Directrices Básicas de la Política de Seguridad de la Información, en el ámbito de la Administración Electrónica de la Audiencia de Cuentas de Canarias

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 30 de junio de 2016 por el Pleno de la Audiencia de Cuentas de Canarias de modificación de la Política de Seguridad de la Información y que fue acordado por el Pleno de la Audiencia de Cuentas de Canarias el día 31 de marzo de 2016.

2. INTRODUCCIÓN

⇒ 1. La implantación y utilización de los medios electrónicos en el ámbito de la Administración Pública supone el desarrollo y establecimiento de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

El Establecimiento de unas directrices básicas para la utilización de los medios electrónicos resulta de diversas normas existentes en el ordenamiento jurídico español, que sirven de referencia para esta Institución.

⇒ 2. Para ello, 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, establece los principios y requisitos de una política de seguridad en la utilización de los medios electrónicos que permita la adecuada protección de la información. El ENS establece que el marco organizativo está constituido por un conjunto de medidas relacionadas con la organización global de la seguridad.

⇒ 3. El artículo 11 del ENS establece que todos los órganos superiores de las Administraciones Públicas deberán disponer formalmente de su política de seguridad, que será aprobada por el titular del órgano superior correspondiente.

⇒ 4. En el ámbito de la Comunidad Autónoma de Canarias el Decreto 19/2011, de 10 de febrero, por el que se regula la utilización de los medios electrónicos en la Administración Pública de la Comunidad Autónoma de Canarias, garantiza, en el marco de los principios y derechos reconocidos en la Ley 11/2007, de 22 de junio de acceso electrónico de los ciudadanos a los Servicios Públicos, la igualdad, autenticidad, integridad, disponibilidad, accesibilidad, confidencialidad y conservación de la información y de los documentos electrónicos, así como la protección de datos de carácter personal. A tal fin prevé en su Disposición Adicional Cuarta la aprobación de la política de seguridad que se ha de aplicar en la utilización de los medios electrónicos.

⇒ 5. Por su parte la Audiencia de Cuentas de Canarias (ACC) creó y reguló la sede electrónica y el registro electrónico mediante Resolución de 15 de mayo de 2013.

⇒ 6. La Orden de 31 de julio de 2013, del Consejero de Presidencia, Justicia e Igualdad, establece el marco común y las directrices básicas de la política de seguridad de la información en el ámbito de la Administración Electrónica de la Administración Pública de la Comunidad Autónoma de Canarias.

⇒ 7. Asimismo las Guías CCN-STIC de Seguridad de los Sistemas de Información y Comunicaciones del Centro Criptológico Nacional (CCN-STIC Serie 800) establecen las políticas y procedimientos adecuados para la implementación de las medidas contempladas en el Esquema Nacional de Seguridad. Concretamente la Guía CCN- STIC 805 considera la Política de Seguridad de la Información como un documento de alto nivel que define lo que significa "seguridad de la información" en una organización. El documento debe estar accesible para todos los miembros de la organización y redactado de forma sencilla, precisa y comprensible, dejando los detalles técnicos para otros documentos normativos de segundo nivel.

⇒ 8. La política de seguridad deberá identificar unos claros responsables de velar por su cumplimiento y ser conocida por todos los miembros de la organización administrativa.

⇒ 9. La Audiencia de Cuentas de Canarias es consciente de la necesidad de utilizar 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.

⇒ 10. En tal sentido, la institución procurará realizar una gestión eficiente de recursos humanos, que dote a los servicios informáticos de la Audiencia de Cuentas de Canarias de los medios necesarios para desarrollar adecuadamente de los servicios TIC y la seguridad de los sistemas de información corporativos.

3. ALCANCE DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

⇒ 11. Esta política se aplica a todos los sistemas TIC de la Audiencia de Cuentas de Canarias y a todos los miembros de la organización, sin excepciones, debiendo ser conocida y cumplida por todo el personal y miembros de la Audiencia de Cuentas de Canarias.

⇒ 12. Se entenderá la Seguridad, como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información, quedando excluidas cualquier tipo de actuaciones puntuales o de tratamiento coyuntural.

4.- MISIÓN

⇒ 13. Corresponden a la Audiencia de Cuentas de Canarias las competencias, ámbito de actuación y funciones establecidas en la Ley 4/1989, de 2 de mayo, de la Audiencia de Cuentas de Canarias, constituyendo el servicio esencial que presta la fiscalización externa de la gestión económica, financiera y contable del sector público de la Comunidad Autónoma de Canarias.

5.- PRINCIPIOS DE LA PSI

⇒ 14. Sin perjuicio de los principios básicos establecidos en el Esquema Nacional de Seguridad, la política de seguridad del organismo se desarrollará, con carácter general, de acuerdo a los siguientes principios:

a) Principio de confidencialidad: los sistemas de información 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.

b) Principio de 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.

c) Principio de disponibilidad y continuidad: se garantizará un nivel de disponibilidad en los sistemas de información y se dotarán los planes y medidas necesarias para asegurar la continuidad de los servicios y la recuperación ante posibles contingencias graves.

d) Principio de gestión del riesgo: se deberá articular un proceso continuo de análisis y tratamiento de riesgos como mecanismo básico sobre el que debe descansar la gestión de la seguridad de los sistemas de información.

e) Principio de proporcionalidad en coste: la implantación de medidas que mitiguen los riesgos de seguridad de los sistemas de información deberá hacerse bajo un enfoque de proporcionalidad en los costes económicos y operativos.

f) Principio de concienciación y formación: se articularán iniciativas que permitan a las personas usuarias conocer sus deberes y obligaciones en cuanto al tratamiento seguro de la información. De igual forma, se fomentará la formación específica en materia de seguridad TIC de todas aquellas personas que gestionan y administran sistemas de información y telecomunicaciones.

g) Principio de prevención: se desarrollarán planes y líneas de trabajo específicas orientadas a prevenir fraudes, incumplimientos o incidentes relacionados con la seguridad TIC.

h) Principio de detección y respuesta: los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia respondiendo eficazmente, a través de los mecanismos establecidos al efecto, a los incidentes de seguridad.

i) Principio de 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 de la Audiencia de Cuentas de Canarias.

j) Principio de seguridad TIC en el ciclo de vida de los sistemas de información: 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.

k) Principio de función diferenciada: la responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios.

6.- DEFINICIONES

⇒ 15. A los efectos previstos en este documento, las definiciones, palabras, expresiones y términos han de ser entendidos en el siguiente sentido:

a) Sistema de Gestión de Seguridad de la Información (SGSI): sistema de gestión que, basado en el estudio de los riesgos, se establece para crear, implementar, hacer funcionar, supervisar, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión incluye la estructura organizativa, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos.

b) Gestión de riesgos: actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.

c) Infraestructura tecnológica corporativa: aquellos recursos físicos y lógicos, sobre los que se soportan los sistemas de información, los cuales gestiona el departamento competente en materia de telecomunicaciones y nuevas tecnologías.

d) Riesgo: estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.

e) Sistema de Información: conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.

7.- MARCO NORMATIVO

⇒ 16. El marco normativo para el desarrollo de la gestión de los servicios y competencias de la Audiencia de Cuentas de Canarias es el siguiente:

a) Ley 4/1989, de 2 de mayo, de la Audiencia de Cuentas de Canarias.

b) Reglamento de organización y funcionamiento de la Audiencia de Cuentas de Canarias, aprobado por Resolución de 1 de julio de 2002 de la Presidencia del Parlamento de Canarias.

c) Resolución de 15 de mayo de 2013 de creación y regulación de la sede electrónica y el registro electrónico de la Audiencia de Cuentas de Canarias.

d) Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. Esta norma quedará derogada, con efectos de 2 de octubre de 2016, por la disposición derogatoria única 2.b) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de la Administraciones Públicas.

e) Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

f) 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.

g) Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

h) 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.

i) Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y Procedimiento Administrativo Común. Esta norma quedará derogada, con efectos de 2 de octubre de 2016, por la disposición derogatoria única.2.a) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. Debe

tenerse en cuenta que la disposición final 7 de la citada ley establece un plazo de dos años desde su entrada en vigor para que produzcan efectos las previsiones relativas al registro electrónico de apoderamientos, registro electrónico, punto de acceso general electrónico de la Administración y archivo único electrónico, y por tanto, hasta ese momento, se mantendrán en vigor los artículos de la presente ley que traten sobre las materias citadas.

j) Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. Esta norma entrará en vigor el 2 de octubre de 2016, no obstante, las previsiones relativas al registro electrónico de apoderamientos, registro electrónico, registro de empleados públicos habilitados, punto de acceso general electrónico de la Administración y archivo único electrónico producirán efectos a los dos años de la entrada en vigor de la Ley.

k) Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. Esta ley entra en vigor el 2 de octubre de 2016, no obstante, las previsiones relativas al registro electrónico de apoderamientos, registro electrónico, registro de empleados públicos habilitados, punto de acceso general electrónico de la Administración y archivo único electrónico producirán efectos a los dos años de la entrada en vigor de la Ley).

l) Ley 59/2003, de 19 de diciembre, de firma electrónica.

Asimismo serán normas de referencia, en lo que se considere de aplicación por el Pleno de la Audiencia de Cuentas de Canarias, la siguiente normativa del Gobierno de Canarias.

m) Decreto 19/2011, de 10 de febrero, por el que se regula la utilización de los medios electrónicos en la Administración Pública de la Comunidad Autónoma de Canarias.

n) Orden de 31 de julio de 2013, por la que se establece el marco común y las directrices básicas de la política de seguridad de la información en el ámbito de la Administración Electrónica de la Administración Pública de la Comunidad Autónoma de Canarias.

8.- ORGANIZACIÓN DE LA SEGURIDAD

⇒ 17. El Pleno de la Audiencia de Cuentas de Canarias se encargará, en todo caso, de la aprobación y modificación de la Política de Seguridad, así como de la Norma de Seguridad de la ACC y demás normativa de carácter general, es decir, la del segundo nivel normativo, como las Normas de Seguridad TIC.

⇒ 18. La estructura organizativa de la gestión de la seguridad de la información en el ámbito de la Administración electrónica de la ACC está compuesta por los siguientes agentes:

- El Responsable de la Información y del Servicio, que es la Comisión de Seguridad Corporativa.
- El Responsable de la Seguridad, que es el Secretario General.
- El Responsable del Sistema y Administrador de Seguridad del Sistema de Información, que lo desempeña el analista informático.

8.1.- El Responsable de la Información y del Servicio

⇒ 19. El Responsable de la Información y del Servicio es la Comisión de Seguridad de la Información Corporativa, que establece las necesidades de seguridad de la información que se maneja, y efectúa las valoraciones del impacto que tendría un incidente que afectara a su seguridad. Tiene además, la potestad de modificar el nivel de seguridad requerido para la misma (Anexo II.5.7.2 del ENS), asimismo, determina los requisitos de seguridad del servicio prestado, según establece los artículos 10 y 44 del ENS, y es la encargada de aprobar la normativa de tercer nivel, como los Procedimientos Operativos STIC e Instrucciones Técnicas STIC.

⇒ 20. La Comisión de Seguridad de la Información Corporativa, es un órgano colegiado compuesto por el presidente, el secretario general, un técnico de auditoría jefe del Gabinete de la Presidencia, el responsable de sistemas y el operador informático.

⇒ 21. Sus funciones son:

a) Especificar los requisitos de la información en materia de seguridad.

b) Establecer las necesidades de seguridad de la información que se maneja.

c) Efectuar las valoraciones del impacto que tendría un incidente que afectara a su seguridad.

d) Modificar el nivel de seguridad requerido para la misma (Anexo 11.5.7.2 del ENS).

e) Organizar las funciones y responsabilidades de la política de seguridad del Organismo y de facilitar los recursos adecuados para alcanzar los objetivos propuestos.

f) Nombrar al resto de responsables.

g) Fijar la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.

h) Determinar los niveles de seguridad de la información tratada, valorando los impactos de los incidentes que afecten a la seguridad de la información (artículo 44 del ENS). A este fin podrá solicitar los informes pertinentes.

i) Aceptar los riesgos residuales calculados en el análisis de riesgos, y de realizar su seguimiento y control. Esta tarea podrá delegarla en el Responsable de Seguridad y en el Responsable del Sistema.

j) Acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.

8.2 El Responsable de Seguridad

⇒ 22. Conforme al artículo 10 del ENS, el Responsable de Seguridad es la persona que determina las decisiones para satisfacer los requisitos de seguridad de la información y del servicio.

⇒ 23. El Responsable de Seguridad será el Secretario General de la Audiencia de Cuentas de Canarias.

⇒ 24. Sus funciones son:

a) Coordinar las distintas áreas y unidades de la Institución para alcanzar los objetivos marcados por la Comisión de Seguridad Corporativa.

b) Dar cuenta a la Comisión de Seguridad Corporativa, a cuyo efecto procederá por medio de los informes correspondientes a:

- Realizar un resumen consolidado de actuaciones en materia de seguridad.
- Realizar un resumen consolidado de incidentes relativos a la seguridad de la información.
- Realizar un informe sobre el estado de la seguridad del sistema, en particular del riesgo residual al que el sistema está expuesto.

c) Promover la seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información.

d) Supervisar el cumplimiento de la política de seguridad, de sus normas, procedimientos derivados y de la configuración de seguridad de los sistemas.

e) Establecer las medidas de seguridad, adecuadas y eficaces para cumplir los requisitos de seguridad, siguiendo en todo momento lo exigido en el Anexo 11 del ENS, declarando la aplicabilidad de dichas medidas.

f) Promover las actividades de concienciación y formación en materia de seguridad en su ámbito de responsabilidad.

g) Realizar la coordinación y seguimiento de la implantación de los proyectos de adecuación al Esquema Nacional de Seguridad.

h) Realizar los preceptivos análisis de riesgos, de seleccionar las salvaguardas a implantar y de revisar el proceso de gestión del riesgo. Asimismo podrá aceptar los riesgos residuales calculados en el análisis de riesgos cuando la Comisión de Seguridad Corporativa haya delegado en él esta tarea.

i) Promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información y analizar los informes de auditoría, elaborando las conclusiones a presentar a la Comisión de Seguridad Corporativa para que adopten las medidas correctoras adecuadas.

j) Coordinar el proceso de Gestión de la Seguridad.

k) Firmar la Declaración de Aplicabilidad, que comprende la relación de medidas de seguridad seleccionadas para un sistema (arl°.27 y Anexo 11.2 del ENS).

l) Elaborar informes periódicos de seguridad que incluyan los incidentes más relevantes en cada período.

m) Determinar la categoría del sistema según el procedimiento descrito en el Anexo 1 del ENS y las medidas de seguridad que deben aplicarse de acuerdo con lo previsto en el Anexo 11 del ENS.

n) Verificar que las medidas de seguridad son adecuadas para la protección de la información y los servicios.

o) Procurar que la documentación de seguridad se mantenga organizada y actualizada y de gestionar los mecanismos de acceso a la misma.

⇒ 25. En la realización de estas funciones podrá contar con el apoyo del personal informático de la Institución y, en su caso, podrá proponer la contratación de la colaboración de los recursos externos que estime necesario.

8.3 El Responsable del Sistema y Administrador de la Seguridad del Sistema

⇒ 26. El Responsable del Sistema y Administrador de la Seguridad del mismo será el analista informático.

⇒ 27. Sus funciones en el ámbito informático son:

a) Encargarse de la operación y de la supervisión, con el apoyo del operador informático.

b) Centrarse en una actividad concreta y controlar cómo se realizan las operaciones.

c) Reportar al Responsable de la Seguridad.

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

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

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

g) Realizar ejercicios y pruebas sobre los procedimientos operativos de seguridad y los planes de continuidad existentes.

h) Seguir del ciclo de vida de los sistemas: especificación, arquitectura, desarrollo, operación y cambios.

i) Implantar las medidas necesarias para garantizar la seguridad del sistema durante todo su ciclo de vida, siguiendo las indicaciones del Responsable de Seguridad.

j) Proponer al Responsable de Seguridad la suspensión del manejo de una determinada información o la prestación de un cierto servicio electrónico si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. La suspensión deberá ser acordada, antes de ser ejecutada, con los responsables de la información afectada y el Responsable de la Seguridad.

k) Informar acerca de la aceptación de los riesgos residuales calculados en el análisis de riesgos.

l) Apoyar en el desarrollo de sus funciones al Responsable de Seguridad.

m) Implementar, gestionar y mantener las medidas de seguridad aplicables al sistema de información, siguiendo las instrucciones del responsable correspondiente.

n) Gestionar, configurar y proponer, en su caso la actualización, del hardware y software en los que se basan los mecanismos y servicios de seguridad de los sistemas de información.

o) Gestionar 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, bajo la supervisión del Responsable de Seguridad.

p) Aplicar los procedimientos operativos de seguridad.

q) Aplicar los cambios de configuración del sistema de información.

r) Asegurar que los controles de seguridad establecidos son cumplidos estrictamente, así como asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.

s) Supervisar las instalaciones de hardware y software, así como sus modificaciones y mejoras, para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.

t) 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, bajo la supervisión del Responsable de Seguridad.

u) Informar a los respectivos Responsables de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.

v) Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

9. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

⇒ 28. Será misión de la Secretaría General de la ACC el análisis y preparación de la revisión anual de estas Directrices Básicas de la Política de Seguridad de la Información, realizando una propuesta de modificación o mantenimiento de la misma que será aprobada por Pleno de la Audiencia de Cuentas de Canarias y difundida para que la conozcan todas las partes afectadas.

⇒ 29. Estas Directrices Básicas se desarrollará por medio de normativa de seguridad que aborde aspectos específicos. Esta normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y de comunicaciones.

⇒ 30. La normativa de seguridad estará disponible en la intranet institucional y página web de la ACC.

10. GESTIÓN DE RIESGOS

⇒ 31. La gestión de riesgos debe realizarse de manera continua sobre los sistemas de información, conforme a los principios de gestión de la seguridad basada en los riesgos (artículo 6 del ENS) y reevaluación periódica (artículo 9 del ENS).

⇒ 32. 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 informarse cada año por parte del

Responsable del Sistema, proponiéndose por el Responsable de Seguridad su aprobación por la Comisión de Seguridad.

11. DESARROLLO NORMATIVO DE LA PSI. DOCUMENTACIÓN DE SEGURIDAD

⇒ 33. El cuerpo normativo sobre seguridad de la información será de obligado cumplimiento y se desarrollará en cuatro niveles según el ámbito de aplicación y nivel de detalle técnico, de manera que cada norma de un determinado nivel de desarrollo se fundamente en las normas de nivel superior. Dichos niveles de desarrollo normativo son los siguientes:

a) Primer nivel normativo: El establecimiento de unas directrices básicas para la utilización de los medios electrónicos resulta de diversas normas existentes en el ordenamiento jurídico español, que sirven de referencia para esta Institución, como marco referencial, la Orden de 31 de julio de 2013 por la que se establece el marco común y las directrices básicas de la política de seguridad de la información de la Administración Pública de la Comunidad Autónoma de Canarias. Las presentes Directrices Básicas de Política de Seguridad de la Información de la Audiencia de Cuentas de Canarias aprobadas mediante acuerdo del Pleno de la Institución.

b) Segundo nivel normativo: Las normas reguladoras de las Políticas Específicas de Seguridad de la Información y las Normas de Seguridad TIC (Normas STIC) que desarrollan con un mayor grado de detalle la PSI dentro de un ámbito determinado. Las Normas dan respuesta, sin entrar en detalles de implementación ni tecnológicos, a qué se puede hacer y qué no en relación a un cierto tema desde el punto de vista de la seguridad: qué se considera un uso apropiado o inapropiado, las consecuencias derivadas del incumplimiento, entre otros aspectos.

   También pertenecen a este nivel la documentación de Procedimientos Generales del Sistema de Gestión de la Seguridad de la Información (SGSI) que establecen la manera en que la Organización establece, implementa, mantiene y mejora de manera continua el SGSI.

   Los documentos relativos a este segundo nivel normativo serán propuestos por la Comisión de Seguridad de la Información Corporativa al Pleno para su aprobación.

c) Tercer nivel normativo: Procedimientos Operativos STIC e Instrucciones Técnicas STIC. Son documentos que dan respuesta, incluyendo detalles de implementación y tecnológicos, a cómo se puede realizar una determinada tarea respetando los principios de seguridad de la organización, y los procesos internos en ella establecidos.
   Los Procedimientos STIC e Instrucciones Técnicas STIC serán propuestos por el Responsable de Seguridad a la Comisión de Seguridad de la Información Corporativa para su aprobación.

d) Cuarto Nivel: Informes, registros y evidencias electrónicas. Documentos de carácter técnico que pueden estar soportados en formatos normalizados que recogen el resultado y las conclusiones de un estudio, una actividad o una valoración; documentos de carácter técnico que recogen amenazas y vulnerabilidades de los sistemas de información, así como también evidencias electrónicas generadas durante todas las fases del ciclo de vida del sistema de información.

   La responsabilidad de que existan este tipo de documentos es del Responsable de Sistemas, de los que dará cuenta al Responsable de Seguridad.

⇒ 34. Aparte de los documentos citados en el punto anterior, la documentación de seguridad del sistema podrá contar, bajo criterio del Responsable de Seguridad, con otros documentos de carácter no vinculante: recomendaciones, buenas prácticas e informes, entre otros.

⇒ 35. El Responsable de Seguridad y el Responsable de Sistemas, serán los encargados de mantener la documentación de seguridad actualizada y organizada y de gestionar los mecanismos de acceso a la misma.

12. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

⇒ 36. Para el tratamiento de datos de carácter personal en los sistema de información se seguirá en todo momento lo desarrollado en el Documento de Seguridad y su documentación asociada conforme a lo exigido en el Título VIII de las medidas de seguridad en el tratamiento de datos de carácter personal del 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.

13. FORMACIÓN Y CONCIENCIACIÓN

⇒ 37. Constituye un objetivo de primer orden de la Audiencia de Cuentas de Canarias lograr la plena conciencia respecto a que la Seguridad de la Información afecta a todo el personal y miembros del organismo y a todas las actividades de acuerdo al principio de seguridad integral recogido en el artículo 5 del ENS. A estos efectos, la Audiencia de Cuentas de Canarias, propondrá y organizará sesiones formativas y de concienciación para que todos los empleados tengan una sensibilidad hacia los riesgos que se corren.

⇒ 38. Previo informe del Responsable del Sistema, el Responsable Seguridad propondrá a la Comisión de Seguridad una política de formación y concienciación en el tratamiento seguro de la información con los siguientes objetivos:

a) Formación sobre la protección de la información de datos de carácter personal, orientada a los responsables de los ficheros y hacia los usuarios con privilegios sobre los datos.

b) Formación sobre la política, normas y procedimientos de seguridad implantados y los riesgos existentes.

14. OBLIGACIONES DEL PERSONAL

⇒ 39. Todo el personal y miembros de la Audiencia de Cuentas de Canarias tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Responsable de la Seguridad disponer las actuaciones necesarias para que la información llegue a todos.

⇒ 40. El incumplimiento manifiesto de la Política de Seguridad de la Información o la normativa y procedimientos derivados de ésta, podrá acarrear el inicio de las medidas disciplinarias oportunas y, en su caso, las responsabilidades legales correspondientes.

15. TERCERAS PARTES

⇒ 41. Cuando la Audiencia de Cuentas de Canarias preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités o Responsables de Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

⇒ 42. Cuando la Audiencia de Cuentas de Canarias utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

⇒ 43. La Audiencia de Cuentas de Canarias podrá contar con empresas y organismos externos que ayuden a mejorar sus sistemas de seguridad, mediante la contratación de auditorías, asistencias técnicas o trabajos y desarrollos especializados.

16. AUDITORÍA

⇒ 44. Los sistemas de información corporativos de la Audiencia de Cuentas de Canarias serán objeto, al menos cada dos años, de una auditoría regular ordinaria externa que verifique el cumplimiento de los requerimientos del ENS. Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad requeridas.

⇒ 45. Estas Directrices Básicas entrarán en vigor al día siguiente de su publicación en la Intranet y página web de la ACC.