ANEXO I

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Historial de Versiones

Versión	Fecha	Autor	Observaciones
1.0	08/06/2018	Servicio de Sistemas de Información	Versión inicial
1.1	21/12/2022	Servicio de Sistemas de Información	Modificación de roles

1 INTRODUCCIÓN

La Agencia Valenciana de Prevención y Lucha contra el Fraude y la Corrupción de la Comunitat Valenciana (en adelante, la Agencia) utiliza sistemas automatizados de tratamiento de información y de comunicaciones para el cumplimiento de sus fines. Estos sistemas deben ser utilizados y administrados con diligencia, y se deben tomar las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la integridad o confidencialidad de la información tratada o a la disponibilidad de los servicios.

El objetivo de la presente política de seguridad de la información es el de establecer los mecanismos básicos que garanticen la calidad de la información y la prestación continuada de los servicios mediante la adopción de acciones preventivas, la supervisión continuada de la actividad y la respuesta ágil a los incidentes que se puedan producir.

Las medidas mínimas de seguridad exigidas por el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, deben aplicarse y cumplirse, y el personal de la Agencia debe asumir que la seguridad de la información es una parte integral de la gestión cotidiana y de los sistemas que la soportan y que, en consecuencia, debe tomarse en consideración desde su concepción y durante todo su ciclo de vida. La protección de la información y la prevención, respuesta, reacción ante cualquier incidente y la recuperación de los sistemas deben formar parte de las obligaciones de todo el personal de la Agencia en sus respectivos ámbitos de responsabilidad.

Los requisitos de seguridad y los recursos necesarios para satisfacerlos deben ser identificados e incluidos en la planificación de los sistemas y en los procedimientos de contratación de soluciones tecnológicas que comporten tratamiento de información.

2 PREVENCIÓN

El personal al servicio de la Agencia 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 es necesario conocer y observar las medidas mínimas de seguridad determinadas por el Esquema Nacional de Seguridad, así como establecer los controles adicionales que resulten aconsejables después de llevar a cabo la correspondiente 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 esta política, el personal debe recabar las autorizaciones oportunas para la puesta en producción de cualquier sistema, evaluar regularmente la seguridad, llevar a cabo revisiones de los cambios de configuración realizados de forma rutinaria y solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente del estado de la seguridad.

2.1 Detección

El estado de los servicios basados en el uso de tecnologías de la información y de las comunicaciones (en adelante, servicios TIC) debe ser monitorizado de manera continua con el fin de detectar anomalías en sus niveles de calidad, según lo establecido en el artículo 8 del Esquema Nacional de Seguridad.

Es necesario establecer mecanismos de detección y análisis de incidentes relacionados con la seguridad de la información, así como canales que permitan su supervisión por parte de la dirección, de forma regular y, especialmente, cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

2.2 Respuesta

La Agencia debe dotarse de mecanismos para garantizar una respuesta adecuada ante cualquier situación anómala o incidente de seguridad detectado. Para ello, desarrollará mecanismos adecuados para la notificación de los incidentes y el intercambio de información relacionada con los equipos de respuesta a incidentes de ámbito autonómico (CSIRT-GV1) y estatal (CCN-CERT2).

2.3 Recuperación

Para garantizar la disponibilidad de los servicios críticos, la Agencia debe desarrollar planes de continuidad y de recuperación de los sistemas TIC, como parte de su plan general de continuidad del servicio. Estos planes deben estar permanentemente actualizados y su eficacia debe ser verificada mediante pruebas periódicas.

3 ALCANCE

Esta política es de aplicación a todos los sistemas TIC de la Agencia y a todo su personal. En los contratos que se suscriban con terceros, se establecerá la obligación de cumplir con esta política por parte del contratista y de su personal, si la misma fuera de aplicación.

4 MISIÓN

La Agencia se crea para prevenir y erradicar el fraude y la corrupción de las instituciones públicas valencianas y para el impulso de la integridad y la ética pública, así como para el fomento de una cultura de buenas prácticas y de rechazo del fraude y la corrupción en el diseño, ejecución y evaluación de políticas públicas y en la gestión de recursos públicos.

Tanto para el cumplimiento de sus fines específicos, como para su funcionamiento como entidad de derecho público, la Agencia hace uso de información y de sistemas automatizados para su tratamiento, que deben ser convenientemente protegidos, supervisados y auditados.

[1]CSIRT-CV (https://www.csirtcv.gva.es/) es el Centro de Seguridad TIC de la Comunitat Valenciana. Actualmente CSIRT-CV está adscrito a la Dirección General de Tecnologías de la Información y las Comunicaciones dentro de la Conselleria de Hacienda y Modelo Económico.

5 MARCO NORMATIVO

En el apartado correspondiente del Sistema de Gestión de la Seguridad de la Información, se mantendrá un listado de disposiciones normativas a las que está sujeta la Agencia y que guardan, en mayor o menor medida, relación con la seguridad de la información.

El mencionado listado se mantendrá actualizado y será objeto de revisión anual por parte de la dirección de Asuntos Jurídicos de la Agencia.

6 DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Para el desarrollo de la presente Política, la Agencia se dotará de una serie de instrumentos que permitan abordar los diferentes aspectos de la seguridad de la información. Con ello se trata de dar concreción a la concepción abstracta de la seguridad que supone la política y llevarla al terreno de su aplicación práctica. Estos elementos son los que se relacionan a continuación.

6.1 Análisis de riesgos

El artículo 7 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, establece que el análisis y la gestión de los riesgos son partes esenciales del proceso de seguridad y deben mantenerse permanentemente actualizados.

La gestión de riesgos debe permitir el mantenimiento de un entorno controlado, que minimice el riesgo hasta un nivel aceptable y que involucre a la dirección de las diferentes unidades administrativas de la Agencia en la aceptación de un determinado riesgo residual.

El análisis y la gestión de los riegos se llevarán a cabo mediante herramientas y metodologías comúnmente aceptadas por las administraciones públicas y tomando como referencia las guías y directrices que publiquen el CCN-CERT o el CSIRT-CV.

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.
- Excepcionalmente:
    - Cuando cambie significativamente la información manejada, en lo que haga referencia a esa información.
    - Cuando cambien significativamente los servicios prestados, en lo que afecte a los sistemas nuevos o modificados.
    - Cuando ocurra un incidente grave de seguridad.
    - Cuando se reporten vulnerabilidades graves.

El análisis y la gestión de riesgos deben estar presentes en todas las fases del ciclo de vida de los sistemas. La selección y la aplicación de los controles de seguridad, así como la evaluación de su eficiencia, deben tomarse en consideración durante el diseño, implantación, contratación, adquisición y explotación de los sistemas y servicios de la Agencia, siendo objeto de especial atención la finalización de estos y el destino de la información que traten.

La Agencia valorará especialmente, en los procesos de contratación, las empresas, productos y servicios que puedan acreditar un determinado nivel de seguridad o que dispongan de las certificaciones de seguridad pertinentes.

6.2 Clasificación de la información

Los activos de información que trate la Agencia deben estar inventariados y clasificados. El nivel de protección y las medidas de seguridad que se aplicarán a la información deben basarse en su clasificación y los mecanismos y criterios para llevarla a cabo deben ser formalmente aprobados y conocidos por todo el personal.

6.3 Planificación y coordinación

Con carácter anual, la Agencia definirá un conjunto de objetivos de seguridad que deben incluir una descripción de la línea o líneas de actuación previstas, los proyectos en los que se concretan, los objetivos a alcanzar y los indicadores de cumplimiento y progreso correspondientes. Estos objetivos deben tomar en consideración los resultados de las auditorías y del análisis de riesgos.

El esquema organizativo de la seguridad de la información incluye los órganos de coordinación y decisión necesarios para la aplicación y control de las medidas de seguridad.

6.4 Acceso a la información

El personal que trate información a través de los sistemas de la Agencia debe estar debidamente acreditado e identificado mediante credenciales electrónicas personales e intransferibles.

Los privilegios de acceso a la información deben limitarse a los estrictamente imprescindibles para el desarrollo de las funciones de cada puesto de trabajo.

6.5 Registros de actividad

Las actuaciones del personal sobre los sistemas podrán ser registradas en aplicación de las exigencias legales de trazabilidad o con el fin de verificar el cumplimiento de esta política. Ese registro conllevará la retención de información para su monitorización, análisis, investigación y documentación.

Los accesos a la información que implican modificaciones de esta o que suponen el acceso a datos especialmente sensibles deben quedar registrados con el nivel de detalle suficiente para garantizar el cumplimiento normativo y la trazabilidad de las acciones efectuadas.

6.6 Uso de los sistemas y medios electrónicos

Con carácter general, la Agencia no permite la utilización de los medios electrónicos corporativos para uso personal. Esta prohibición no será de aplicación en aquellos casos en los que el servicio sea diseñado específicamente con el fin de permitir el uso de dispositivos personales o en aquellos otros en los que el uso personal del servicio sea autorizado de forma explícita. Esta autorización únicamente podrá concederse si el servicio afectado no permite el tratamiento de información sensible de la Agencia.

6.7 Confidencialidad y deber de secreto

Aquellas personas al servicio de la Agencia que traten información que no tenga el carácter de pública han de observar la necesaria reserva, confidencialidad y sigilo. Esta obligación perdura después de haber finalizado el vínculo con la Agencia.

Este compromiso debe hacerse constar, de forma individual y por escrito, mediante una declaración responsable de confidencialidad.

6.8 Instalaciones y equipamiento

Los sistemas y las infraestructuras informáticas y de comunicaciones que no formen parte de los puestos de trabajo deben ubicarse en zonas aisladas, de acceso restringido y suficientemente protegidas.

6.9 Sistemas de información

Los sistemas de información de la Agencia deben proporcionar la funcionalidad estrictamente necesaria para cumplir la finalidad que haya motivado su diseño o adquisición. Esta finalidad debe estar documentada y formalmente aprobada por sus responsables.

Los responsables de las distintas unidades administrativas de la Agencia son responsables de los sistemas de información que dan soporte a los procesos que desarrollan. En el caso de sistemas comunes, esta responsabilidad la ejercerá la dirección.

Las funciones de operación, administración, mantenimiento y registro de actividad deben estar documentadas y sujetas a control.

6.10 Protección de la información no automatizada

La información de la Agencia en soporte no electrónico debe ser protegida con el mismo nivel de seguridad que la que haya sido sometida a tratamiento automatizado.

Los documentos deberán almacenarse en una ubicación adecuada, evitando su cercanía a sistemas de refrigeración, canalizaciones de agua o instalaciones que puedan afectar al papel.

Se guardarán en los armarios o cajoneras y se evitará la acumulación de documentos sobre las mesas que pueda causar pérdidas o filtraciones de información.

La documentación desechada debe destruirse de manera segura. En el caso de que el volumen de documentación a destruir sea elevado, puede resultar aconsejable contratar la retirada y destrucción a un proveedor externo. En este caso, los contratos establecerán las cláusulas de confidencialidad pertinentes y la obligación de proporcionar certificados de destrucción segura.

6.11 Sistema de Gestión de la Seguridad de la Información

La planificación, organización y control de los recursos relativos a la seguridad de la información requiere ser abordada de forma sistemática y documentada. El conjunto de procedimientos, normas y guías de seguridad que se desarrollen deberá ser integrado en un Sistema de Gestión de la Seguridad de la Información (en adelante, SGSI), que sea periódicamente revisado, verificado mediante auditorías y adaptado a las necesidades de la Agencia y a los requisitos legales vigentes

en cada momento. El SGSI de la Agencia estará orientado a dar cumplimiento a lo previsto en el Esquema Nacional de Seguridad e incluirá los documentos siguientes:

- Declaración de aplicabilidad de las medidas previstas en el Anexo II del Esquema Nacional de Seguridad.
- Lista de activos de información y sistemas con su valoración correspondiente en función de las diferentes dimensiones de la seguridad.
- Procedimientos de seguridad, con indicaciones concretas sobre la forma de manejar la información y de actuar sobre los sistemas, y que deben describir cómo dar cumplimiento a lo previsto en el Esquema Nacional de Seguridad.
- Normas de seguridad, que regularán el uso correcto y las responsabilidades de los usuarios y que tendrán carácter obligatorio.

El sistema de gestión de la seguridad de la información debe estar sometido a monitorización, control y mejora continuos para mantener su eficacia ante la constante evolución de las amenazas y de los sistemas técnicos de protección.

6.12 Guías de seguridad

Las guías de seguridad deben tener un carácter formativo y estarán orientadas a instruir y orientar a los usuarios en la correcta aplicación de las medidas de seguridad para las que no existan procedimientos concretos. Dichas guías de seguridad se podrán a disposición del personal de modo que resulte sencillo su acceso y se promueva su conocimiento y aplicación, tanto si son de origen interno, como si han sido elaboradas por organismos externos a la Agencia.

6.13 Especiales requisitos de seguridad de los activos de la Agencia

La Agencia, para el cumplimiento de sus fines, trata informaciones diversas y cuenta con sistemas para llevar a cabo esos tratamientos. Los activos de información y los sistemas constituyen el objeto de protección de esta política, debiendo aplicarse las medidas que corresponda en función de su criticidad y de lo que se prevea en cada momento en la normativa vigente.

La seguridad de la información se aborda desde cinco dimensiones diferentes:

- La confidencialidad, que toma en consideración las consecuencias que tendría la revelación de información a personas no autorizadas o que no necesitan conocerla.
- La integridad, que considera el impacto que podría tener la modificación malintencionada o involuntaria de la información.
- La autenticidad, que valora las consecuencias derivadas de que la información no fuera auténtica.
- La trazabilidad, que se plantea los problemas que supondría el hecho de no poder verificar los accesos o modificaciones llevados a cabo sobre una cierta información.
- La disponibilidad, que considera las consecuencias que tendría para la que una persona o un sistema interconectado no pudiera acceder a un sistema dentro del periodo de servicio establecido y anunciado por la Agencia.

Con carácter general, la Agencia valorará, conforme a los criterios establecidos en el Esquema Nacional de Seguridad, la disponibilidad de los sistemas y la integridad, confidencialidad, autenticidad y trazabilidad de la información.

La Agencia valora el Buzón de Denuncias y la información relacionada con denuncias y expedientes de investigación como activos a los que debe aplicarse la máxima protección, siendo especialmente relevante la confidencialidad de esta información que afecte a personas físicas.

7 ORGANIZACIÓN DE LA SEGURIDAD

El Esquema Nacional de Seguridad prevé que en los sistemas de información de las administraciones públicas existan tres roles diferenciados:

- El responsable de la información, que determinará los requisitos de la información tratada.
- El responsable del servicio, que determinará los requisitos de los servicios prestados.
- El responsable de seguridad, que tomará 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 debe estar diferenciada de la responsabilidad sobre la prestación de los servicios y la Política de Seguridad de la Agencia es la que debe detallar las atribuciones de cada responsable y los mecanismos de coordinación y de resolución de conflictos.

Dada la dimensión de la Agencia, los roles de responsable de la información y de responsable del servicio, al igual que el de responsable de seguridad, serán asumidos por la dirección. Esta configuración corresponde a la estructura mínima contemplada en el Anexo C de la Guía CCN-STIC-8012, que establece recomendaciones sobre las responsabilidades derivadas de la aplicación del Esquema Nacional de Seguridad.

Con el fin de garantizar una cierta independencia a nivel de operación entre la función de seguridad y la de prestación del servicio, se designan dos personas administradoras de seguridad, una de ellas encargada del aseguramiento de la prestación del servicio y otra encargada de la protección de la información, que rendirán cuentas en materia de seguridad al Comité de Seguridad de la Información.

7.1 Funciones y responsabilidades de la dirección

Son funciones de la dirección de la Agencia, en relación con la seguridad de la información, las siguientes:

a) Asumir la responsabilidad última del uso que se haga de la información, así como de la disponibilidad, accesibilidad e interoperabilidad de los servicios.
b) Asumir la responsabilidad última de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad de la información, o bien de disponibilidad del servicio.
c) Determinar, junto con el Comité de Seguridad de la Información y previo informe de las personas administradoras de la seguridad, los niveles de seguridad de la información y la categoría de los servicios.
d) Con la asistencia del Comité de Seguridad de la Información y de las personas administradoras de la seguridad, mantener la seguridad de la información manejada por la

[2]La guía "CCN-STIC-801 Responsabilidades y Funciones en el ENS" establece unas pautas de carácter general que son aplicables a entidades de distinta naturaleza, dimensión y sensibilidad. El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones por parte de Centro Criptológico Nacional para facilitar un mejor cumplimiento de dichos requisitos mínimos por parte de las diferentes administraciones.

Agencia y de los servicios prestados por los sistemas de información, así como promover la formación y concienciación del personal al servicio de la Agencia en materia de seguridad de la información.

7.2 Funciones de la persona responsable del sistema

La función de responsable del sistema (RSIS) la ejercerá la persona que ocupe la Jefatura del Servicio de Sistemas de Información (puesto 9). El responsable del sistema podrá delegar determinadas funciones en los administradores de seguridad. Estas delegaciones, que se harán en función de criterios técnicos, se deben hacer constar en los procedimientos del Sistema de Gestión de la Seguridad de la Información.

Las funciones del responsable del sistema son las siguientes:

a) Informar y rendir cuentas a la dirección y al Comité de Seguridad de la Información en materia de seguridad de los sistemas y equipos de la Agencia.
b) Valorar los resultados del análisis de riesgos y proponer la toma de decisiones sobre la manera de tratarlos.
c) Asumir la responsabilidad técnica sobre la prestación de los servicios basados en los sistemas de la información de la Agencia.
d) Supervisar el desarrollo, operación y mantenimiento de los sistemas durante todo su ciclo de vida.
e) Definir los principios de gestión de cada sistema y establecer las políticas de uso y los servicios disponibles.
f) Asegurarse de que las medidas generales y políticas de seguridad están integradas en los sistemas.
g) Tomar decisiones urgentes en materia de suspensión o interrupción temporal del servicio, si se detectan deficiencias graves de seguridad.
h) Velar por la elaboración y aprobación de los procedimientos operativos de seguridad.
i) Proponer planes y objetivos de mejora de la seguridad.
j) Promover la formación del personal a su cargo en materia de seguridad.
k) Elaborar planes de continuidad que garanticen la prestación del servicio en caso de incidencias.
l) Gestionar los acuerdos de nivel de servicio.
m) Velar por la seguridad física de las instalaciones en las que se ubiquen los sistemas de tratamiento de información, en coordinación con el área de Administración, y de la gestión del personal a su cargo.

7.3 Funciones y responsabilidades de la administración de seguridad de los sistemas

La administración de seguridad de los sistemas (ASS) la ejercerá la persona que ocupe la Jefatura de Unidad de Producción y Explotación de los Sistemas Informáticos (puesto 19) y tendrá encomendadas las funciones de seguridad orientadas al aseguramiento de la prestación del servicio y los medios de tratamiento de la información. Estas funciones se concretan en las siguientes:

a) Asumir, en coordinación con el responsable del sistema, la responsabilidad del diseño, implantación y control de las medidas técnicas de seguridad en cada sistema y aplicar los procedimientos operativos.
b) Llevar a cabo la gestión, configuración y actualización del hardware y software en el que se basan los mecanismos de seguridad de los sistemas.
c) Gestionar las autorizaciones de uso y perfiles de acceso a los sistemas.
d) Elaborar los planes de recuperación de sistemas.
e) Monitorizar continuamente el estado de seguridad de los sistemas.

f) Registrar los incidentes de seguridad e informar periódicamente al Comité de Seguridad de la Información.
g) Informar periódicamente al Comité de Seguridad de la Información.
h) Ejercer las funciones delegadas por el responsable del sistema o por la dirección en su ámbito de competencia.
i) Colaborar en la resolución e investigación de incidentes de seguridad.

7.4 Funciones y responsabilidades de la administración de seguridad de la información

La administración de seguridad de la información (ASI) la ejercerá la persona que ocupe la Jefatura de Unidad de Coordinación Informática (puesto 18) y tendrá encomendadas las funciones de seguridad orientadas a la protección de la información. Estas funciones se concretan en las siguientes:

a) Mantener y administrar el Sistema de Gestión de la Seguridad de la Información.
b) Coordinar la elaboración de políticas, normas y guías de seguridad.
c) Llevar a cabo el análisis de los riesgos que afrontan los sistemas de tratamiento de la información y proponer acciones para su tratamiento al Comité de Seguridad de la Información.
d) Proponer al Comité de Seguridad de la Información la categorización de los activos de la Agencia y la aplicabilidad de las medidas de protección contempladas en el Esquema Nacional de Seguridad.
e) Coordinar la realización periódica de auditorías de seguridad y de conformidad con el Esquema Nacional de Seguridad.
f) Monitorizar el cumplimiento estricto de los controles de seguridad.
g) Registrar los incidentes de seguridad, notificarlos a las autoridades de control, en su caso, y llevar a cabo su seguimiento hasta la completa resolución de estos.
h) Informar periódicamente al Comité de Seguridad de la Información.
i) Ejercer las funciones delegadas por el responsable del sistema o por la dirección en su ámbito de competencia.
j) Colaborar en la resolución e investigación de incidentes de seguridad.

7.5 El Comité de Seguridad de la Información

El Comité de Seguridad de la Información (CSI) tiene la función de asesorar a la dirección de la Agencia en la toma de decisiones relacionadas con la seguridad de la información.

7.5.1 Composición

El Comité de Seguridad de la Información está integrado por:
a) La persona que ocupe la dirección de la Agencia, que actuará como presidente.
b) Las personas que ocupen las direcciones de las diferentes unidades administrativas de la Agencia:
    - Análisis e Investigación.
    - Prevención, Formación y Documentación.
    - Asuntos Jurídicos.
    - Gabinete de Relaciones Institucionales, Comunicación y Participación.
    - Administración, Recursos Humanos y Gestión Económica.
c) El responsable del sistema.
d) El administrador de seguridad de sistemas.
e) El administrador de seguridad de la información, que actuará como secretario.

7.5.2 Funciones

Son funciones del Comité de Seguridad de la Información las que a continuación se enumeran:

a) Planificar las auditorías necesarias para garantizar el cumplimiento de la legalidad vigente y el ciclo de vida del sistema de gestión de la seguridad de la información.
b) Analizar los riesgos que afronta la Agencia y tomar decisiones ejecutivas sobre el modo de gestionarlos y el nivel de riesgo residual que resulta aceptable.
c) Fijar objetivos de seguridad y planificar y dotar de recursos su ejecución.
d) Velar por que se establezcan mecanismos de continuidad de las actividades ante incidentes de seguridad.
e) Supervisar la eficacia de las medidas de seguridad establecidas para proteger la información y garantizar la disponibilidad y correcto funcionamiento de los servicios prestados por los sistemas de información.
f) Dirigir la estrategia corporativa en materia de seguridad y supervisar el Sistema de Gestión de la Seguridad de la Información.
g) Proponer a la Dirección cambios en la política de seguridad.
h) Aprobar las normas en materia de seguridad de la información.
i) Dirigir la política de comunicación de las cuestiones relacionadas con la seguridad de la información.
j) Analizar los resultados más significativos de las auditorías periódicas.
k) Priorizar las líneas de actuación en materia de seguridad.
l) Resolver los conflictos de responsabilidades en materia de seguridad de la información que puedan surgir.

7.5.3 Régimen de funcionamiento

El Comité de Seguridad de la Información se reunirá con carácter ordinario al menos una vez al año y, con carácter extraordinario, cuando así lo decida su presidente.
El funcionamiento del Comité de Seguridad de la Información se regirá por los siguientes principios:

- El presidente, previo informe del responsable del sistema o de los administradores de seguridad, establecerá el orden del día y convocará las reuniones.
- Las actas de las reuniones del Comité de Seguridad de la Información tendrán la clasificación de confidenciales y la difusión estará restringida a los miembros que lo integren. El Comité, durante las reuniones, puede decidir qué aspectos de sus decisiones y deliberaciones pueden ser públicos y el alcance de la comunicación.
- El Comité quedará válidamente constituido cuando comparezcan, al menos, la mitad de sus miembros y esté presente el responsable del sistema o uno de los administradores de seguridad.
- Para todas las comunicaciones del Comité de Seguridad de la Información se utilizarán los medios electrónicos corporativos.
- El Comité de Seguridad de la Información debe ajustar su funcionamiento a lo previsto en la legislación vigente con carácter general relativa al funcionamiento de los órganos colegiados.

7.6 Funciones y responsabilidades derivadas de la aplicación de la normativa en materia de tratamiento de datos de carácter personal.

La normativa en materia de Protección de Datos de Carácter Personal tiene numerosos puntos de contacto con el Esquema Nacional de Seguridad, en particular en lo que atañe a la necesidad de

que se establezca una responsabilidad sobre las decisiones que definan los fines de los tratamientos y sobre la seguridad de estos.

Adicionalmente, esta normativa contempla la figura de la persona delegada de protección de datos (en adelante, DPD), con un rol específico de asesoramiento y supervisión del cumplimiento de lo dispuesto en normativa de protección de datos y de las políticas de la Agencia en materia de protección de datos personales. Dado que es previsible que el DPD deba compaginar estas funciones con otras, es necesario evitar conflictos de intereses entre las diversas tareas. El DPD actúa como asesor y supervisor interno, por lo que no puede ocupar un puesto dentro de la organización que lo lleve a determinar los fines y los medios del procesamiento de datos personales. Si esta figura se asocia a uno de los anteriores perfiles de seguridad relacionados en el Esquema Nacional de Seguridad, se deberá tener en cuenta esta incompatibilidad.

El DPD será designado por la dirección de la Agencia y rendirá cuentas, en materia de tratamiento de datos de carácter personal, directamente a esta, la cual tiene la capacidad de adoptar o promover decisiones basadas en las recomendaciones, propuestas o evaluaciones del DPD.

El DPD se encargará del mantenimiento del Registro de actividades de tratamiento que lleve a cabo la Agencia y, en tanto persista la obligación de notificar las altas, bajas y modificaciones de ficheros con datos de carácter personal al Registro General de Protección de Datos de la Agencia Española de Protección de Datos, se le facultará para que pueda llevar a cabo los mencionados trámites en representación de la Agencia.

8 OBLIGACIONES DEL PERSONAL

El personal de la Agencia tiene la obligación de conocer y cumplir esta Política de Seguridad de la Información y la normativa de seguridad que de ella se derive, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para hacerla llegar a los afectados. 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 llevar a cabo sus funciones.

El Comité de Seguridad de la Información determinará el carácter obligatorio o voluntario de las acciones formativas.

9 TERCEROS

En el caso de que la Agencia preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, y se establecerán canales de coordinación y procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando la Agencia utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la normativa de seguridad que ataña a dichos servicios o información. Dicho tercero quedará sujeto a las obligaciones establecidas en esta 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 esté 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 un tercero, se requerirá un informe del Comité de Seguridad de la Información que precise los riesgos en que se incurre y la forma de tratarlos.

10 APROBACIÓN Y REVISIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Política de Seguridad de la Información será revisada, a propuesta del Comité de Seguridad de la Información, por resolución de la dirección de la Agencia.

Al menos una vez al año, el Comité de Seguridad de la Información incluirá entre los temas a discutir la revisión, actualización y propuestas de modificaciones de la Política de Seguridad.