RESOLUCIÓN DEL PRESIDENTE DE LA CONFENDERACIÓN HIDROGRÁFICA DEL GUADIANA POR LA QUE SE APRUEBA LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN EL ÁMBITO DE ADMINISTRACIÓN ELECTRÓNICA Y DE PRIVACIDAD DE LOS TRATAMIENTOS DE DATOS PERSONALES (PSIP)

CONFEDERACIÓN HIDROGRÁFICA DEL GUADIANA

Índice de Contenidos

1 OBJETO Y ALCANCE

El objeto del presente documento es la definición de la política de seguridad de la información y protección de datos (PSIP) en el marco de los sistemas de información y de las actividades de tratamiento con datos de carácter personal de Tecnologías de la Información y la Comunicación, Aplicaciones y Redes para la CONFEDERACIÓN HIDROGRÁFICA DEL GUADIANA (CHG), incluyendo a la información que se almacena y/o procesa mediante los sistemas informáticos y soportes de uso habitual, ya sean internos o externos vinculados a la entidad en cuanto a las dimensiones de disponibilidad, integridad, confidencialidad, trazabilidad y autenticidad de los datos, según lo establecido por el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS).

Para ello el presente documento establece las directrices generales que garanticen la gestión de la seguridad de la información de manera íntegra y coordinada con los objetivos y líneas estratégicas del Organismo. La protección frente a dichas amenazas, intencionadas o accidentales, requiere una estrategia que permita actuar, tanto de forma preventiva, como reactiva, supervisando y monitorizando todo el ciclo de vida de los sistemas con el fin de reaccionar de forma efectiva a los incidentes y dotar al Organismo de los recursos necesarios para ello

La PSIP será de obligado cumplimiento para todas las unidades que conforman la estructura de la CHG y para todo el personal con acceso a la información, con independencia de su destino, condición laboral o relación por la que se accede a la información.

La PSIP afectará a la información y datos personales tratados por medios electrónicos y en soporte papel que la CHG gestiona en el ámbito de sus procesos delimitado a los sistemas de información y recursos que dan soporte a los siguientes servicios e información:

a) Gestión de la Información Hidrológica de la cuenca.

b) Gestión del Plan Hidrológico de la cuenca.

c) Gestión de expedientes de Dominio Público Hidráulico, de calidad de las aguas y

aprovechamientos de uso de agua.

d) Gestión y explotación de las obras hidráulicas para la gestión de recursos hídricos.

e) Gestión administrativa, económica y jurídica de la CHG

Esta política, así como el resto de documentación relativa a la Seguridad de la Información, al ENS y Protección de Datos. Dicha aprobación se considerará fehaciente cuando[1]:

[1] CCN-STIC-808 ENS (Verificación del cumplimiento), pag. 11, apartado 4.6.

a. El documento esté firmado electrónicamente por el/los responsables(s) pertinentes.

b. El documento esté impreso y firmado por el/los responsables(s) pertinentes, conservándose la copia original del mismo.

c. El documento haya sido aprobado en una reunión formal del órgano o comité competente, donde los responsables estén involucrados, y su aprobación conste reflejada en el acta de la sesión.

2 MISIÓN Y SERVICIOS PRESTADOS.

La CHG ejerce sus competencias según la regulación actual de las Confederaciones Hidrográficas derivada del Texto Refundido de la Ley de Aguas, aprobado por Real Decreto legislativo 1/2001, de 20 de julio, en el que se establecen las funciones para los organismos de cuenca, en concreto:

1. La elaboración del plan hidrológico de cuenca, así como su seguimiento y revisión.
2. La administración y control del dominio público hidráulico.
3. La administración y control de los aprovechamientos de interés general o que afecten a más de una Comunidad Autónoma.
4. El proyecto, la construcción y explotación de las obras realizadas con cargo a los fondos propios del organismo, y las que les sean encomendadas por el Estado.
5. Las que se deriven de los convenios con comunidades autónomas, corporaciones locales y otras entidades públicas o privadas, o de los suscritos con los particulares.

Así mismo se definen, las siguientes atribuciones y cometidos para para el desempeño de sus funciones:

6. El otorgamiento de autorizaciones y concesiones referentes al dominio público hidráulico, salvo las relativas a las obras y actuaciones de interés general del Estado, que corresponderán al Ministerio de Medio Ambiente.
7. La inspección y vigilancia del cumplimiento de las condiciones de concesiones y autorizaciones relativas al dominio público hidráulico.
8. La realización de aforos, estudios de hidrología, información sobre crecidas y control de la calidad de las aguas.
9. El estudio, proyecto, ejecución, conservación, explotación y mejora de las obras incluidas en sus propios planes, así como de aquellas otras que pudieran encomendárseles.
10. La definición de objetivos y programas de calidad de acuerdo con la planificación hidrológica.

11. La realización, en el ámbito de sus competencias, de planes, programas y acciones que tengan como objetivo una adecuada gestión de las demandas, a fin de promover el ahorro y la eficiencia económica y ambiental de los diferentes usos del agua mediante el aprovechamiento global e integrado de las aguas superficiales y subterráneas, de acuerdo, en su caso, con las previsiones de la correspondiente planificación sectorial.
12. La prestación de toda clase de servicios técnicos relacionados con el cumplimiento de sus fines específicos y, cuando les fuera solicitado, el asesoramiento a la Administración General del Estado, Comunidades Autónomas, Corporaciones Locales y demás entidades públicas o privadas, así como a los particulares.

Estas actividades se encuadran dentro de un contexto de amenazas, riesgos de ciberseguridad y expectativas de las partes interesadas.

3 MARCO NORMATIVO.

Las referencias tenidas en cuenta para la redacción de esta política han sido las siguientes:

En materia de Administración electrónica:

- Ley 9/1968, de 5 de abril, sobre secretos oficiales.
- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- Ley 8/2011 por la que se establecen medidas para la Protección de las Infraestructuras Críticas.
- R.D. 704/2011 por la que se aprueba el Reglamento para la Protección de las Infraestructuras Críticas.
- Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

En materia de aguas

- Real Decreto Legislativo 1/2001, de 20 de julio, por el que se aprueba el Texto Refundido de la Ley de Aguas.
- Directiva 2000/60/CE del Parlamento Europeo y del Consejo, de 23 de octubre de 2000, por la que se establece un marco comunitario de actuación en el ámbito de la política de aguas.
- Real Decreto 929/1989, de 21 de julio, por el que se constituye el Organismo de cuenca Confederación Hidrográfica del Guadiana.
- Real Decreto 927/1988, de 29 julio, que aprueba el Reglamento de la Administración Pública del Agua y de la Planificación Hidrológica.
- Real Decreto 849/1986, de 11 abril, que aprueba el Reglamento del Dominio Público Hidráulico.
- Ley 27/2006, de 18 de julio, que regula los derechos de acceso a la información, de participación pública y de acceso a la justicia en materia de medio ambiente.

En materia de protección de datos:

- Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en cuanto al tratamiento y la libre circulación de datos personales, en adelante RGPD.
- Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales, en adelante LOPDGDD).
- Dictámenes, informes, guías y recomendaciones de la Agencia Española de Protección de Datos.

Otras referencias, estándares y buenas prácticas:

- Normas y estándares sobre Seguridad de la Información, en especial la última versión vigente de las normas ISO/IEC 27001 e ISO 27002, La información contenida en los sistemas de información queda regulada por la norma ISO/IEC 27001, Sistemas de Gestión de Seguridad de la Información (SGSI).

4 PRINCIPIOS Y OBJETIVOS DE PROTECCIÓN.

La CHG tratará la información y los datos personales bajo su responsabilidad conforme a los siguientes principios de protección de datos y seguridad de la información:

1. **Licitud, lealtad y transparencia:** los datos de carácter personal serán tratados de manera lícita, leal y transparente en relación con el interesado.
2. **Legitimación en el tratamiento de datos personales:** solo se tratarán los datos de carácter personal cuando dicho tratamiento se encuentre amparado en alguna de las causas de legitimación establecidas en los artículos 6 y 9 del RGPD.
3. **Limitación de la finalidad:** los datos de carácter personal serán tratados para el cumplimiento de fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.
4. **Minimización de datos:** los datos de carácter personal serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
5. **Exactitud:** los datos de carácter personal serán exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.
6. **Limitación del plazo de conservación:** los datos de carácter personal personales serán mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines que justificaron su tratamiento.
7. **Responsabilidad proactiva:** La CHG será responsable del cumplimiento de los principios anteriormente señalados y adoptará las medidas técnicas y organizativas que le permitan estar en condiciones de demostrar dicho cumplimiento.
8. **Atención de los derechos de los afectados:** se adoptarán medidas en la organización que garanticen el adecuado ejercicio por los afectados, cuando proceda, de los derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad respecto de sus datos de carácter personal.
9. **Protección de datos y seguridad desde el diseño:** La CHG promoverá la implantación del principio de protección de datos desde el diseño con el objetivo de cumplir los requisitos definidos en el RGPD y, por tanto, los derechos de los interesados de forma que la protección de datos se encuentre presente en las primeras fases de concepción de un proyecto. Asimismo, la seguridad de la información se aplicará desde el diseño inicial de los sistemas de información.
10. **Confidencialidad e Integridad:** se deberá garantizar que la información sea completa, precisa y accesible únicamente para aquellas personas expresamente autorizadas para ello.

11. **Disponibilidad:** se garantizará la prestación continua de los servicios y la recuperación inmediata ante posibles contingencias, mediante medidas de recuperación orientadas a la restauración de los servicios y de la información asociada.
12. **Trazabilidad.** Permite el rastreo de un mensaje o contenido hasta su origen.
13. **Negativa al repudio.** Garantiza al receptor de una comunicación que el mensaje fue originado por el emisor, previniendo que el emisor niegue el envío de esa comunicación.
14. **La autenticidad:** se basa en la garantía de la legitimidad del origen de la transmisión de la información (el emisor de la información es quien dice ser). Muy vinculada a la integridad, ya que hace referencia a la veracidad total del mensaje.
15. **Gestión del riesgo:** conjunto de actividades coordinadas que la CHG desarrolla para dirigir y controlar el riesgo, entendiendo como riesgo el efecto de la incertidumbre sobre la consecución de los objetivos que, en el marco del RGPD, es la protección de los derechos y libertades de los titulares de los datos que trata la CHG. El análisis y gestión de riesgos es una parte esencial del proceso de protección de datos y de seguridad de la información, de forma que permita el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad.
16. **Mejora continua:** se revisará de manera recurrente el grado de eficacia de los controles de seguridad implantados para aumentar la capacidad de adaptación a la constante evolución del entorno alineando la PSI y el cuerpo normativo de seguridad de la información con la legislación aplicable, estándares, 'mejores prácticas' y criterios internacionales de reconocido prestigio.
17. **Proporcionalidad en coste:** la implantación de medidas que mitiguen los riesgos de seguridad de los activos deberá hacerse dentro del marco presupuestario previsto a tal efecto y siempre buscando el equilibrio entre las medidas de seguridad, la naturaleza de la información y el presupuesto previsto.
18. **Concienciación y formación:** se articularán programas de formación, sensibilización y concienciación para las personas usuarias en materia de seguridad de la información.
19. **Proceso de verificación:** La CHG implantará un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad de los tratamientos.

5 ESTRUCTURA ORGANIZATIVA DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

Según la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, el Titular del Organismo de CHG ostenta la máxima responsabilidad en el desarrollo de las competencias de la entidad, incluidas las de seguridad de la información. Es, por tanto, el máximo responsable de la implantación y aplicación del ENS.

La PSIP debe identificar unos claros responsables para velar por su cumplimiento y ser conocida por todos los miembros de CHG

La estructura organizativa para la gestión de la seguridad de la información y privacidad en la CHG se nombrará formalmente por resolución de la Presidencia y estará compuesta por los siguientes roles, organizados y coordinados a través del órgano gestor Comité Responsable de Seguridad de la Información (CRSI) el cual será encargado de asignar responsabilidades nominativas para cada función de seguridad que serán formalmente nombrados conforme a la presente PSIP.

1. Comité Responsable de Seguridad de la Información (CRSI).
2. Responsable de la información.
3. Responsable del servicio.
4. Responsable del sistema.
5. El Administrador de seguridad del sistema.
6. Responsable de seguridad de la información (CISO).
7. Delegado de la Protección de Datos (DPD).
8. Responsable de seguridad y enlace para la protección de las infraestructuras críticas.

La concreción de qué personas ostentan cada cargo figurará en el Anexo A. Nombramientos del presente documento. A continuación, se describen los roles y responsabilidades de cada uno de estos cargos.

5.1 COMITÉ RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN (CRSI).

Es el órgano colegiado que coordinará las medidas de la Seguridad de la Información y la Privacidad a nivel de organización. Estará constituido por el Responsable de Seguridad de la Información y por representantes de las áreas afectadas por el ENS y el Delegado de Protección de Datos.

La composición y funcionamiento del Comité Responsable de Seguridad de la Información (CRSI) se constituirá de conformidad con lo dispuesto en la Sección 3ª del Capítulo II de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y podrá desarrollarse a través de resolución aprobada por el titular del Organismo.

Estará constituido por representantes de las áreas afectadas por el Esquema Nacional de Seguridad entre los que se encontrarán al menos

- El Secretario\a General, que actuará como Presidente\a del Comité.

- El Responsable de Seguridad de la Información (en adelante Responsable de Seguridad), que actuará como Secretario del Comité de Seguridad

- Vocales:

  - Los Jefes de Unidad del Organismo: Comisaría de Aguas, Dirección Técnica y la Oficina de Planificación Hidrológica

  -El Responsable de las instalaciones del Organismo y del archivo documental, como responsable de la seguridad física

  - El Responsable del servicio de RRHH

  -El Responsable del asesoramiento jurídico

  -El Responsable del sistema

  - El Administrador de seguridad del sistema

  -El Responsable de seguridad y enlace para la protección de las infraestructuras críticas

Podrán ser invitados al Comité de Seguridad, en función de las circunstancias, cualquier otro Jefe de Área/Servicio implicado en alguno de los aspectos relativos a la seguridad de la información, así como asesores externos, siempre y cuando el Presidente\a del Comité de Seguridad lo considere adecuado. También podrán constituirse grupos de trabajo especializados internos, externos o mixtos. En caso que se estime necesario por el Presidente\a del Comité de Seguridad se autorizará la asistencia de miembros del mismo a cursos u otro tipo de entornos formativos o de intercambio de experiencias relacionadas directamente con su actividad en el Comité.

Sus funciones serán las siguientes:

1. Atender las inquietudes de la Presidencia y de las diferentes áreas.
2. Informar regularmente del estado de la seguridad de la información a la Presidencia.
3. Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información.
4. Elaborar la estrategia de evolución de la Organización en lo que respecta a la seguridad de la información.

5. Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
6. Elaborar (y revisar regularmente) la Política de Seguridad de la información y Privacidad para que sea aprobada por la Dirección.
7. Aprobar la normativa de seguridad de la información.
8. Establecer criterios para el procedimiento de análisis de riesgos y elaborar propuestas de niveles de riesgos aceptables para seguridad de la Información.
9. Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.
10. Monitorizar los principales riesgos residuales asumidos por la Organización y recomendar posibles actuaciones respecto de ellos.
11. Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.
12. Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
13. Analizar los informes facilitados por el Responsable de Seguridad en los que, relativos al resultado de los análisis de riesgos, de las auditorías realizadas, de los proyectos y de las iniciativas y acciones de mejora de la seguridad requeridas.
14. Aprobar planes de mejora de la seguridad de la información de la Organización. En particular, velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.
15. Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
16. Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la Organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

En caso de ocurrencia de incidentes de seguridad de la información aprobará el Plan de Mejora de la Seguridad, con su dotación presupuestaria correspondiente.

El Comité asumirá además las siguientes funciones:

- Responsabilidades derivadas del tratamiento de datos de carácter personal.

- Asunción de la figura del Responsable del Servicio para todos los servicios prestados en el marco de la Ley 39/2015.

- Asunción de la figura de Responsable de la Información para todas las informaciones manejadas por los servicios prestados en el marco de la Ley 39/2015.

El CRSI no es un comité técnico, pero recabará regularmente del personal técnico propio o externo, la información pertinente para tomar decisiones. El CRSI se asesorará de los temas sobre los que tenga que decidir o emitir una opinión, este asesoramiento se determinará en cada caso, pudiendo materializarse de diferentes formas y maneras:

- Grupos de trabajo especializados internos, externos o mixtos.
- Asesoría externa.

El Responsable de la Seguridad de la Información es el secretario del Comité de Seguridad de la Información y como tal:

- Convoca las reuniones del Comité de Seguridad de la Información.
- Prepara los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elabora el acta de las reuniones.
- Es responsable del traslado de las decisiones del Comité que afecten en su ejecución a otras Unidades.

5.2 RESPONSABLE DE LA INFORMACIÓN.

Corresponde al CRSI como órgano colegiado y en calidad de Responsable de la Información el establecimiento de los niveles y medidas de seguridad de la información dentro del marco de lo previsto en los Anexos I y II del 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.

Así mismo, corresponde al CRSI como responsable de los tratamientos de datos personales el establecimiento de los niveles y medidas de seguridad establecidas por la L.O. 3/2018 que se concretan en las medidas establecidas por el Esquema Nacional de Seguridad.

Tiene entre sus funciones las siguientes:[2]

1. Tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.
2. El Responsable de la Información es el responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad de integridad.
3. Establece los requisitos de la información en materia de seguridad. En el marco del ENS, equivale a la potestad de determinar los niveles de seguridad de la información.

[2] CCN-STIC-801 Esquema Nacional de Seguridad – Responsabilidades. Pag 14. Epígrafe 5.1.

4. Determinará los niveles de seguridad en cada dimensión dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad.

Aunque la aprobación formal de los niveles corresponda al Responsable de la In formación, podrá recabar una propuesta al Responsable de la Seguridad y conviene que escuche la opinión del Responsable del Sistema.

La Presidencia de la CHG, podrá revocar o ratificar las decisiones del CRSI. Corresponde a la Presidencia en calidad de máximo responsable aprobar la PSIP.

5.3 RESPONSABLE DEL SERVICIO.

Corresponde al CRSI como órgano colegiado y en calidad de Responsable del Servicio el establecimiento de los niveles y medidas de seguridad de la información dentro del marco de lo previsto en los Anexos I y II del 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.

Tiene entre sus funciones las siguientes[3]:

1. Establece los requisitos de los servicios en materia de seguridad. En el marco del ENS, equivale a la potestad de determinar los niveles de seguridad de la información.
2. Tiene la responsabilidad última del uso que se haga de determinados servicios y, por tanto, de su protección.
3. El Responsable del Servicio es el responsable último de cualquier error o negligencia que lleve a un incidente de disponibilidad de los servicios.
4. Determinará los niveles de seguridad en cada dimensión[4] del servicio dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad.
5. Aunque la aprobación formal de los niveles corresponda al Responsable del Servicio, podrá recabar una propuesta al Responsable de la Seguridad y conviene que escuche la opinión del Responsable del Sistema.
6. La prestación de un servicio siempre debe atender a los requisitos de seguridad de la información que maneja, de forma que pueden heredarse los requisitos de seguridad de la misma, añadiendo requisitos de disponibilidad, así como otros como accesibilidad, interoperabilidad, etc.

5.4 RESPONSABLE DEL SISTEMA.

Será el encargado del desarrollo, la operación y mantenimiento de los sistemas de información durante su ciclo de vida completo y podrá delegar en el responsable del servicio las funciones de explotación del sistema que puedan suponer una mejora en el servicio.

---

[3] CCN-STIC-801 Esquema Nacional de Seguridad – Responsabilidades. Pag. 14. Epígrafe 5.2.

[4] a) Confidencialidad [C]. b) Integridad [I]. c) Trazabilidad [T]. d) Autenticidad [A]. e) Disponibilidad [D].

Las funciones del Responsable del Sistema, serán las siguientes:

1. Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
2. Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
3. Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
4. El Responsable del Sistema puede 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. Esta decisión debe ser acordada con los Responsables de la Información afectada, del Servicio afectado y con el Responsable de la Seguridad antes de ser ejecutada.
5. Aplicar los procedimientos operativos de seguridad elaborados y aprobados por el Responsable de Seguridad.
6. Monitorizar el estado de la seguridad del Sistema de Información y reportarlo periódicamente o ante incidentes de seguridad relevantes al Responsable de Seguridad de la Información.
7. En su caso, elaborar los Planes de Continuidad del Sistema para que sean validados por el Responsable de Seguridad de la Información, y coordinados y aprobados por el Comité Responsable de Seguridad de la Información (CRSI).
8. En su caso, realizar ejercicios y pruebas periódicas de los Planes de Continuidad del Sistema para mantenerlos actualizados y verificar que son efectivos.
9. Elaborará las directrices para considerar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos (especificación, arquitectura, desarrollo, operación y cambios) y las facilitará al Responsable de Seguridad de la Información para su aprobación.
10. Planificará la implantación de las salvaguardas en el sistema.
11. Ejecutará el plan de seguridad aprobado.

5.5 ADMINISTRADOR DE LA SEGURIDAD DEL SISTEMA

El rol no podrá ser desarrollado por un órgano colegiado, ni podrá delegar parte de sus funciones en otras personas. En su caso, se nombrarían nuevos Administradores de la Seguridad del Sistema. Será propuesto por el Responsable del Sistema, a quien reportará en todo lo relacionado con seguridad de la información.

Sus funciones serán las siguientes:

1. La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.
2. Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.

3. Asegurar que la trazabilidad, pistas de auditoría y otros registros de seguridad requeridos se encuentren habilitados y registren con la frecuencia deseada, de acuerdo con la Política de Seguridad establecida por el Organismo.
4. Aplicar a los sistemas, usuarios y otros activos y recursos relacionados con el mismo, tanto internos como externos, los Procedimientos Operativos de Seguridad y los mecanismos y servicios de seguridad requeridos.
5. Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información y los mecanismos y servicios de seguridad requeridos.
6. 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.
7. Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida.
8. Aprobar los cambios en la configuración vigente del sistema de información, garantizando que sigan operativos los mecanismos y servicios de seguridad habilitados.
9. Informar a los Responsables de la Seguridad de la información y del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
10. Monitorizar el estado de la seguridad del sistema

En caso de ocurrencia de incidentes de seguridad de la información:

1. Llevar a cabo el registro, contabilidad y gestión de los incidentes de seguridad en los sistemas bajo su responsabilidad.
2. Ejecutar el Plan de Seguridad aprobado.
3. Aislar el incidente para evitar la propagación a elementos ajenos a la situación de riesgo.
4. Tomar decisiones a corto plazo si la información se ha visto comprometida de tal forma que pudiera tener consecuencias graves (estas actuaciones deberían estar procedimentadas para reducir el margen de discrecionalidad del Administrador de Seguridad del Sistema al mínimo número de casos).
5. Asegurar la integridad de los elementos críticos del sistema si se ha visto afectada la disponibilidad de los mismos (estas actuaciones deberían estar procedimentadas para reducir el margen de discrecionalidad del Administrador de Seguridad del Sistema al mínimo número de casos).
6. Mantener y recuperar la información almacenada por el sistema y sus servicios asociados.
7. Investigar el incidente: determinar el modo, los medios, los motivos y el origen del incidente

5.6 RESPONSABLE DE LA SEGURIDAD FÍSICA E INSTALACIONES

Cuando la seguridad física (de las instalaciones) esté segregada de la seguridad lógica, esta se ajustará a lo establecido por el Esquema Nacional de Seguridad en materia de seguridad física de forma análoga a lo establecido en los puntos anteriores.

El Responsable de Seguridad Física implantará las medidas de seguridad que le competan dentro de las determinadas por el Responsable de Seguridad, e informará a éste de su grado de implantación, eficacia e incidentes.

5.7 RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN (CISO).

Las funciones del Responsable de Seguridad de la Información de la CHG, sin perjuicio de las que en el futuro pueda asignarle el Responsable de la Información, serán las siguientes:

1) Reportará directamente al Comité de Seguridad.
2) Actuará como Secretario del Comité de Seguridad.
3) Convocará al Comité de Seguridad, recopilando la información pertinente
4) Promover la seguridad de la información entre el personal de la CHG.
5) Promover el mantenimiento de la mejora continua de la seguridad de la información.
6) La elaboración de procedimientos y normativa de seguridad que serán presentados al Comité de Seguridad para su revisión y aprobación.
7) El impulso y la realización de análisis de riesgos anuales sobre los sistemas de información de la CHG.
8) La elaboración de un informe de revisión anual sobre el estado de la seguridad.
9) La realización de auditorías periódicas internas o externas para verificar el cumplimiento de las obligaciones de la CHG con relación a la seguridad de la información.
10) La coordinación de las actuaciones en materia de seguridad de la información entre las unidades que explotan la información y los responsables de los servicios de la CHG.
11) La coordinación con el Centro Criptológico Nacional (CCN-CERT) y el Instituto Nacional de Ciberseguridad (INCIBE) en la utilización de servicios de respuesta a incidentes de seguridad de la información.
12) La coordinación y control del cumplimiento de las medidas de seguridad definidas para la protección de los tratamientos de datos de carácter personal.
13) El mantenimiento actualizado del marco documental de la Seguridad de la Información en el ámbito de la Ley Orgánica 3/2018 LOPDGD de 5 de diciembre y el Real Decreto 311/2022 ENS de 3 de mayo y sus respectivas normativas de desarrollo.
14) La gestión de las incidencias de seguridad de la información que se produzcan informando de las más relevantes al Comité de Seguridad y a los responsables de las unidades de la CHG afectadas por las incidencias.

5.8 DELEGADO DE PROTECCIÓN DE DATOS[5].

Cumplirá sus funciones dentro del marco de las funciones del Delegado de Protección de Datos de la CHG, entre las que se encuentran[6]:

1. Asesorar y supervisar el cumplimiento de principios relativos al tratamiento, como los de limitación de finalidad, minimización o exactitud de los datos
2. Asesorar y supervisar que se han definido plazos de conservación para los datos y que existen y se aplican procedimientos correctos para su destrucción cuando correspon da
3. Supervisar que los tratamientos disponen de bases jurídicas o legitimación
4. Asesorar sobre la compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos
5. Asesorar sobre la existencia de normativa sectorial que pueda determinar condiciones de tratamiento específicas distintas de las establecidas por la normativa general de protección de datos
6. Asesorar y supervisar el diseño e implantación de medidas de información a los afectados por los tratamientos de datos (cláusulas)
7. Asesorar y supervisar que existen mecanismos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de los interesados
8. Supervisar las solicitudes de ejercicio de derechos por parte de los interesados
9. Supervisar la diligencia en la contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación responsable-encargado.

---

[5] LO 3/2018, de 5 de diciembre, LOPDGD. Art. 34.3. Los responsables y encargados del tratamiento comunicarán en el plazo de diez días a la Agencia Española de Protección de Datos o, en su caso, a las autoridades autonómicas de protección de datos, las designaciones, nombramientos y ceses de los delegados de protección de datos tanto en los supuestos en que se encuentren obligadas a su designación como en el caso en que sea voluntaria.

[6] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, art. 38. 3. El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones. No será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones. El delegado de protección de datos rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado.

RD 3/2018, artículo 36. 2. Posición del delegado de protección de datos. Cuando se trate de una persona física integrada en la organización del responsable o encargado del tratamiento, el delegado de protección de datos no podrá ser removido ni sancionado por el responsable o el encargado por desempeñar sus funciones salvo que incurriera en dolo o negligencia grave en su ejercicio. Se garantizará la independencia del delegado de protección de datos dentro de la organización, debiendo evitarse cualquier conflicto de intereses.

10. Asesorar y supervisar sobre los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de la organización y de las razones que justifiquen la transferencia
11. Asesorar y supervisar el diseño e implantación de políticas de protección de datos
12. Revisar los controles y auditorías de Seguridad y protección de datos y reportar conclusiones a la Dirección
13. Supervisar la primera versión de los registros de actividades de tratamiento, así como los cambios que se realicen en los mismos
14. Asesorar y supervisar los supuestos de necesidad de realización de evaluaciones de impacto sobre la protección de datos

15) Asesorar, revisar y validar los análisis de riesgo y Evaluaciones de Impacto realizados

16) Asesorar y supervisar la implantación de las medidas de protección de datos desde el diseño y protección de datos por defecto adecuadas a los riesgos y naturaleza de los tratamientos

17) Asesorar y supervisar en la Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos

18) Supervisar los procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de los afectados y los procedimientos de notificación a las autoridades de supervisión y a los afectados

19) Comunicar las violaciones de seguridad a las autoridades e interesados cuando se requiera

20) Asesorar y supervisar los supuestos de necesidad de realización de evaluaciones de impacto sobre la protección de datos

21) Supervisar las evaluaciones de impacto sobre la protección de datos

22) Mantener las relaciones con las autoridades de supervisión

23) Mantener el contacto con los interesados

24) Asesorar y supervisar en el diseño de programas de formación, concienciación y sensibilización de usuarios

25) Reportar periódicamente a Dirección sobre el estado de cumplimiento en la materia y las acciones que haya que acometer, así como reportar ante incidencias y circunstancias que se produzcan puntualmente.

El Delegado de Protección de Datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento[7].

[7] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, art. 39.2.

5.9 RESOLUCIÓN DE CONFLICTOS

En caso de conflictos entre dos o más Responsables, el Comité de Seguridad emitirá una opinión y dará traslado de la misma a los superiores jerárquicos inmediatos a las partes que hubieran dado lugar al conflicto. Los superiores jerárquicos a las partes en conflicto emitirán una decisión o elevarán su propuesta a la Presidencia de la CHG donde se resolverá el conflicto de forma definitiva. Corresponderá en última instancia a la Presidencia la resolución de conflictos en calidad de máximo responsable de la Organización.

6 GESTIÓN DE RIESGOS.

El análisis de riesgos es la utilización sistemática de la información disponible para identificar peligros y estimar los riesgos a los que se encuentra o puede encontrarse expuesta la información.

La gestión de riesgos se entiende como el conjunto de actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.

Según lo establecido en la normativa vigente[8], el análisis y gestión de riesgos será parte esencial del proceso de seguridad y será la base para determinar las medidas de seguridad que se deben adoptar además de los mínimos establecidos por el ENS. Deberán tratarse, como mínimo, todos los riesgos que puedan impedir la prestación de los servicios o el cumplimiento de la misión del Organismo de forma grave, especialmente los riesgos que impliquen un cese en la prestación de servicios a los ciudadanos y se mantendrá permanentemente actualizado minimizando los riesgos hasta niveles aceptables.

Este análisis se repetirá:

- Regularmente, al menos una vez al año un análisis semiformal[9].

- Cuando se produzcan cambios significativos en la información manejada.

- Cuando se produzcan cambios significativos en los servicios prestados.

- Cuando se produzcan cambios significativos en los sistemas que tratan la información e intervienen en la prestación de los servicios

[8] Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, art. 14 y art. 39.

[9] Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, Anexo II 4.1.1 Análisis de riesgos [op.pl.1]. + Refuerzo 1. Análisis de riesgos semiformal.

- Cuando ocurra un incidente grave de seguridad.

- Cuando se reporten vulnerabilidades graves.

La metodología para la evaluación del riesgo es MAGERIT v.3 implementada mediante la herramienta PILAR y recomendada por el Centro Criptológico Nacional.

El Comité de Seguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

7 GESTIÓN DE INCIDENTES DE SEGURIDAD.

Las unidades deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello las unidades del Organismo, en el ámbito de sus competencias y para aquellos sistemas que gestionen de forma directa, implementarán las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos y aprobado por el Comité Responsable de la Seguridad de la información (CRSI). Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar definidos y documentados.

Para garantizar el cumplimiento de la política, las unidades deben:

1) Identificar y Autorizar los sistemas antes de entrar en operación.
2) Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
3) Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una disminución hasta el cese del nivel de prestación, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación y actuar en consecuencia. Recaerá en el administrador del sistema la responsabilidad de monitorizar un riesgo, aunque dicha función puede ser delegada en el día a día.

La monitorización es especialmente relevante cuando se establecen líneas de defensa, y de acuerdo con el ENS, se establecerán mecanismos de detección, análisis y reporte que puedan informar a los responsables tanto regularmente como cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

En base a las guías CCN STIC:

-Quien recopila la información sobre el desempeño del sistema de información en materia de seguridad es el propio administrador de dicho sistema.

-Que el sistema de información se comporta dentro de los márgenes aceptados de riesgo es función del Responsable de la Seguridad mediante su monitorización.

-Los Responsables de la Información y de los Servicios (en este caso el CRSI) han de ser informados de aquellas desviaciones significativas de los riesgos a la que están sujetos. Si estas desviaciones llegan a alcanzar un valor excesivo, el Responsable del Sistema puede acordar la suspensión temporal del servicio hasta que se puedan garantizar niveles aceptables de riesgo, teniendo en cuenta que, es la Dirección de la entidad pública la que en última instancia administrativamente, está competencialmente autorizada para suspender la prestación de los servicios.

Las respuestas a las incidencias tienen que:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar puntos de contacto para las comunicaciones con respecto a incidente 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).
- Establecer planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

Con independencia de los procedimientos de respuesta a las incidencias, los sistemas de información de la CHG deben garantizar la conservación de los datos e información en soporte electrónico. Estos sistemas deben estar concebidos en sus procedimientos para preservar el patrimonio digital del Organismo

8 DESARROLLO NORMATIVO

Todos los miembros que integran la estructura organizativa de la PSIP de la CHG promoverán el desarrollo de normas procedimientos y guías de seguridad de carácter general aplicables a todo la CHG o con carácter específico aplicable para un área concreta de la CHG.

En el desarrollo normativo el Comité Responsable de la Seguridad de la Información (CRSI) podrá requerir la colaboración de las áreas organizativas que componen la estructura orgánica de la CHG.

La PSIP se cumplimentará con documentos más precisos que ayudan a llevar a cabo lo propuesto. Para ello se utilizarán:

1) normas de seguridad
2) guías de seguridad
3) procedimientos de seguridad

Las normas uniformizan el uso de aspectos concretos del sistema. Indican el uso correcto y las responsabilidades de los usuarios. Son de carácter obligatorio.

Las guías tienen un carácter formativo y buscan ayudar a los usuarios a aplicar correctamente las medidas de seguridad proporcionando razonamientos donde no existen procedimientos precisos. Por ejemplo, suele haber una guía sobre cómo escribir procedimientos de seguridad. Las guías ayudan a prevenir que se pasen por alto aspectos importantes de seguridad que pueden materializarse de varias formas.

Los procedimientos operativos de seguridad afrontan tareas concretas, indicando lo que hay que hacer, paso a paso. Son útiles en tareas repetitivas.

9 CONCIENCIACIÓN Y FORMACIÓN.

Según refiere el principio de Seguridad Integral recogido en el artículo 6 del 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 y según lo previsto en la LOPDGDD, la CHG dispondrá los medios necesarios para que todas las personas con acceso a la información de la que es responsable o titular, sean informadas acerca de sus deberes y obligaciones así como de los riesgos existentes en el tratamiento de la información.

Será el Responsable de la Seguridad quien se encargue de promover dicha tarea de concienciación y formación en el ámbito del Comité Responsable de Seguridad de la Información (CRSI) como una de sus funciones fundamentales.

10 REVISIÓN DE LA POLITICA DE SEGURIDAD Y PRIVACIDAD.

La Política de Seguridad de la Información y Privacidad se someterá a un proceso de revisión anual[10] para adaptarse a las circunstancias técnicas u organizativas a fin de evitar su obsolescencia, así como cuando se produzcan cambios o circunstancias que por su trascendencia así lo aconsejen.

11 OBLIGACIONES DEL PERSONAL.

Todas las personas que presten servicio en la CHG tienen la obligación de conocer y cumplir lo previsto en la presente Política y lo previsto en sus correspondientes normas guías y procedimientos de seguridad. Con este objetivo, la CHG proporcionará la información y el

[10] CCN-STIC-808 ENS. Verificación del cumplimiento. pag. 25. Op.pl.1 (NI).

asesoramiento al personal en materia de protección de datos e instrucciones sobre las medidas de seguridad que establece 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.

Todos los miembros de la organización atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez cada dos años. Se establecerá un programa de concienciación continua para atender a todos los miembros de la organización, 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 cumplimiento de la presente Política de Seguridad es obligatorio por parte de todo el personal interno o externo que intervenga en los procesos la organización, constituyendo su incumplimiento infracción grave a efectos laborales.

Además de lo expuesto, todo el personal que presta servicio en la CHG tiene el deber de colaborar en la mejora de la seguridad de la información evitando y aminorando los riesgos a los que se encuentra expuesta la información y los datos personales de los que es titular la Organización debiendo en todo momento participar al Comité de Seguridad cualquier propuesta o sugerencia que ayude a preservar la confidencialidad, la integridad y la disponibilidad de la información.

12 TERCERAS PARTES

Cuando se presten servicios o se gestione información de otras organizaciones, se les hará partícipes de esta Política de Seguridad de la Información y Privacidad, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando se utilicen servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

Se establecerán procedimientos específicos de reporte y resolución de incidencias.

Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Administrador de Seguridad del

Sistema que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por el responsable de la seguridad de la información.

13 APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día de su firma por la Presidencia.

Esta Política se Seguridad de la Información y Privacidad es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política. La presente versión de la Política de Seguridad de la Información ha sido aprobada por D. Samuel Morale da Ludeña en calidad de Presidente de la Confederación Hidrográfica del Guadiana.

ANEXO A. NOMBRAMIENTOS.

1. Comité Responsable de Seguridad de la Información (CRSI).

- Presidencia: Secretaria General María Yolanda García Seco

- Miembros:

  - Jefes de Unidad del Organismo:

    -Comisaría de Aguas María Hayas López

    -Dirección Técnica Fernando Aranda Gutiérrez

    -Oficina de Planificación Hidrológica María José Fernández Silva

  -El Responsable de las instalaciones del Organismo y del archivo documental, como responsable de la seguridad física. Jefa de Área de RRHH y Servicios Luisa María Moreno Pizarro

  -Personal del servicio de RRHH. Jefe de Servicio de RR.HH Rafael Sánchez Cayetano

  -Personal del asesoramiento jurídico. Jefe de Sección Álvaro Gómez García

  -El Responsable del sistema. Jefe de Servicio de Informática Lino González López

  - El Administrador de seguridad del sistema. Jefe de Sección Informática Joaquín Diaz Jiménez

  -El Responsable de seguridad y enlace para la protección de las infraestructuras críticas Álvaro Paniagua de la Calle

- Secretario: Responsable de seguridad de la información (CISO). Jefe de Área Roberto Carballo Vinagre

2. Responsable de la información: competencias asumidas por Comité Responsable de Seguridad de la Información (CRSI)

3. Responsable del servicio: competencias asumidas por Comité Responsable de Seguridad de la Información (CRSI)

4. Delegado de la Protección de Datos (DPD). Jefe de Área Roberto Carballo Vinagre

ANEXO B. GLOSARIO DE TÉRMINOS Y ABREVIATURAS

Análisis de riesgos. Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.

Datos de carácter personal. Cualquier información concerniente a personas físicas identificadas o identificables. Ley Orgánica 3/2018.

Gestión de incidentes. Plan de acción para atender a las incidencias que se den. Además de resolverlas debe incorporar medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas.

Gestión de riesgos. Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.

Incidente de seguridad. Suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información.

Información. Caso concreto de un cierto tipo de información.

Política de seguridad. Conjunto de directrices plasmadas en documento escrito, que rigen la forma en que una organización gestiona y protege la información y los servicios que consideran críticos.

Principios básicos de seguridad. Fundamentos que deben regir toda acción orientada a asegurar la información y los servicios.

Responsable de la información. Persona que tiene la potestad de establecer los requisitos de una información en materia de seguridad.

Responsable de la seguridad. El responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

Responsable del servicio. Persona que tiene la potestad de establecer los requisitos de un servicio en materia de seguridad.

Responsable del sistema. Persona que se encarga de la explotación del sistema de información.

Servicio. Función o prestación desempeñada por alguna entidad oficial destinada a cuidar intereses o satisfacer necesidades de los ciudadanos.

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.