Política de Seguridad de la Información, de Redes y Protección de Datos

2021

HISTORIAL DE CAMBIOS

Nombre del fichero	Versión	Resumen de cambios producidos	Fecha
STIC – 01 - Política de Seguridad de la Información, Redes y Protección de Datos	1.00	Primera versión.	18/03/2021
STIC – 01 – Política de Seguridad de la Información, Redes y Protección de Datos	2.00	Adecuación a la Directiva NIS.	09/04/2021
STIC – 01 – Política de Seguridad de la Información, Redes y Protección de Datos	2.01	Ajustes sin relevancia en el apartado 3-Legislación y normativa de referencia (cambio de orden de legislación).	23/06/2021

CLASIFICACIÓN

INFORMACIÓN PÚBLICA
Nota de confidencialidad: La información contenida en este documento es INFORMACIÓN PÚBLICA. Es responsabilidad del Área o Departamento receptor de este documento su distribución interna en base a la necesidad de conocer la información aquí contenida.

CONTROL DE DIFUSIÓN

AUTOR/ES: Ingeniería e Integración Avanzadas (Ingenia), S.A.
DISTRIBUCIÓN: **Aguas de Cádiz S.A.**

Índice

1 Introducción

Agua de Cádiz S.A. (en adelante, ACASA), como muestra de compromiso con la seguridad de la información de sus sistemas[1] ha desarrollado la presente Política de Seguridad de la Información, de Redes y Protección de Datos, en adelante **Política de Seguridad**, de conformidad con lo establecido en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (en adelante ENS) en el ámbito de la Administración Electrónica e incluye, asimismo, los principios básicos que permiten garantizar el cumplimiento de la legislación en materia de protección de datos vigente acorde con el Reglamento UE 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, en adelante RGPD, así como la Ley Orgánica 3/2018 de Protección de Datos de Carácter Personal y garantía de derechos digitales y el Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

La **Política de Seguridad** es una declaración ética, responsable y de estricto cumplimiento en ACASA, la cual es desplegada a través de las diferentes Normativas y Procedimientos con los que se procura que los riesgos sean tratados adecuadamente.

El uso de los activos de información debe estar en consonancia con las buenas prácticas y procedimientos de trabajo profesionales, así como con los requisitos legales, reglamentarios y contractuales, que deben garantizar la Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad de la información y de los servicios.

1 Sistema de información: Conjunto de aplicaciones software, datos, plataformas, equipamiento, locales, personal y otro tipo de elementos que permiten alojar, tratar y administrar información por parte de usuarios para la consecución de un fin.

2 Objetivo y ámbito de aplicación

- Este documento constituye el establecimiento de un marco organizativo y tecnológico en ACASA.
- Se entenderá la Seguridad de la información como un proceso integral constituido por todos los elementos técnicos, humanos y materiales, y organizativos relacionados con los sistemas de información, quedando excluidas cualquier tipo de actuaciones puntuales o de tratamiento coyuntural.
- Debe ser conocida y cumplida por todo el personal de ACASA, independientemente del puesto, cargo y responsabilidad dentro de la misma.

3 Legislación y normativa de referencia

El marco normativo de las actividades de ACASA en el ámbito de esta **Política de Seguridad** está integrado por las siguientes normas:

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Ley 7/1985, de 2 de abril, reguladora de las bases del régimen local.
- Real Decreto Legislativo 1/2010, de 2 de julio, por el que se aprueba el texto refundido de la Ley de Sociedades de Capital.
- 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.
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- 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.
- Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

- Reglamento Europeo de Firma Electrónica (eIDAS). Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo.
- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
- Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

4 Principios y directrices

Los principios que deben contemplarse a la hora de garantizar la seguridad de la información son la prevención, la detección, la respuesta y la recuperación, de manera que las amenazas existentes no se materialicen o en caso de materializarse no afecten gravemente a la información que maneja, o los servicios que se prestan.

4.1 Prevención

Se debe evitar, o al menos prevenir en la medida de lo posible, que la información, los servicios o redes se vean perjudicados por incidentes de seguridad. Para ello deberán implementarse las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, los departamentos deben:

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

4.2 Detección

Dado que los servicios y redes se pueden degradar rápidamente debido a incidentes, que van desde una simple ralentización hasta su detención, se debe monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS.

Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

4.3 Respuesta

Se deben:

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

4.4 Recuperación

Para garantizar la disponibilidad de los servicios críticos, se deben desarrollar planes de continuidad de los sistemas TIC y actividades de recuperación.

4.5 Otros principios generales:

- El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado.
- La información debe ser protegida contra accesos y alteraciones no autorizados, manteniéndola confidencial e íntegra.
- La información debe estar disponible, permitiendo su acceso autorizado, siempre que sea necesario.
- La Seguridad de la Información debe comprometer a todos los miembros de ACASA, sin excepción. Por lo tanto, es responsabilidad de todos. Todas las personas que tienen acceso a la información de ACASA deben protegerla, por lo que deben estar adecuadamente formadas y concienciadas.

- La Seguridad de la Información no es algo estático, debe ser constantemente controlada y periódicamente revisada.
- Todos aquellos activos (infraestructura, redes, soportes, sistemas, comunicaciones, etc.) donde reside la información, viaja o es procesada, deben estar adecuadamente protegidos.
- Las medidas de seguridad que se implanten deben estar en proporción a la criticidad de la información que protejan y a los daños o pérdidas que se pueden producir en ella. En todo momento se seguirá como mínimo las medidas de seguridad impuestas por el ENS, así como las guías CCN-STIC elaboradas por el Centro Criptológico Nacional del Centro Nacional de Inteligencia.
- El tratamiento de datos de carácter personal debe estar siempre de acuerdo con las leyes aplicables en cada momento, siendo especialmente importantes el Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.

5 Organización de la Seguridad de la Información

La estructura organizativa de la gestión de la seguridad de la información en el ámbito de la seguridad de la información y redes de ACASA está compuesta por los siguientes agentes:

a) El Comité de Gestión de la Seguridad de la Información.
b) El Responsable de Seguridad.
c) El Responsable de la Administración de la Seguridad
d) Responsables de la Información y de los Servicios.
e) Responsables del Sistema de Información.
f) Delegado de Protección de Datos.
g) Responsable del Tratamiento.
h) Responsables funcionales del Tratamiento.

La implementación de esta organización está en el marco normativo cubierto por el establecimiento de un sistema de Gestión de la Seguridad, basado en el ENS.

5.1 Comité de Gestión de la Seguridad de la Información

Para la gestión de la Seguridad de la Información, se crea el Comité de Gestión de la Seguridad de la Información, en adelante el Comité de Seguridad, dentro del ámbito de la presente **Política de Seguridad** formado por un equipo multidisciplinar que coordinará las actividades y controles de seguridad establecidos en ACASA y que vela por el cumplimiento de la normativa vigente, interna y externa, en materia de protección de datos de carácter personal y seguridad.

Son funciones del Comité de Seguridad las siguientes:

a) Identificar los objetivos de ACASA en el ámbito de la Seguridad de la Información.
b) Elaborar la **Política de Seguridad**, establecer los criterios de revisión de la misma, revisarla, distribuirla y velar por su cumplimiento.
c) Promover y respaldar los planes de acción e iniciativas que garanticen la implantación de la **Política de Seguridad** en ACASA.
d) Establecer los requisitos de seguridad que deben cumplir a nivel organizativo, técnicos y de control, los sistemas y servicios de ACASA.
e) Garantizar que la seguridad forma parte del proceso de planificación de la gestión de la información y como proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información.
f) Comunicar a los terceros que colaboren en la explotación de los sistemas de información la realización de la misma conforme a los exigidos en el ENS.
g) Aprobar los nombramientos de responsables y responsabilidades en materia de seguridad de la información.
h) Valorar el grado de conformidad de los procedimientos implantados en ACASA con las normas definidas en la política, estableciendo planes de mejora para aquellos que requieran de una modificación para su conformidad.
i) Aprobar y supervisar las normativas y procedimientos de seguridad que se definan para dar cumplimiento y desarrollo a la **Política de Seguridad**.
j) Acordar y aprobar metodologías y procesos específicos relativos a la Seguridad de la Información.
k) Verificar que todas las acciones llevadas a cabo en materia de Seguridad sean compatibles o se encuentren respaldadas por la **Política de Seguridad**.
l) Promover la realización de auditorías periódicas que permitan verificar el cumplimiento de las obligaciones de las Administraciones en materia de Seguridad.
m) Promover la formación y concienciación en materia de Seguridad de la Información a todo el personal.
n) Mantener contactos periódicos con grupos, otras entidades, organismos, foros, etc. que resulten de interés en el ámbito de la Seguridad de la Información, compartiendo experiencias y conocimiento que ayuden a mejorar y mantener la seguridad de los sistemas de ACASA.
o) Valorar y evaluar los recursos necesarios para dar soporte al proceso de planificación e implantación de la seguridad en ACASA.

El Comité de Seguridad, se reunirá con carácter ordinario, al menos una vez al año, pudiéndose reunir de manera extraordinaria, por razones de urgencia y causa justificada, en periodos inferiores.

Para la celebración de las reuniones del Comité de Seguridad será preciso la presencia de, al menos, el 51% de los miembros permanentes.

5.2 Responsable de Seguridad

Es el responsable de que los servicios, las redes y sistemas de información de ACASA se mantengan con el mayor grado de seguridad atendiendo a los principios de:

a) *Confidencialidad*: la información asociada a los servicios electrónicos al ciudadano y las redes, solo debe poder ser conocida por las personas autorizadas para ello.
b) *Integridad*: la información asociada a los servicios electrónicos al ciudadano y las redes, no debe ser alterada por personas no autorizadas.
c) *Disponibilidad*: garantía de que los usuarios autorizados tengan acceso a la información, a las redes y a los recursos relacionados con la misma siempre que lo requieran, así como garantía de que los servicios relativos a la Administración Electrónica permanecerán disponibles.

Son funciones del Responsable de Seguridad:

a) Supervisar el cumplimiento de la presente Política, normativas y procedimientos derivados de la misma, para la protección de los sistemas de información y seguridad de las redes, así como llevar controles periódicos.
b) Asesorar en materia de seguridad a los integrantes de ACASA que así lo requieran.
c) Coordinar la interacción con otros organismos especializados y autoridades de supervisión.
d) Tomar conocimiento y supervisar la investigación y monitorización de los incidentes de seguridad.
e) Establecer las medidas de seguridad, adecuadas y eficaces para cumplir los requisitos de seguridad establecidos por los Responsables de los Servicios y de la Información, siguiendo en todo momento lo exigido en el Anexo II del ENS.
f) Se tiene que documentar en la declaración de aplicabilidad las medidas de seguridad en el cumplimiento del ENS, RGPD, LOPDgdd, la Directiva NIS, Real Decreto-ley 12/2018, de 7 de septiembre y Real Decreto 43/2021, de 26 de enero. Dicho documento, deberá remitirse a la autoridad competente respectiva, de acuerdo a las exigencias del Real Decreto 43/2021, en el plazo establecido en el mismo.
g) Asesorar, en colaboración con el Responsable del Sistema, los Responsables de las redes, los Responsables de los Servicios y de la Información en la realización de los análisis y gestión de riesgos, elevando el informe resultante al Comité de Seguridad.

   El análisis y gestión de riesgos tiene que contemplar los riesgos de seguridad detectados para la correcta la protección de los sistemas de información y seguridad de las redes, teniendo en cuenta el cumplimiento del ENS, LOPDgdd, RGPD y la Directiva NIS, Real Decreto-ley 12/2018, de 7 de septiembre y Real Decreto 43/2021, de 26 de enero.
h) Promover las actividades de concienciación y formación en materia de seguridad en su ámbito de responsabilidad, siguiendo las directrices del Comité de Seguridad. El ámbito se extiende al

cumplimiento del (ENS, RGPD, LOPDgdd, la Directiva NIS, Real Decreto-Ley 12/2018, de 7 de septiembre y Real Decreto 43/2021, de 26 de enero).

i) Habilitar y mantener un registro de incidencias para la información que esté bajo su responsabilidad. Este registro deberá estar disponible para cualquier revisión o auditoría, ante el Comité de Seguridad, entidad auditora y/o autoridad CSIRT de referencia.
j) Asegurar que los contratos de prestación de servicios disponga de cláusulas de seguridad y de materia de protección de datos, para proteger las redes y/o sistemas de información.
k) Asegurar que se mantiene un listado actualizado del personal autorizado a acceder a los sistemas de información (automatizados o no automatizados) y/o comunicación.
l) Asegurar que se autorice los permisos de acceso a los usuarios sobre los recursos, (automatizados y no automatizados) que se encuentran bajo su responsabilidad y que sean estrictamente necesarios para el desarrollo de las funciones del trabajador.
m) Revisar los permisos y perfiles de acceso de la información que se encuentra bajo su gestión.
n) Analizar los informes de auditoría y proponer al responsable del tratamiento, responsable del sistema de redes y sistemas de información, responsable del servicio/información las medidas correctoras oportunas.

Respecto a la documentación:

a) Preparar los temas a tratar en las reuniones del Comité de Seguridad, aportando información puntual para la toma de decisiones.
b) Aprobar y proponer al Comité de Seguridad la documentación de seguridad de segundo nivel (Normativas y Procedimientos de Seguridad) de obligado cumplimiento.
c) Supervisar la documentación de tercer nivel (Procedimientos de Seguridad) de obligado cumplimiento.
d) Mantener la documentación organizada y actualizada, gestionando los mecanismos de acceso a la misma.

Respecto a la protección de datos de carácter personal:

a) Garantizar la seguridad de los datos, implantando y haciendo cumplir las medidas, procedimientos, instrucciones y normativas establecidas en el Manual jurídico definido en ACASA, así como sus anexos.
b) Colaborar con el responsable del tratamiento en la difusión del Manual jurídico y de sus anexos.
c) Mantener un listado actualizado del personal autorizado a acceder a los sistemas de información.
d) Realizar los controles periódicos establecidos para verificar el cumplimiento del Manual jurídico y de sus anexos.
e) Analizar los informes de auditoría y proponer al responsable del tratamiento las medidas correctoras oportunas.

f) Cumplir con el procedimiento de ejercicio de derechos de los interesados según las solicitudes recibidas.
g) Autorizar permisos de acceso a los usuarios sobre los recursos, (automatizados y no automatizados) que se encuentran bajo su responsabilidad y que sean estrictamente necesarios para el desarrollo de las funciones del trabajador.
h) Realizar un inventario y un registro de entrada y salida de soportes.
i) Autorizar la salida de soportes con datos personales que se encuentren bajo su responsabilidad.
j) Autorizar la generación de copias o reproducción de documentos.
k) Mantener un listado de personal autorizado a la información (automatizada o no automatizada).
l) Revisar los permisos y perfiles de acceso de la información que se encuentran bajo su gestión.
m) Autorizar la recuperación de datos tratados.
n) Habilitar y mantener un registro de incidencias para la información que esté bajo su responsabilidad. Este registro deberá estar disponible para cualquier revisión o auditoría.

Respecto a la Directiva NIS:

a) Actuar como punto de contacto único y coordinación con las autoridades competentes, tanto para la evaluación de las medidas de seguridad implantadas como para la notificación de posibles incidentes.
b) Elaborar y proponer para su aprobación dentro de la organización las políticas de seguridad necesarias para el cumplimiento de esta normativa (establecido en el art. 6.2 del Real Decreto).
c) Supervisión de la aplicación y revisión tanto de las políticas como de las medidas de seguridad.
d) Actuar como capacitador de buenas prácticas en seguridad de las redes y sistemas de información, tanto en aspectos físicos como lógicos.
e) Aprobar el documento de Declaración de Aplicabilidad con las medidas de seguridad.
f) Se abre la posibilidad de que este Responsable sea asesorado y reciba soporte por parte de un tercero experto.
g) Remitir a la autoridad competente, a través del CSIRT de referencia y sin dilación indebida, las notificaciones de incidentes que tengan efectos perturbadores en la prestación de los servicios a los que se refiere el artículo 19.1 del Real Decreto-ley 12/2018, de 7 de septiembre.
h) Recibir, interpretar y supervisar la aplicación de las instrucciones y guías emanadas de la autoridad competente, tanto para la operativa habitual como para la subsanación de las deficiencias observadas.
i) Recopilar, preparar y suministrar información o documentación a la autoridad competente o el CSIRT de referencia, a su solicitud o por propia iniciativa.

El Responsable de Seguridad es la figura que determina las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos. Deberá ser una persona física, unidad u órgano colegiado,

jerárquicamente superior e independiente del Responsable del Sistema de Información y del Responsable de las redes.

El Responsable de Seguridad será nombrado y cesado por el Comité de Seguridad.

5.3 Responsable de la Administración de la Seguridad

Son funciones generales del Responsable de Administración de la Seguridad del ENS de ACASA:

a) Asesorar en materia de seguridad a los integrantes de ACASA que así lo requieran.
b) Comunicar a los empleados correspondientes las conclusiones de los informes derivados de las incidencias que afecten a los Sistemas de Información, así como de cualquier amenaza que se haya producido en ACASA.
c) Colaborar con el resto de las figuras nombradas, para elaborar los informes de incidentes que se han de reportar al Comité de Seguridad, en sus revisiones periódicas.
d) Asegurar el cumplimiento de las medidas de seguridad establecidas en ACASA en cumplimiento del ENS.
e) Asegurar el cumplimiento de los procedimientos técnicos y organizativos de ACASA.
f) Organizar la realización del análisis y gestión de riesgos en coordinación con el Responsable de Seguridad, Responsable del Sistema y Responsables de la información y de los servicios.
g) Realizar el seguimiento del plan de mejora de la seguridad de la información.
h) Elaborar el documento de Declaración de Aplicabilidad de medidas de seguridad.
i) Revisar e incluir, en los contratos de prestación de servicios, las cláusulas que establezcan las obligaciones de las empresas de servicios en materia de seguridad de los datos.
j) Colaborar con el Responsable de Seguridad en la preparación de las reuniones del Comité de Seguridad.
k) Colaborar con el resto de las figuras nombradas para recopilar las últimas versiones de las normativas y procedimientos de seguridad de ACASA en materias de seguridad.
l) Adoptar medidas oportunas para que todo el personal conozca las normas de seguridad que afecten el desarrollo de sus funciones y las consecuencias en que pueden incurrir en caso de incumplimiento.
m) Notificar al Responsable de Seguridad cualquier modificación de la que tenga constancia en la estructura y el tratamiento de datos de los sistemas de información.
n) Asegurar el cumplimiento de los procedimientos técnicos y organizativos de ACASA.

o) Revisar los permisos de acceso a los usuarios sobre los recursos (automatizados y no automatizados) que sean estrictamente necesarios para el desarrollo de las funciones del trabajador. Todo ello siguiendo los procedimientos establecidos en ACASA.
p) Realizar un inventario y un registro de los soportes de información, independientemente de los datos que contengan.
q) Controlar periódicamente que se cumplen las normas y procedimientos relativos a la gestión de soportes, así como a las copias de seguridad y recuperación de datos.

Respecto a la protección de datos de carácter personal:

a) Analizar los informes derivados de las incidencias que afecten de manera grave a los Sistemas de Información.
b) Analizar las incidencias cuya resolución requiera la recuperación de ficheros, tablas u otras estructuras de almacenamiento desde las copias de seguridad.
c) Notificar las violaciones de seguridad de los datos personales en los términos exigidos por el RGPD a la Autoridad de Control competente.
d) Supervisar el adecuado cumplimiento del Documento de Seguridad y verificar periódicamente la aplicación del mismo en los aspectos que le compete.
e) Analizar las medidas correctoras a implantar, derivadas de los informes de auditoría que se realicen en materia de seguridad de datos de carácter personal.
f) Informar respecto a las demandas de cesión de datos a terceras personas.
g) Llevar a cabo, cuando sea necesario, las Evaluaciones de Impacto de las actividades de tratamiento que lo requieran
h) Concienciar a los usuarios y verificar su actividad para que éstos informen de la creación de ficheros temporales y para que eliminen periódicamente los ficheros temporales de los ordenadores personales y de sus carpetas en los servidores.
i) Incluir, en los contratos de prestación de servicios que impliquen acceso a datos de carácter personal, las cláusulas que establezcan las obligaciones de las empresas de servicios en materia de seguridad de los datos.
j) Dictar normas específicas y supervisar las relaciones de Aguas de Cádiz con empresas externas que vayan a efectuar el mantenimiento de los sistemas.
k) Elaborar y modificar en su caso el Documento de Seguridad para proponerlo a aprobación del Responsable del Tratamiento, así como implantar las medidas y los procedimientos técnicos y organizativos recogidos en el mismo.

l) Notificar al Responsable del Tratamiento y al Delegado de Protección de Datos cualquier modificación que se produzca en la estructura y el tratamiento de datos de los sistemas de información.

m) Garantizar que se incluya en los formularios, documentos, impresos o cualquier medio de recogida de datos personales el texto informativo correspondiente para cumplir con el deber de información al interesado.

n) Elaborar un Registro de Actividades de Tratamiento y mantenerlo actualizado en todo momento.

o) Recibir y valorar las notificaciones de los Responsables Internos de los Tratamientos, respecto de las modificaciones que se produzcan en la estructura de los sistemas de información, con objeto de proceder a la actualización del Documento.

p) Dar respuesta a las necesidades de protección de información de la organización en forma de recomendaciones.

q) Recibir y valorar las nuevas exigencias legales que vayan surgiendo y que pueden repercutir en las medidas de seguridad implantadas en la organización.

r) Supervisar las altas, modificaciones y bajas de usuarios con acceso autorizado a los tratamientos que contengan datos personales y los perfiles de los mismos.

s) Supervisar la conducta de los usuarios en el cumplimiento de sus obligaciones, surgidas con respecto a lo que se señala en el Documento de Seguridad.

t) Velar por la existencia y veracidad de una relación actualizada de usuarios con acceso autorizado a los Sistemas de Información.

u) Revisar las autorizaciones de la salida, fuera de Aguas de Cádiz, de soportes informáticos con datos de carácter personal.

v) Verificar que las empresas externas aplican las medidas necesarias para garantizar la seguridad de los tratamientos y ficheros de datos de carácter personal, cualquiera que sea el soporte utilizado.

w) Autorizar la salida de copias de seguridad que contengan datos personales del almacenamiento de seguridad.

x) Controlar periódicamente las normas y procedimientos relativos a las copias de seguridad y recuperación a través de su auditoría y prueba periódica, al menos dos veces al año.

Respecto a la Directiva NIS:

a) Desarrollar la aplicación de las políticas de seguridad, normativas y procedimientos derivados de ACASA supervisar su efectividad y llevar a cabo controles periódicos de seguridad.

b) Apoyar al Responsable de Seguridad para recopilar la información de gestión de incidentes para su posterior reporte a CSIRT.

c) Supervisar la aplicación de las instrucciones y guías emanadas de la autoridad competente, tanto para la operativa habitual como para la subsanación de las deficiencias observadas.

d) Colaborar con el Responsable de Seguridad para recopilar, preparar y suministrar información o documentación a la autoridad competente o el CSIRT de referencia, a su solicitud o por propia iniciativa.
e) Colaborar en la recogida de evidencias de las notificaciones de incidentes que tengan efectos perturbadores en la prestación de los servicios a los que se refiere el artículo 19.1 del Real Decreto-ley 12/2018, de 7 de septiembre.
f) Elaborar el documento de Declaración de Aplicabilidad de medidas de seguridad considerado en el artículo 6.3 párrafo segundo de este real decreto 43/2021 de 26 de enero.
g) Apoyar en la elaboración de buenas prácticas en seguridad de las redes y sistemas de información, tanto en aspectos físicos como lógicos.
h) Actuar como capacitador de buenas prácticas en seguridad de las redes y sistemas de información, tanto en aspectos físicos como lógicos.
i) Garantizar que los proveedores externos tomen las medidas necesarias cuando las redes y/o sistemas de información aplicables sean suyos o sean gestionados por ellos. Este es un punto importante, ya que al igual que en otras regulaciones como el RGPD, se impone un nivel de responsabilidad a nivel regulatorio sobre las Compañías respecto a sus proveedores críticos en materia de redes y sistemas de información.
j) En el caso de que ACASA esté siendo revisada por la autoridad competente, para determinados casos debido a su tamaño o complejidad, ésta podrá pedir a la empresa un Informe de Auditoría presentado por una entidad externa e independiente.

Respecto a medidas de seguridad:

a) Supervisar que la gestión de los permisos de acceso a la información de los usuarios siguen los procedimientos establecidos por ACASA. Para ello en coordinación con el Responsable de Seguridad, deberán revisar los permisos y perfiles de acceso de la información con cierta periodicidad.
b) Supervisar que el registro de entrada y salida de soportes de información se utiliza de acuerdo a lo dispuesto en las normativas y procedimientos internos.
c) Supervisar que la contratación de servicios que impliquen el tratamiento de información cumple con lo exigido en el ENS.

Respecto a las auditorías:

a) Colaborar en los procesos de auditoría de cumplimiento de Protección de Datos en cuanto a las medidas de seguridad desplegadas en ACASA.
b) Acompañar y colaborar activamente en los procesos de auditoría de cumplimiento del ENS
c) Supervisar el cumplimiento de ejecución de las medidas correctivas derivadas de los informes de auditoría del ENS

d) Establecer el Plan de auditorías que se ha de realizar en Aguas de Cádiz, tanto para los tratamientos automatizados como para los no automatizados con datos de personales y cuantas otras medidas, lógicas, de seguridad, físicas, etc. deban incluirse.
e) Llevar a cabo la auditoría, bien con personal interno de ACASA o con personal externo.
f) Analizar el informe de auditoría y proponer las medidas para solventar las anomalías y deficiencias detectadas, así como las modificaciones pertinentes en el presente documento.

5.4 Responsables de la Información y de los Servicios

Esta responsabilidad recaerá en el titular del órgano o unidad administrativa que gestione cada procedimiento administrativo, pudiendo una misma persona acumular las responsabilidades de la información de todos los procedimientos que gestione.

Son los responsables de clasificar la información conforme a los criterios y categorías establecidas en el ENS y en cada una de las dimensiones de seguridad conocidas y aplicables, dentro del marco establecido en el Anexo I del ENS.

Son los responsables de determinar los niveles de seguridad de los servicios en cada dimensión de seguridad dentro del marco establecido en el Anexo I del ENS y en cada una de las dimensiones de seguridad conocidas y aplicables (disponibilidad, autenticidad, trazabilidad, confidencialidad e integridad).

Son los encargados, contando con la participación y asesoramiento del Responsable de Seguridad y del Responsable del Sistema de Información, de realizar los preceptivos análisis de riesgos, y de seleccionar las salvaguardas a implantar.

Son los responsables de aceptar los riesgos residuales calculados en el análisis de riesgos y de realizar su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

Los responsables de información y de los servicios son establecidos en el Plan Director de Seguridad[2], el cual contiene la planificación de actuaciones destinadas a subsanar las insuficiencias detectadas, para el cumplimiento del ENS.

Los responsables de información y de los servicios son nombrados y cesados por el Comité de Seguridad.

[2] Plan Director de Seguridad: Es la relación de acciones que debe acometer ACASA para el cumplimiento de la norma y reducir su nivel de riesgos, así como gestionar el riesgo de seguridad.

5.5 Responsable del Sistema de Información

Personal designado cuyas responsabilidades son:

a) Desarrollo, operación y mantenimiento de las redes y del sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
b) Garantizar que las medidas de seguridad se integren adecuadamente dentro del marco general de las redes y de la Seguridad de la Información.
c) Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.
d) Elaborar procedimientos de seguridad de las redes y de los sistemas de información.
e) Elaborar planes de continuidad de las redes y de los sistemas de información.

Podrá acordar la suspensión del manejo de determinada 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 deberá ser acordada con el Responsable de la Información y servicios afectados, y el Responsable de Seguridad antes de ser ejecutada.

El responsable del Sistema de Información es nombrado y cesado por el Comité de Seguridad. Por regla general, será el departamento de Informática, pudiendo delegar en los responsables de cada uno de los sistemas afectados.

5.6 Delegado de Protección de Datos

El Delegado de Protección de Datos será único para todos los órganos y organismos de ACASA y se informará de su nombramiento y cese a la Agencia Española de Protección de Datos (AEPD).

Son funciones del Delegado de Protección de Datos:

- Informar y asesorar a ACASA y a todos los empleados que se ocupen del tratamiento de datos personales, de las obligaciones que se deriven del Reglamento General de Protección de Datos y de otras disposiciones relacionadas con la protección de datos.
- Supervisar el cumplimiento del Reglamento General de Protección de Datos en ACASA.
- Asesorar acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.
- Cooperar con la Autoridad de control.

- Actuar como punto de contacto de la Autoridad de Control.

Además, asesorará y supervisará en las siguientes áreas:

- Cumplimiento de principios relativos al tratamiento, como los de limitación en la finalidad, minimización o exactitud de los datos.
- Identificación de las bases jurídicas de los tratamientos.
- Valoración de compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos.
- Existencia de normativa sectorial que pueda determinar condiciones de tratamiento específicas distintas de las establecidas por la normativa general de protección de datos.
- Diseño e implantación de medidas de información a los afectados por los tratamientos de datos.
- Establecimiento de mecanismos de recepción y gestión de solicitudes de ejercicio de derechos por parte de los interesados.
- Valoración de las solicitudes de ejercicio de derechos por parte de los interesados.
- Contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación de ACASA – encargado de tratamiento.
- Identificación de los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de ACASA y de las razones que justifiquen la transferencia.
- Diseño e implantación de políticas de protección de datos.
- Auditorías de protección de datos.
- Establecimiento y gestión de los registros de actividades de tratamiento.
- Análisis de riesgo de los tratamientos realizados.
- 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.
- Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos.
- Establecimiento de 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.
- Determinación de la necesidad de realización de evaluaciones de impacto sobre la protección de datos.
- Realización de evaluaciones de impacto sobre la protección de datos.
- Relaciones con las autoridades de supervisión.
- Implantación de programas de formación y sensibilización del personal de ACASA en materia de protección de datos.

El Delegado de Protección de Datos es nombrado y cesado por el Comité de Seguridad.

5.7 Responsable del Tratamiento

El responsable del tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determina los fines y medios del tratamiento.

El responsable del tratamiento debe, entre otras cosas:

- Garantizar la observancia de los principios relativos al tratamiento y aprobar la política, normativa y procedimientos concernientes a la protección de datos personales.
- Designar a quien ejerza como Responsable de Seguridad, quien deberá coordinar y controlar las medidas de seguridad definidas.
- Designar al Delegado de Protección de Datos, cuando corresponda.
- Adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos personales y evitar su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural. En particular, difundirá entre el personal las normas de seguridad que afecten al desarrollo de sus funciones, así como las consecuencias en que pudieran incurrir en caso de incumplimiento.
- Garantizar el cumplimiento de las políticas y normativas aprobadas e implementadas en ACASA.
- Asegurar que la realización de tratamientos por cuenta de terceras partes esté regulada en un contrato, que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que la persona encargada del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará (ni siquiera para su conservación) a otras personas.
- Adoptar las medidas correctoras adecuadas.

5.8 Responsables funcionales del Tratamiento

El Responsable funcional del tratamiento es la persona física sobre la que recae las funciones del Responsable del tratamiento en uno o más tratamientos concretos de ACASA. En concreto son funciones del Responsable funcional del tratamiento:

- Garantizar la observancia de los principios relativos al tratamiento.
- Garantizar el cumplimiento de las medidas técnicas y organizativas definidas.
- Garantizar el cumplimiento de las políticas y normativas aprobadas e implementadas en ACASA.
- Asegurar que la realización de tratamientos por cuenta de terceras partes esté regulada en un contrato, que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que la persona encargada del tratamiento únicamente tratará los datos

conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará (ni siquiera para su conservación) a otras personas.

- Adoptar las medidas correctoras adecuadas.

Los Responsables Funcionales del Tratamiento son nombrados y cesados por el Comité de Seguridad.

5.9 Resolución de conflictos

Los conflictos entre las diferentes personas, unidades u órganos responsables que componen la estructura organizativa de la Política de Seguridad, serán resueltos por el superior jerárquico común, que podrá elevar consulta previa al Comité de Seguridad. En caso de conflicto prevalecerán las decisiones del Consejo de Administración.

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

5.10 Obligaciones del Personal

Todo el personal, interno y externo de ACASA, tiene la obligación de conocer y cumplir la presente **Política de Seguridad**, las normativas y procedimientos derivados de la misma, tales como las relativas a la protección de datos de carácter personal, siendo responsabilidad del Comité de Seguridad disponer de los mecanismos necesarios para que la información llegue a todo el personal indicado.

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

6 Asesoramiento especializado en materia de seguridad

6.1 Asesoramiento especializado

El Responsable de Seguridad será el encargado de coordinar los conocimientos y las experiencias disponibles en ACASA con el fin de proporcionar ayuda en la toma de decisiones en materia de seguridad de las redes y sistemas de información, pudiendo obtener asesoramiento de otros organismos.

6.2 Cooperación entre organismos y otras Administraciones Públicas

A efectos de intercambiar experiencias y obtener asesoramiento para la mejora de las prácticas y controles de seguridad, ACASA mantendrá contactos periódicos con organismos y entidades especializadas en temas de seguridad de la información y de redes.

6.3 Revisión independiente de la Seguridad de la Información

El Comité de Seguridad propondrá la realización de revisiones periódicas independientes sobre la vigencia e implementación de la **Política de Seguridad** con el fin de garantizar que las prácticas en ACASA reflejan adecuadamente sus disposiciones.

7 Protección de Datos de Carácter Personal

Para el tratamiento de datos de carácter personal en los sistemas de información se seguirá en todo momento lo desarrollado en el documento de seguridad y su documentación asociada conforme a lo exigido en el Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), así como lo establecido en la Ley 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales.

8 Formación y concienciación

El objetivo es lograr la plena conciencia respecto a que la Seguridad de la Información y de las redes, que afecta a todo el personal de ACASA y a todas las actividades de acuerdo al principio de seguridad integral recogido en el art. 5 del ENS y en el art. 6.2 del Real Decreto 43/2021. A estos efectos, ACASA propondrá y organizará sesiones formativas y de concienciación para que todas las personas que intervienen en el proceso y sus responsables jerárquicos tengan una sensibilidad hacia los riesgos que se corren.

9 Análisis y gestión de riesgos

ACASA asume el compromiso de controlar los riesgos de seguridad, así como dar cumplimiento a la legislación y normas internas vigentes bajo un proceso de mejora continua conforme a los marcos y metodologías existentes en la actualidad.

Para ello, con el objetivo de conocer el nivel de exposición de los activos de información (servicios, infraestructuras, redes, sistemas de información, terceros o proveedores) a los riesgos y amenazas en materia de seguridad, los Responsables de los Sistemas de Información y de las redes realizarán, con

periodicidad al menos anual, análisis de riesgos cuyas consecuencias se plasmarán en actuaciones para tratar y mitigar el riesgo, o incluso, replantear la seguridad de los sistemas en caso necesario.

La descripción de la metodología y evaluación del riesgo están desarrollados en "Metodología de análisis y gestión de riesgos".

Se realizará un análisis de riesgos:

- Regularmente, una vez al año.
- Cuando haya cambios en los servicios esenciales prestados o cambios significativos en las redes y/o infraestructuras que los soportan.
- Cuando se vaya a iniciar o a modificar un tratamiento de datos de carácter personal, en línea a lo establecido en el Reglamento General de Protección de Datos. En estos casos se contemplarán en el alcance del análisis todos aquellos activos que intervengan en el tratamiento, considerando tanto activos relacionados con los sistemas de información, como humanos, locales o terceros.
- Cuando ocurra un incidente de seguridad grave.
- Cuando se identifiquen amenazas severas que no hubieran sido tenidas en cuenta o vulnerabilidades graves que no estén contrarrestadas por las medidas de protección implantadas.

A raíz de los resultados obtenidos en el análisis de riesgos se determinarán las medidas necesarias para proteger dichos datos y cuyas conclusiones serán elevadas al Responsable de Seguridad y éste lo hará al Comité de Seguridad.

10 Catálogo de medidas de seguridad organizativas, tecnológicas y físicas

La relación de medidas adoptadas se formalizará en un documento denominado Declaración de Aplicabilidad de medidas de seguridad.

Las medidas de seguridad, acorde a los riesgos analizados, que se toman como línea de base a implantar en la organización son las del Esquema Nacional de Seguridad.

11 Estructura normativa

La documentación relativa a la Seguridad de las redes y sistemas de Información, estará clasificada en cuatro niveles, de manera que cada documento de un nivel se fundamenta en los de nivel superior:

- Primer nivel: Política de Seguridad.
- Segundo nivel: Normativas y Procedimientos de Seguridad.
- Tercer nivel: Procedimientos Técnicos de Seguridad.

- Cuarto nivel: Informes, registros y evidencias electrónicas.

11.1 Primer nivel: Política de Seguridad

Documento de obligado cumplimiento por todo el personal, interno y externo de ACASA, recogido en el presente documento y aprobado mediante resolución de la Dirección.

11.2 Segundo Nivel: Normativas de Seguridad

De obligado cumplimiento de acuerdo al ámbito organizativo, técnico o legal correspondiente.

La responsabilidad de aprobación de los documentos redactados en este nivel será competencia de Comité de Seguridad, a propuesta del Responsable de Seguridad.

11.3 Tercer Nivel: Procedimientos de Seguridad

Documentos orientados a resolver las tareas, consideradas críticas por el perjuicio que causaría una actuación inadecuada, de seguridad, desarrollo, mantenimiento y explotación de las redes y de los sistemas de información.

La responsabilidad de aprobación de estos procedimientos es del Responsable de Seguridad, a propuesta del Responsable del Sistema y del Responsable de las redes.

11.4 Cuarto Nivel: Informes, registros y evidencias electrónicas

Documentos de carácter técnico que recogen el resultado y las conclusiones de un estudio o una valoración; documentos de carácter técnico que recogen amenazas y vulnerabilidades de las redes y de los sistemas de información, así como también evidencias electrónicas generadas durante todas las fases del ciclo de vida de las redes y del sistema de información.

La responsabilidad de que existan este tipo de documentos es de cada uno de los Responsables de los Sistemas de Información y Responsables de las redes, en su ámbito.

11.5 Otra documentación

Se podrá seguir en todo momento los procedimientos, normas e instrucciones técnicas STIC, así como las guías CCN-STIC de las series 400, 500 y 600.

12 Anexo I. Requisitos de seguridad de obligado cumplimiento

Para la correcta implementación y cumplimiento de la presente **Política de Seguridad** es necesario aplicar una serie de requisitos de obligado cumplimiento:

12.1 Gestión de personal

En la normativa de seguridad referente a los recursos humanos se detalla la obligatoriedad de conocimiento y concienciación en materia de seguridad según sus responsabilidades. Los recursos necesarios para la implementación del sistema de seguridad, así como aquellos que lleven a cabo su operación, mantenimiento, supervisión, o tenga relación con el sistema se establece anualmente en los planes estratégicos de ACASA.

El Responsable de Recursos Humanos incluirá las funciones relativas a la seguridad de la información en las descripciones de puestos de trabajo, informará a todo el personal nuevo que ingrese en ACASA o cambie de ubicación de sus obligaciones con respecto del cumplimiento de la **Política de Seguridad**, gestionará las Cláusulas de Confidencialidad y coordinará las tareas de concienciación y formación respecto de la presente Política.

Periódicamente se realizarán evaluaciones de desempeño y seguimiento del personal. Asimismo, se capacitará al personal en buenas prácticas en seguridad de las redes y sistemas de información, tanto en aspectos físicos como lógicos.

12.2 Profesionalidad

En la normativa de seguridad referente a los recursos humanos se detallan las funciones, las responsabilidades del personal, así como los objetivos de las acciones de formación y concienciación.

Periódicamente se diseña un plan de formación específico en el que se tiene en cuenta las necesidades de profesionalización del sistema de seguridad.

12.3 Autorización y control de Acceso

El acceso a los sistemas de información y redes estará restringido y limitado a aquellos usuarios o procesos que lo necesiten para el desarrollo de su actividad y estén previamente autorizados.

El acceso a la información seguirá el principio de “necesidad de conocer”, de forma que los privilegios otorgados a cada entidad sean los mínimos imprescindibles para el desarrollo de su actividad.

La identificación de los usuarios será tal que se pueda conocer en todo momento quién recibe derechos de accesos y quién ha realizado alguna actividad, por lo que los identificadores deberán ser personales, no compartidos e intransferibles.

Todo ello se recoge en la normativa que se refiera al control de los accesos lógicos al sistema y la gestión de los usuarios.

Los lugares con acceso restringido igualmente deben estar controlados y previamente autorizados por los responsables asignados, tal y como se debe establecer en la normativa referente a la seguridad física del equipamiento de ACASA.

12.4 Protección de las instalaciones

Los sistemas de información deberán estar ubicados en zonas protegidas, con acceso restringido, habilitado únicamente al personal autorizado, tal y como se debe indicar en la normativa referente a la seguridad física del equipamiento y en la relativa al control de acceso físico al sistema y a las redes.

12.5 Adquisición de productos o servicios de seguridad.

Para el proceso de Adquisición, aceptación o autorización de nuevos componentes (productos y/o servicios de seguridad) se establecen protocolos de análisis de riesgos con proveedores y se mantienen actualizados los listados de proveedores habituales. Las adquisiciones deben ser autorizadas por los responsables del área implicada y el Área de Compras, tal y como se ha de indicar en la normativa en relación a la aceptación de nuevos componentes.

12.6 Seguridad por Defecto

Los sistemas, las aplicaciones y las redes se diseñarán y construirán bajo el principio de seguridad por defecto, de tal forma que:

- El sistema ofrecerá la funcionalidad mínima necesaria, y ninguna adicional. Cualquier función que no sea de interés o innecesaria será deshabilitada o no implementada.
- La operación y explotación de los sistemas estará limitada a aquellas personas o ubicaciones que se autoricen, quedando prohibidas para el resto.
- El uso del sistema ha de ser seguro, de tal forma que el uso inseguro requiera intención por parte del usuario.

La seguridad estará presente desde la concepción de un sistema o aplicación y permanecerá presente durante todo su ciclo de vida.

En la concepción de un nuevo sistema o aplicación, o modificación sustancial de un sistema o aplicación existentes, se contará siempre, y desde el inicio, con la participación del Responsable de Seguridad de la Información y el Responsable de las redes.

12.7 Integridad y actualización del sistema

Se deberán seguir en todo momento las informaciones acerca de las vulnerabilidades que afectan a los sistemas de información.

Se seguirán las recomendaciones de los fabricantes de equipos y software en cuanto a actualizaciones de seguridad, que deberán ser analizadas en cuanto a su idoneidad y conveniencia, y aplicadas en caso positivo con la menor dilación. Tal como se ha de especificar en la normativa referente al mantenimiento del software y en la referente a la contratación y las relaciones con terceros.

12.8 Protección de la Información Almacenada y en Tránsito

Se deberán proteger los entornos que contienen información almacenada y en tránsito entre entornos inseguros. En este sentido se deberán proteger convenientemente los equipos portátiles que puedan contener información, así como los soportes extraíbles (lápices de memoria, discos duros extraíbles, etc.) de acuerdo a los criterios de protección especificados en la normativa correspondiente acerca de la clasificación, etiquetado e intercambio de la información.

12.9 Registro de Actividad de los usuarios

Los sistemas, las aplicaciones y las redes generarán los registros de actividad necesarios para conocer la actividad en los sistemas, de forma que se pueda determinar en todo momento qué persona actúa, sobre qué datos, con qué operaciones y sus privilegios de acceso.

12.10 Gestión de Incidentes de Seguridad

ACASA definirá e implantará una normativa general en relación a la comunicación y la gestión de los incidentes, así como con procedimientos de respuesta a incidentes de seguridad con el objetivo de asegurar la correcta detección, gestión y respuesta efectiva que permita anular o minimizar el impacto del incidente en la información, las redes, los servicios, los empleados, los usuarios y, en general, en la actividad de ACASA.

Tal normativa contemplará la comunicación y notificación de los incidentes a los organismos receptores de dicha información, de acuerdo con la legalidad vigente.

12.11 Continuidad de Negocio

Para asegurar la disponibilidad de los servicios, las redes y los sistemas de información, ACASA diseñará e implantará Planes de Continuidad de Servicio que eviten las interrupciones de las actividades de ACASA y garanticen, ante una contingencia, la reanudación de los servicios, los sistemas de información y las redes a los niveles adecuados de operatividad.

12.12 Gestión de la Seguridad y Mejora Continua

Se deberá establecer un Sistema de Gestión de la Seguridad que permita conocer en cada momento el estado de la seguridad de las redes y los sistemas de información, mediante la definición y medida de indicadores, y permita, a su vez, tomar las decisiones informadas pertinentes para cumplir los requisitos de seguridad establecidos.

Se establecerá un proceso de mejora continua mediante el análisis de la situación, la implantación de nuevas medidas de seguridad, la mejora de las existentes y la aportación de mejoras sugeridas por el Comité de Seguridad y por toda ACASA en su conjunto.

12.13 Interconexión de sistemas

Se desplegarán las protecciones necesarias para proteger el perímetro de la red corporativa de ACASA, de forma que se neutralicen las posibles intrusiones procedentes de aquellas partes aquellas de la organización no implicadas en las provisiones del servicio esencial, del exterior, ya sea iniciadas malintencionadamente por terceros o como consecuencia de la interconexión con sistemas de terceros.

ACASA cuenta con normativas de seguridad que tratan sobre la protección de la red, donde se indican las directrices en cuanto a seguridad del perímetro, segmentación y redundancia.

ACASA, para asegurar la protección integral de su sistema de información, deberá salvaguardar el mismo de las posibles consultas o conexiones…que se realice desde partes aquellas de la organización no implicadas en las provisiones del servicio esencial, desde terceros organismos o instituciones al sistema de información de ACASA, así como proteger y asegurar que tales comunicaciones sean seguras.

13 Publicación de la Política de Seguridad

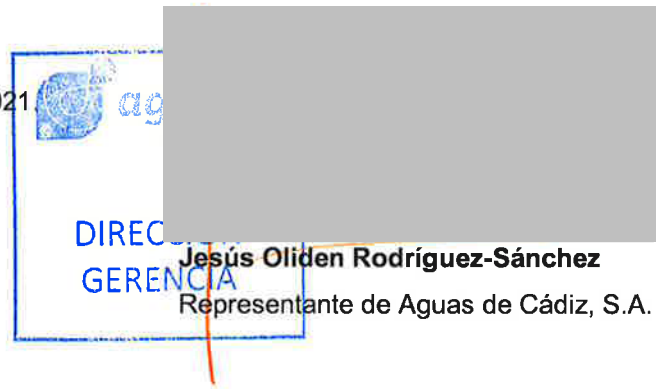
La presente Política, será publicada en la página web de ACASA (https://www.aguasdecadiz.es/) y en las sedes electrónicas que resulte de aplicación.

14 Entrada en vigor

La **Política de Seguridad**, que se aprueba mediante acta de reunión del Comité de Seguridad de Aguas de Cádiz.

Esta **Política de Seguridad** es efectiva desde dicha fecha y hasta que sea remplazada por una nueva Política.

Cádiz, 24 de Junio de 2021



Jesús Oliden Rodríguez-Sánchez
Representante de Aguas de Cádiz, S.A.