MARCO ORGANIZATIVO

-

POLÍTICA DE SEGURIDAD

Código:	ISENS-2023-PO-org.1
Versión:	23.00
Fecha de la versión:	30-08-23
Creado por:	RSEG
Aprobado por:	CEO
Nivel de confidencialidad:	PÚBLICO

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
30-08-23	23.00	RSEG	Definición de la política de Seguridad de la Información para el ENS

Tabla de contenido

1. Objetivo, alcance y usuarios (Org 1.1)

AR Vision se dedica al desarrollo de productos de Tecnologías Inmersivas (Realidad Virtual, Realidad Aumentada y Realidad Mixta) creando soluciones para sectores específicos con el objetivo de ser un apoyo en la transformación digital del mercado.

1.1. Misión.-

Liderar e impulsar el uso universal de tecnologías inmersivas, mejorando la vida de las personas a través de la creación de soluciones que rompan las barreras físicas, y ayuden a entender y vivir en realidades mixtas..

Nos encargamos del tratamiento de los datos de nuestros clientes facilitando su:

- Disponibilidad, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran;
- Integridad, asegurando que la información y sus métodos de proceso son exactos y completos;
- Confidencialidad, asegurando que sólo quienes estén autorizados pueden acceder a la información;
- Trazabilidad, posibilitando el seguimiento de los accesos indebidos a la información;
- Autenticidad, garantizando que los usuarios que tienen acceso son quien dicen ser;

El objetivo del presente documento es definir de forma clara las reglas para el uso de los sistemas y de otros activos de información en AR Vision.

La política de seguridad se establecerá, de acuerdo con los principios básicos señalados en el capítulo II del ENS y se desarrollará aplicando los siguientes requisitos mínimos:

a) Organización e implantación del proceso de seguridad.
b) Análisis y gestión de los riesgos.
c) Gestión de personal.
d) Profesionalidad.
e) Autorización y control de los accesos.
f) Protección de las instalaciones.
g) Adquisición de productos de seguridad y contratación de servicios de seguridad.
h) Mínimo privilegio.
i) Integridad y actualización del sistema.
j) Protección de la información almacenada y en tránsito.
k) Prevención ante otros sistemas de información interconectados.
l) Registro de la actividad y detección de código dañino.
m) Incidentes de seguridad.
n) Continuidad de la actividad.

1.2. Alcance.-

Este documento se aplica a todo el alcance del Sistema de Gestión de Seguridad de la Información (SGSI); es decir, a todas las personas, los sistemas y demás activos de la información utilizados dentro del alcance del SGSI.

1.3. Usuarios.-

Los usuarios de este documento son todos los empleados de AR Vision.

2. Marco legal y regulatorio (Org 1.2)

Requisito	*Documento que impone el requisito*	*Persona responsable del cumplimiento*	*Partes interesadas*
Protección de datos y privacidad de la información	Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales	RSEG	Empleados, Clientes, Proveedores y colaboradores
Principios básicos y requisitos mínimos para la protección adecuada de la formación tratada por las organizaciones. Evaluación de riesgos	Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad	RSEG	Empleados, Clientes
Regulación y armonización de la propiedad intelectual	Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual	RSEG	Empleados Clientes
Instalación y explotación de las redes de comunicaciones electrónicas, la prestación de los servicios de comunicaciones electrónicas, sus recursos y servicios asociados	Ley 11/2022, de 28 de junio, General de Telecomunicaciones.	RSEG	Empleados, Clientes y proveedores

Obligaciones web, y comunicaciones comerciales vía electrónica	Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI).	RSEG	Empleados, Clientes y proveedores
Controles criptográficos, y certificados electrónicos	Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza	RSEG	Empleados
Gestión de riesgos	Guía de aproximación para el empresario guia_ciberseguridad_gestion_riesgos_metad.pdf (incibe.es)	RSEG	Empleados
Gestión y evaluación de las brechas de seguridad notificadas por los responsables de tratamiento.	Guias AEPD guia-brechas-seguridad.pdf (aepd.es)	RSEG	Empleados Clientes y proveedores
Firma electrónica	Ley 59/2003, de 19 de diciembre, de firma electrónica	RSEG	Empleados, clientes y proveedores
Guías CCN-CERT	Guias Esquema Nacional de Seguridad 800_Guía_Esquema_Nacional_de_Seguridad (cni.es)		Empleados
UNE – ISO 27001:2013	Especificaciones para los Sistemas de Gestión de la Seguridad de la Información.	RSEG	Empleados
Procedimiento Administrativo y Régimen Jurídico del Sector Público	Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público	RSEG	Empleados clientes y proveedores

3. Roles y funciones de seguridad (Org 1.3)

El Esquema Nacional de Seguridad (ENS) es una normativa en España que establece los principios y requisitos necesarios para garantizar la seguridad de la información en las administraciones públicas y otras entidades que manejan información sensible. En el contexto del ENS, se definen varios roles y funciones de seguridad que son esenciales para implementar y mantener una adecuada gestión de la seguridad de la información.

1. La responsabilidad del éxito de una Organización recae en última instancia, en su Dirección. La Dirección es responsable de organizar las funciones y responsabilidades, la política de seguridad del Organismo, y de facilitar los recursos adecuados para alcanzar los objetivos propuestos.
2. Los directivos son también responsables de dar buen ejemplo siguiendo las normas de seguridad establecidas.
3. En una organización pueden coexistir diferentes informaciones y servicios, debiendo identificarse al responsable (o propietario) de cada uno de ellos. Una misma persona puede aunar varias responsabilidades.
4. La seguridad de los sistemas de información deberá comprometer a todos los miembros de la organización.

Bloques de responsabilidad

5. La política de seguridad, en aplicación del principio de diferenciación de responsabilidades a que se refiere el artículo 11 del ENS y según se detalla en la sección 3.1 del anexo II, deberá ser conocida por todas las personas que formen parte de la organización, e identificar de forma inequívoca a los responsables de velar por su cumplimiento, los cuales tendrán las siguientes funciones:

3.1. El responsable de la información.

Determinará los requisitos de la información tratada.

El Responsable de la Información (information owner) es habitualmente una persona que ocupa un alto cargo en la dirección de la organización. Este cargo tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección. El Responsable de la Información es el responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.

El ENS asigna al 'Responsable de la Información' la potestad de establecer los requisitos de la información en materia de seguridad.

El Responsable de la Información puede ser una persona concreta nombrada por el CEO, o puede ser un órgano corporativo.

Aunque la aprobación formal de los niveles corresponda al Responsable de la Información, se puede recabar una propuesta al Responsable de la Seguridad y conviene que se escuche la opinión del Responsable del Sistema.

La determinación de los niveles de seguridad en cada dimensión de seguridad debe realizarse dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad.

Se recomienda que los criterios de valoración estén respaldados por la Política de Seguridad en la medida en que sean sistemáticos, sin perjuicio de que puedan darse criterios particulares en casos singulares.

3.2. El responsable del servicio.

El ENS asigna al 'Responsable del Servicio' la potestad de establecer los requisitos del servicio en materia de seguridad.

El Responsable del Servicio puede ser una persona concreta o puede ser un órgano corporativo, que revestirá la forma de órgano colegiado de acuerdo con la normativa administrativa. Ver Comités.

Aunque la aprobación formal de los niveles corresponda al Responsable del Servicio, se puede recabar una propuesta al Responsable de la Seguridad y conviene que se escuche la opinión del Responsable del Sistema.

La determinación de los niveles de seguridad en cada dimensión de seguridad debe realizarse dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad. Se recomienda que los criterios de valoración estén respaldados por la Política de Seguridad en la medida en que sean sistemáticos, sin perjuicio de que puedan darse criterios particulares en casos singulares.

La prestación de un servicio siempre debe atender a los requisitos de seguridad de la información que maneja (a veces se dice que 'se heredan los requisitos'), y suele añadir requisitos de disponibilidad, así como otros como accesibilidad, interoperabilidad, etc.

RESPONSABILIDADES UNIFICADAS

Es posible que coincidan en la misma persona u órgano las responsabilidades de la información y del servicio.

3.3. El responsable de la seguridad.

Es la persona designada por el CEO para liderar y coordinar las actividades de seguridad de la información en la entidad.

Sus funciones incluyen entre otras definir la política de seguridad, supervisar su cumplimiento, gestionar incidentes de seguridad y asegurarse de que se implementen las medidas adecuadas para proteger la información, determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos, y reportará al CEO sobre estas cuestiones.

FUNCIONES:

a. Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo con lo establecido en la Política de Seguridad de la Organización.
b. Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.
c. Cuando el sistema trate datos personales, el responsable de seguridad recogerá los requisitos de protección de datos que sean fijados por el responsable o por el encargado del tratamiento, contando con el asesoramiento del DPD, y que sean necesarios implementar en los sistemas de acuerdo a la naturaleza, alcance, contexto y fines del mismo, así como de los riesgos para los derechos y libertades de acuerdo a lo establecido en los artículos 24 y 32 del RGPD, y de acuerdo a la evaluación de impacto en la protección de datos, si se ha llevado a cabo.

3.4. El responsable del sistema.

Es la persona designada por el CEO. Ejerce sus funciones por sí o a través de recursos propios o contratados, se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad.

El responsable de la seguridad será distinto del responsable del sistema, no debiendo existir dependencia jerárquica entre ambos. En aquellas situaciones excepcionales en las que la ausencia justificada de recursos haga necesario que ambas funciones recaigan en la misma persona o en distintas personas entre las que exista relación jerárquica, deberán aplicarse medidas compensatorias para garantizar la finalidad del principio de diferenciación de responsabilidades previsto en el artículo 11.

FUNCIONES:

a. El responsable del sistema, por sí o a través de recursos propios o contratados, se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad

b. Los informes de auditoría serán presentados al responsable del sistema y al responsable de la seguridad.

   Estos informes serán analizados por este último que presentará sus conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.

c. El responsable del sistema podrá suspender temporalmente el tratamiento de informaciones, la prestación de servicios o la total operación del sistema, hasta su adecuada subsanación o mitigación.

d. La identificación del usuario permitirá al Responsable del Sistema, al Responsable de la Seguridad o a sus respectivos administradores delegados, singularizar a la persona asociada al mismo, así como sus responsabilidades en el sistema.

e. El responsable del sistema garantizará que los dispositivos permanecen bajo control y que satisfacen sus requisitos de seguridad mientras están siendo desplazados de un lugar a otro, fuera de las zonas controladas por la organización.

f. Los informes de autoevaluación y de auditoría serán analizados por el responsable de la seguridad competente, que elevará las conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.

En el caso de servicios externalizados, salvo por causa justificada y documentada, la organización prestataria de dichos servicios deberá designar un POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado, que cuente con el apoyo de los órganos de dirección, y que canalice y supervise, tanto el cumplimiento de los requisitos de seguridad del servicio que presta o solución que provea, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio.

Dicho POC de seguridad será el propio Responsable de Seguridad de la organización contratada, formará parte de su área o tendrá comunicación directa con la misma. Todo ello sin perjuicio de que la responsabilidad última resida en la entidad del sector público destinataria de los citados servicios.

3.5. Administrador/Delegado/Oficial de Seguridad.

Son nombrados por el Responsable de Seguridad y serán los encargados de asesorar y colaborar con el Responsable de Seguridad en la puesta en marcha, y supervisión de las medidas de seguridad implementadas en la organización. También puede ser responsable de la gestión de riesgos y de coordinar la formación y concienciación en seguridad.

4. Nombramientos

La Dirección de la Organización nombra:

1. Al Responsable de la Información que, puede ser un cargo unipersonal o un órgano colegiado (Integrado habitualmente en el Comité de Seguridad de la Información).
2. Al Responsable del Servicio que, puede ser el mismo que el Responsable de la Información; puede ser un cargo unipersonal o un órgano colegiado (Integrado habitualmente en el Comité de Seguridad la Información).
3. Al Responsable de la Seguridad que, debe reportar directamente a la Dirección o, cuando existan, a los comités de Seguridad de la Información y al de Seguridad Corporativa.
4. Al Responsable del Sistema que, en materia de seguridad, debe reportar al Responsable de la Seguridad.

4.1. Procedimiento

El procedimiento de nombramiento de los responsables mencionados en el párrafo anterior debe constar en la Política de Seguridad de la Información de la Organización.

El nombramiento debe ser formal, mediante resolución del CEO.

La designación será unipersonal cuando las responsabilidades recaigan en personas.

Los Responsables de la Información y del Servicio pueden ser órganos colegiados; el Responsable de la Seguridad conviene que sea unipersonal.

4.2. Designación

La Dirección de la Organización designa a la persona Responsable del Sistema

- A propuesta del Responsable de la Información, cuando el Sistema de información trate una única información.
- A propuesta del Responsable del Servicio prestado, cuando el Sistema de información preste un único servicio.
- Directamente cuando el Sistema de información trata diferentes informaciones o presta diferentes servicios, oídos los responsables de las informaciones y los servicios afectados

5. Comités

Algunas responsabilidades pueden instrumentalizarse por medio de Comités, que se constituirán como órganos colegiados, de conformidad con lo señalado en la Ley 40/2015. Estos Comités, que estarán formados por miembros de todas las partes implicadas, y facilitarán el desenvolvimiento de la organización.

5.1. Comité de Seguridad de la Información.

Es un órgano colegiado cuyas funciones son entre otras las siguientes:

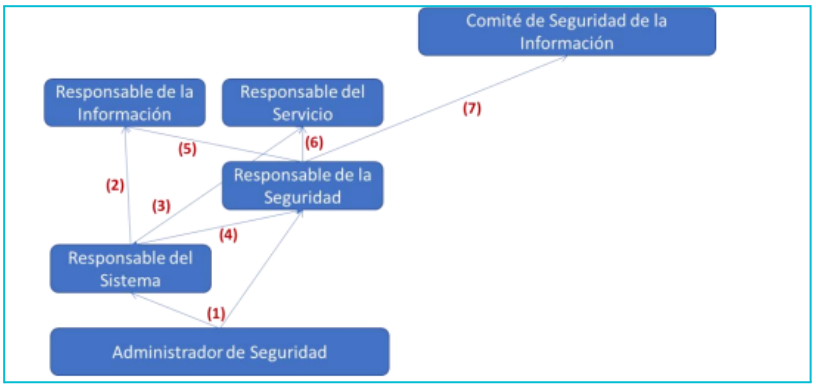
- Elaborar la Política de Seguridad Corporativa, que deberá ser aprobada por la Dirección de AR Vision.
- Coordinar todas las funciones de seguridad de la organización.
- Velar por el cumplimiento de la normativa legal y sectorial que sea de aplicación.
- Velar por el alineamiento de las actividades de seguridad a los objetivos de la organización.
- Coordinar los Planes de Continuidad, para asegurar una actuación sin fisuras en caso de que deban ser activados.
- Coordinar y aprobar, en su caso, las propuestas de proyectos recibidas de los diferentes ámbitos de seguridad, encargándose gestionar un control y presentación regular del progreso de los proyectos y anuncio de las posibles desviaciones.
- Recibir las inquietudes en materia de seguridad de la Dirección de la organización y transmitirlas a los responsables departamentales pertinentes, recabando de ellos las correspondientes respuestas y soluciones que, una vez coordinadas, habrán de ser comunicadas a la Dirección.
- Recabar de los responsables de seguridad departamentales informes regulares del estado de la seguridad de la organización y de los posibles incidentes. Estos informes, se consolidan y resumen para su comunicación a la Dirección de la entidad.
- Coordinar y dar respuesta a las inquietudes transmitidas a través de los responsables de seguridad departamentales
- Definir, dentro de la Política de Seguridad Corporativa, la asignación de roles y los criterios para alcanzar las garantías pertinentes en lo relativo a segregación de funciones
- Aprobar la Normativa de Seguridad de la Información.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios, desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por la organización y recomendar posibles actuaciones.

- 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 tales incidentes.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar planes de mejora de la seguridad de la información de la organización. En particular velará por la coordinación de distintos planes que puedan realizarse en diferentes áreas.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.

El Responsable de la Seguridad, actúa como Secretario del Comité de Seguridad de la Información y entre sus cometidos se encuentran:

- Convoca al Comité de Seguridad de la Información, recopilando la información pertinente.
- Elaborará el acta de las reuniones, donde se reflejará el quórum de asistentes, fecha y lugar de la celebración, el orden del día, un resumen de los asuntos tratados, los acuerdos adoptados, y la forma de aprobación de los acuerdos (unanimidad/mayoría...).
- Recaba las inquietudes de la Dirección de la entidad y de los responsables de seguridad departamentales, incorporándolas al Orden del Día del Comité de Seguridad Corporativa, para su examen y acciones pertinentes.
- Es responsable, junto con los diferentes responsables de seguridad departamentales, de estar al tanto de cambios regulatorios o normativos (leyes, reglamentos o prácticas sectoriales) que afecten a la entidad, debiendo informarse de las consecuencias para las actividades de la organización, alertando al Comité de Seguridad de la Información y proponiendo las medidas oportunas de adecuación al nuevo marco.
- Es el responsable de la toma de decisiones cotidianas entre dos reuniones del Comité de Seguridad de la Información. Estas decisiones darán respuesta a propuestas de los responsables de seguridad departamentales, velando por la unidad de acción y la coordinación de actuaciones, especialmente en caso de incidencias que tengan repercusión fuera de la organización y en caso de desastres

El Responsable de la Seguridad Corporativa formará parte del Comité de Crisis en caso de desastre, coordinando todas las actuaciones relacionadas con cualquier aspecto de la seguridad de la organización.



CARGO	PERSONA	FECHA NOMBRAM.
CEO	JAVIER ARGENTE LINARES	
RESP. DE SEGURIDAD	ANA TERESA V. ARREBOLA	07-10-23
RESP. DEL SISTEMA	Fº BORJA MAZO ESTEBANEZ	07-10-23
RESP. DE LA INFORMACIÓN	ANA TERESA V. ARREBOLA	07-10-23
RESP. DEL SERVICIO	ANA TERESA V. ARREBOLA	07-10-23

COMITÉ DE SEGURIDAD DE LA INFORMACIÓN			
CARGO	PERSONA	FECHA NOMBRAM.	ROL
CEO	JAVIER ARGENTE LINARES		PRESIDENTE
RESP. DE SEGURIDAD	ANA TERESA V. ARREBOLA	07-10-23	SECRETARIA
RESP. DE LA INFORMACIÓN	ANA TERESA V. ARREBOLA	07-10-23	SECRETARIA

5.2. Comité de Crisis

El comité de crisis es el máximo órgano decisorio para la gestión unificada de una situación de crisis.

Su principal cometido será acelerar el proceso de toma de decisiones para resolver incidencias, definiendo las prioridades, estableciendo la estrategia y la táctica a seguir. Deberá considerar los principales escenarios para tener en cuenta, cómo actuar y cómo comunicarlo, dirigiendo todos los equipos de recuperación y comunicación

Una crisis es una situación de baja probabilidad que cuando sucede genera un gran impacto y cuyos efectos perduran en el tiempo. Estos efectos se producen sobre:

- El bien o servicio de la organización que lo sufre
- Su reputación e imagen
- La sociedad en general

En el ámbito de la ciberseguridad, las cibercrisis requieren tomar decisiones rápidas con información limitada. La probabilidad de que este acontecimiento tenga lugar dependerá del grado de preparación previa de la organización.

La probabilidad será muy pequeña si se han tomado un gran número de medidas preventivas y progresivamente mayor cuanto menor sea el trabajo de prevención llevado a cabo con anterioridad.

El comité de Crisis estará presidido por el CEO, y serán miembros de este:

COMITÉ DE SEGURIDAD DE LA INFORMACIÓN			
CARGO	PERSONA	FECHA NOMBRAM.	ROL
CEO	JAVIER ARGENTE LINARES		PRESIDENTE
RESP. DE SEGURIDAD	ANA TERESA V. ARREBOLA	07-10-23	SECRETARIA
RESP. DE LA INFORMACIÓN	ANA TERESA V. ARREBOLA	07-10-23	SECRETARIA

6. Tareas

CSI – Comité de Seguridad de la Información
RINFO – Responsable de la Información
RSERV – Responsable del Servicio
RSEG – Responsable de la Seguridad
RSIS – Responsable del Sistema
ASS – Administrador de la Seguridad del Sistema

TAREA	RESPONSABLE
Determinación de los niveles de seguridad requeridos en cada dimensión	RINFO + RSERV o CSI
Determinación de la categoría del sistema	RSEG
Análisis de riesgos	RSEG
Declaración de aplicabilidad	RSEG
Medidas de seguridad adicionales	RSEG
Configuración de seguridad	elabora: RSEG aplica: ASS
Implantación de las medidas de seguridad	ASS
Aceptación del riesgo residual	RINFO + RSERV
Documentación de seguridad del sistema	RSEG
Política de seguridad	elabora: aprueba : Dirección
Normativa de seguridad	elabora: RSEG aprueba: CSI
Procedimientos operativos de seguridad	elabora: RSIS aprueba: RSEG aplica: ASS
Estado de la seguridad del sistema	monitoriza: ASS reporta: RSEG
Planes de mejora de la seguridad	elaboran: RSIS + RSEG aprueba: CSI
Planes de concienciación y formación	elabora: RSEG aprueba: CSI
Planes de continuidad	elabora: RSIS, valida: RSEG coordina y aprueba: CSI
Suspensión temporal del servicio	RSIS
Ciclo de vida: especificación, arquitectura, desarrollo, operación, cambios	elabora: RSIS y aprueba: RSEG

7. Estructuración de la documentación del sistema (Org 1.5)

Será el RSIS la persona encargada de la custodia y divulgación de la versión aprobada de la documentación generada. La documentación sobre la que se soporta esta política estará compuesta por un conjunto de Normas, guías y procedimientos que ayudarán a los usuarios en el desarrollo de sus tareas.

Esta documentación se encuentra dentro del sistema de documentación del drive corporativo, donde existen dos carpetas:

- ISO 9001, que incluye la documentación relativa a la documentación catalogada con carácter de PÚBLICO
- ENS; documentación relativa al sistema de información del Esquema Nacional de Seguridad catalogada con carácter PÚBLICO

8. Validez y gestión de documentos

Este documento es válido hasta el 31 de diciembre de 2024.

El propietario de este documento es el RSEG, que debe verificar, y si es necesario actualizar el documento, al menos una vez al año.

RSEG
D. ANA TERESA V. ARREBOLA

Firmado por VALENZUELA ARREBOLA ANA TERESA - ***4178** el día 12/05/2024 con un certificado emitido por AC FNMT Usuarios