y sistema de gestión de los Sistemas de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Llevar a cabo el preceptivo proceso de análisis y gestión de riesgos en el Sistema y asesorar en colaboración con el RSEG, a los RI y a los RSER, en el proceso de la gestión de riesgos.
- 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 y aprobar la documentación de seguridad del Sistema.
- Delimitar las responsabilidades de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del Sistema.
- Velar por el cumplimiento de las obligaciones del Administrador de Seguridad del Sistema (ASS).
- Investigar los incidentes de seguridad que afecten al Sistema, y en su caso, comunicación al Responsable de Seguridad o a quién éste determine.
- Suspender el 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 el RI de la información afectada, el RSER del servicio afectado y el RSEG, antes de ser ejecutada.
- Elaborar los procedimientos operativos de seguridad y ponerlos a disposición del RSEG para su aprobación.
- Planificar la implantación de salvaguardas en el sistema.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el

personal se familiarice con ellos.

- Elaborar los planes de continuidad y ponerlos a disposición del RSEG para su validación.
- Elaborar las definiciones del ciclo de vida de los sistemas: especificación, arquitectura, desarrollo, operación y cambios, para que el RSEG los apruebe.

9.10. ADMINISTRADOR DE SEGURIDAD DEL SISTEMA (ASS)

El ASS dependerá jerárquica y funcionalmente del Responsable del Sistema. La persona designada figurará en la documentación de seguridad del Sistema de Información

Sus funciones son las siguientes:

- La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información.
- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información.
- La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- La aplicación de los Procedimientos Operativos de Seguridad.
- Aprobar los cambios en la configuración vigente del Sistema de Información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.
- Informar al RSEG y al RSIS de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución. Ante incidentes de seguridad de la información:
    - Llevará a cabo el registro, contabilidad y gestión de los incidentes de seguridad en los Sistemas bajo su responsabilidad.
    - Aislará el incidente parapara evitar la propagación a elementos ajenos a la situación de riesgo.
    - Tomará decisiones a corto plazo si la información se ha visto comprometida de tal forma que pudiera tener consecuencias graves. Estas actuaciones deberán estar procedimentadas para reducir el margen de discrecionalidad del ASS al mínimo número de casos.
    - Asegurará la integridad de los elementos críticos del Sistema si se ha visto afectada la disponibilidad de los mismos. Estas actuaciones deberán estar procedimentadas para reducir el

margen de discrecionalidad del ASS al mínimo número de casos.

- Mantendrá y recuperará la información almacenada por el Sistema y sus servicios asociados.
- Investigará el incidente, determinando el modo, los medios, los motivos y el origen del incidente.

El ASS será designado por la Dirección General a la que pertenece el CICA, a propuesta del RSIS.

El ASS reportará al RSIS:

- Sobre la implantación de las medidas de seguridad.
- Sobre la supervisión de las medidas de seguridad.

El ASS reportará al RSEG:

- Sobre la gestión de las autorizaciones.
- Sobre el estado de seguridad del Sistema.

10. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del Comité de Seguridad TIC la revisión anual de esta PSTIC y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por la persona titular de la Dirección General a la que se adscribe el CICA y difundida para que la conozcan todas las partes afectadas.

11. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política se desarrollará por medio de normativa de seguridad y procedimientos operativos de seguridad que afronten aspectos específicos.

El cuerpo normativo sobre seguridad de la información se desarrollará en cuatro niveles con diferente ámbito de aplicación, nivel de detalle técnico y obligatoriedad de cumplimiento, de manera que cada norma de un determinado nivel de desarrollo se fundamente en las normas de nivel superior. Todos estos niveles prestarán especial atención a las exigencias derivadas del Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, así como a la normativa aplicable en materia de protección de datos de carácter personal.

Dichos niveles de desarrollo normativo son los siguientes:

a) Primer nivel: constituido por la presente PSTIC y las directrices generales de seguridad aplicables a los órganos superiores o directivos del CICA a los que sea de aplicación la presente PSTIC. Es de obligado cumplimiento en todo el CICA.

b) Segundo nivel: constituido por las normas de seguridad que desarrollan la presente PSTIC y describen de forma general los principios y normas de seguridad que serán concretados en los niveles posteriores. Son de obligado cumplimiento en todo el CICA y deben ser aprobadas por el CSTIC.

c) Tercer nivel: constituido por procedimientos, guías e instrucciones técnicas. Son documentos que, cumpliendo con lo expuesto en la PSTIC, determinan las acciones o tareas a realizar en el desempeño de un proceso. Dependen de las normas de seguridad y los aprueba la persona titular de la Dirección del CICA.

d) Cuarto nivel: Documentación técnica. En este último nivel se incluye todo tipo de documentación técnica o especializada que se considere necesario para completar y facilitar el desarrollo de las medidas de seguridad. La aprueba la persona titular de la Jefatura de Informática.

El Comité de Seguridad TIC establecerá los mecanismos necesarios para compartir la documentación derivada del desarrollo con el propósito de regularizarlo, en la medida de lo posible, en todo el ámbito de aplicación de la política de seguridad TIC.

La siguiente tabla resume el marco de desarrollo y la competencia para su aprobación:

Nivel	Documento	Aprueba
Primero	Política de seguridad	Persona titular de la Dirección General en la que se enmarca el CICA.
Segundo	Normas de seguridad	Comité de Seguridad TIC
Tercero	Procedimientos	Persona titular de la Dirección del CICA
Cuarto	Documentación técnica	Persona titular de la Jefatura de Informática

El RSEG se encarga de la gestión de los documentos indicados, debiendo asegurar que ésta sea completa y proporcione información suficiente para definir las necesidades de protección de la información y los activos asociados a la misma en el ámbito del CICA.

La normativa de seguridad, los procedimientos, las guías y las instrucciones técncias estarán a disposición de todos los miembros de la organización que necesiten conocerlos, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

La normativa de seguridad estará disponible en la intranet: https://www.cica.es/politica-de-seguridad/.

12. OBLIGACIONES DEL PERSONAL

Todos los miembros del CICA tienen la obligación de conocer y cumplir esta PSTIC y la Normativa de Seguridad, siendo responsabilidad del CSTIC disponer los medios necesarios para que la información llegue a las personas afectadas.

Todo el personal que se incorpore al CICA o vaya a tener acceso a alguno de sus sistemas de información o la información gestionada por ellos deberá ser informado de la PSTIC.

Todos los miembros del CICA atenderán 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 del CICA, 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 personal del CICA deberá cumplir además con las instrucciones y normas que regulen el comportamiento del personal empleado público en el uso de los sistemas informáticos y redes de comunicaciones de la

Administración de la Junta de Andalucía.

Cualquier persona que actúe bajo la autoridad del Responsable o del Encargado de un Tratamiento de datos personales en el ámbito de aplicación de esta Política de Seguridad y tenga acceso a datos personales solo tratará dichos datos siguiendo instrucciones del Responsable, salvo que se lo impida el ordenamiento jurídico comunitario, nacional o autonómico.

13. TERCERAS PARTES

Debido a la naturaleza de los servicios que presta el CICA, el centro maneja información de otros organismos, por lo que se les hará partícipes de esta PSTIC, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando el CICA utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta PSTIC 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 RSEG 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.

14. GESTIÓN DE RIESGOS

La gestión de riesgos deberá realizarse de manera continua sobre el sistema de información, conforme a los principios de gestión de la seguridad basada en los riesgos y de reevaluación periódica de los mismos.

Las personas encargadas de la categorización de los sistemas serán los Responsables de la Información y de los Servicios, siendo el RSEG el encargado de supervisar los análisis de riesgos y proponer las medidas de seguridad a aplicar.

Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos de carácter personal, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, así como la comunicación o acceso no autorizados a dichos datos.

Los Responsables de la Información y de los Servicios son los responsables de aceptar los riesgos residuales calculados en el análisis sobre la información y los servicios, respectivamente, y de realizar su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

El proceso de gestión de riesgos, que comprende las fases de categorización de los sistemas, análisis de riesgos y selección de medidas de seguridad a aplicar, que deberán ser proporcionales a los riesgos y estar justificadas, deberá revisarse al menos con periodicidad anual por parte del RSEG, que elevará un informe al Comité de Seguridad TIC.

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 CSTIC establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El CSTIC dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

15. CLASIFICACIÓN Y CONTROL DE ACTIVOS

Los recursos informáticos y la información del CICA se encontrarán inventariados, con una persona responsable asociada y, en caso de ser necesario, una persona responsable de la custodia de los mismos. Los inventarios se mantendrán actualizados para asegurar su validez, revisándose exhaustivamente al menos una vez al año.

Los activos de información estarán clasificados de acuerdo a su sensibilidad y criticidad para el desarrollo de la actividad del CICA, se establecerán las medidas de seguridad exigidas para su protección en función de dicha clasificación.

16. AUDITORÍAS DE SEGURIDAD

Los sistemas de información serán objeto de una auditoría regular ordinaria, al menos cada dos años, que verifique el cumplimiento de los requerimientos del ENS. Estas auditorías ordinarias así como las extraordinarias se harán de acuerdo con lo establecido en el art. 34 del Real Decreto 3/2010, de 8 de enero, y la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información, aprobada por Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública.

Los informes de auditoría serán presentados a la persona Responsable del Sistema competente, al Delegado de Protección de Datos, si afectara a estos, y a la persona Responsable de Seguridad TIC. Estos informes serán analizados por esta última persona que presentará sus conclusiones a la persona Responsable del Sistema para que adopte las medidas correctoras adecuadas. Los resultados obtenidos determinarán las líneas de actuación a seguir y las posibles modificaciones a realizar sobre los controles y la normativa de seguridad.

Con el fin de optimizar la utilización de los recursos públicos y garantizar una mejor coordinación entre seguridad TIC y seguridad de protección de datos, siempre que sea posible, se realizarán de manera conjunta las auditorías de seguridad de sistemas de información y las auditorías de protección de datos o medidas análogas de verificación, evaluación y valoración de seguridad de los tratamientos.

17. NOTIFICACIONES DE VIOLACIONES DE SEGURIDAD

Es de carácter obligatorio para todo el personal empleado, contratista o usuarios terceros del CICA, la

notificación inmediata de cualquier problema o violación de la seguridad; esta notificación debe realizarse por escrito vía correo electrónico a la dirección cica-cert@cica.es.

Está fundamentado como una exigencia que el personal del CICA conozca sus responsabilidades, sanciones y medidas a tomar al momento de incurrir en alguna violación o falta, escrita en las Políticas de Seguridad. Por esta razón se apoyará la concienciación para obtener la colaboración de los empleados, haciéndoles conscientes de los riesgos que se pueden correr y de la importancia del cumplimiento de las normas.

18. DATOS DE CARÁCTER PERSONAL

El CICA 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 del CICA se ajustarán a lo exigido por el Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, por el que se aprueba el Reglamento General de Protección de Datos, en adelante RGPD, y el resto de la normativa general o sectorial de protección de datos de carácter personal que sea de aplicación. Todos los tratamientos de datos de carácter personal, automatizados o no automatizados, se someterán a la citada norma cuando se encuentren dentro de su ámbito de aplicación.

En dicho ámbito cada Responsable del Tratamiento de datos de carácter personal aplicará las medidas técnicas y organizativas apropiadas a fin de garantizar y ser capaz de demostrar que los tratamientos de datos de carácter personal son conformes con dicha normativa, de acuerdo con el principio de responsabilidad proactiva, de conformidad con el artículo 24 del RGPD. En caso de conflicto con la normativa de seguridad, prevalecerá el criterio que presente un mayor nivel de exigencia respecto a la protección de los datos de carácter personal.

Teniendo en cuenta el estado de la tecnología, los costes de aplicación y la naturaleza, el alcance, el contexto y los fines del tratamiento de datos de carácter personal, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, y de conformidad con el artículo 32 del RGPD, el Responsable y el Encargado del Tratamiento en el ámbito de aplicación de esta Orden, aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) La seudonimización y el cifrado de datos personales.

b) La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

c) La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.

d) Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Cuando sea probable que un tipo de tratamiento de datos personal, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el Responsable del Tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales, de conformidad con el artículo 32 del RGPD. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares. Para ello recabará el asesoramiento del Delegado de Protección de Datos.

El Responsable del Tratamiento llevará un registro de las actividades de tratamiento de datos de carácter personal efectuadas bajo su responsabilidad, de acuerdo con lo establecido en el artículo 35 del RGPD y el resto de normativa de datos de carácter personal aplicable. Cada Encargado del Tratamiento llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un Responsable, de acuerdo con el mismo precepto.

En caso de violación de la seguridad de los datos personales, el Responsable del Tratamiento la notificará a la autoridad de control competente sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el Responsable del Tratamiento la comunicará al interesado sin dilación indebida. Dicha notificación y comunicación se atendrán a lo establecido en los artículos 33 y 34 del RGPD y el resto de normativa de datos de carácter personal aplicable.

La notificación a la autoridad de control a la que se refiere el apartado anterior podrá realizarse a través de AndalucíaCERT y otros CERT de ámbito nacional con los que se relacione el CICA, siempre que se cumplan los requisitos del RGPD, en los casos en los que así lo disponga de la política de seguridad de las tecnologías de la información y comunicaciones de la Junta de Andalucía.

18.1. RESPONSABLES DE LOS TRATAMIENTOS DE DATOS DE CARÁCTER PERSONAL

- Los Responsables de los Tratamientos de datos de carácter personal en el ámbito de aplicación de esta PSTIC son las personas u organismos que determinen los fines y medios de los tratamientos, de conformidad con el artículo 4.7 del RGPD.
- En el ámbito de la política de seguridad TIC del CICA, los Responsables de la Información, tendrán la condición de Responsables del Tratamiento respecto a los tratamientos sobre los que determinen sus fines y medios, salvo que las normas aplicables sobre asignación de atribuciones en materia de protección de datos de carácter personal dispongan otra cosa.

18.2. ENCARGADOS DE LOS TRATAMIENTOS DE DATOS DE CARÁCTER PERSONAL

- Si los Responsables de los Tratamientos designaran a un Encargado del Tratamiento lo harán únicamente por cada tratamiento a un Encargado de Tratamiento que ofrezca garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas para que el tratamiento sea conforme al RGPD y garantice la protección de los derechos de las personas interesadas, de conformidad con el artículo 28 del RGPD.
- Las principales funciones y responsabilidades, dentro de su ámbito de actuación, son las establecidas en el artículo 28 del RGPD y demás normativa de aplicación.
- Tanto el Responsable como el Encargado del Tratamiento deberá determinar claramente cuándo el tratamiento se realiza bajo su autoridad, conforme a lo establecido en el artículo 29 del RGPD y cuándo se realiza mediante un Encargado de Tratamiento sujeto a lo establecido en el artículo 28 de

dicho RGPD.

18.3. DELEGADO DE PROTECCIÓN DE DATOS

- Existirá una persona que ostente la condición de Delegado de Protección de Datos a efectos de lo establecido en los artículos 37 y 38 del RGPD.
- La persona que ostente la condición de Delegado de Protección de Datos será designada por la persona titular de Dirección General a la que se encuentra adscrita el CICA, entre personal funcionario de éste, no pudiendo ser removida ni sancionada por desempeñar sus funciones, salvo que incurriera en dolo o negligencia grave en su ejercicio.
- La persona que ostente la condición de Delegado de Protección de Datos podrá poner en conocimiento del Comité de Seguridad TIC las cuestiones relacionadas con la protección de datos que sea necesario y participará, desde el inicio, en todas las cuestiones relacionadas con la protección de datos, contribuyendo así al cumplimiento de la protección de datos de carácter personal desde el diseño y por defecto.
- Son funciones de la persona que ostente la condición de Delegado de Protección de Datos, entre las demás que le corresponden de conformidad con el artículo 39 del RGPD y demás normativa de aplicación, las siguientes:

  a) Ser consultado sobre la contratación, análisis, diseño, operación y mantenimiento de los tratamientos realizados sobre datos de carácter personal. También debe ser consultado sobre todo proyecto normativo que suponga un tratamiento de datos de carácter personal.

  b) Asesorar sobre la confección de los modelos de formularios de recogida de datos de carácter personal.

  c) Asesorar sobre la evaluación de impacto relativa a la protección de datos, tanto en la necesidad de su realización como en su elaboración.

  d) Supervisar la gestión del registro de actividades de tratamiento de los Responsables de Tratamiento del CICA, debiendo éstos facilitarle la información necesaria para ello.

  e) Asesorar a los Responsables de los Tratamientos sobre la oportunidad y modo de notificar los incidentes de seguridad sobre datos de carácter personal a la autoridad de control correspondiente en materia de protección de datos de carácter personal.

  f) Asesorar a los Responsables de los Tratamientos sobre la oportunidad y modo de informar a las personas interesadas y afectadas por violaciones de la seguridad de sus datos de carácter personal que entrañen un alto riesgo para los derechos y libertades de las personas físicas, conforme a lo establecido en el artículo 34 del RGPD.