1. INTRODUCCIÓN

La Política de Seguridad de la Información se elabora en cumplimiento de la exigencia 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.

Esta Política de Seguridad sigue también las indicaciones de la guía CCN-STIC-805 del Centro Criptológico Nacional, centro adscrito al Centro Nacional de Inteligencia

Azigrene Consultores, hace uso de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. En consecuencia, estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

Por ello, el objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con diligencia a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución y con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios.

Esto implica que la organización y su personal debe aplicar las medidas establecidas, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

La organización debe cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación.

La organización debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 9 del ENS.

1.1. PREVENCIÓN

La organización debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello se deben implementar 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, la organización debe:

- 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.

1.2. DETECCIÓN

Dado que los servicios se pueden degradar rápidamente debido a incidentes, se debe monitorizar la operación de manera continuada para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 10 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 9 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando

se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

1.3. RESPUESTA

La organización debe:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en áreas de la entidad o en otros organismos relacionados con **Azigrene Consultores**
- 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) reconocidos a nivel nacional: Iris-CERT, CCN- CERT,…

1.4. RECUPERACIÓN

Para garantizar la disponibilidad de los servicios críticos, la organización debe desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

2. MISIÓN

Azigrene Consultores es una organización, dotada de personalidad jurídica cuya actividad es:

Ingeniería y consultoría de servicios especializados en energía y medio ambiente. Asistencia técnica para el desarrollo de pliegos de contratación, seguimiento y control. de contratos públicos.

De forma estrechamente relacionada con el cumplimiento de esta misión, la organización desea manifestar la necesidad de una infraestructura TIC que prime y fomente las operativas abiertas, enfocadas a la funcionalidad, conectividad y servicio al usuario, como funciones prioritarias para la consecución de los objetivos estratégicos e institucionales.

3. OBJETIVOS

Azigrene Consultores persigue los siguientes objetivos:

1. Alinear la seguridad de la información con la estrategia de negocio para apoyar los objetivos de la organización.
2. Establecer las medidas necesarias para garantizar la seguridad de la información.
3. Establecer políticas de seguridad para la protección adecuada de la información.
4. Monitorización y reporte de los procesos para garantizar la seguridad.
5. Optimizar las inversiones en seguridad en apoyo a los objetivos de negocio.

4. ALCANCE

La organización aplicará la presente política de seguridad a todo el conjunto del sistema de información.

De forma concreta la presente política de seguridad es aplicable sobre los siguientes servicios y los sistemas TIC que los conforman:

Los sistemas de información que dan soporte a los servicios de consultoría e ingeniería energética y medio ambiente mediante el tratamiento de datos a gran escala según la categorización del sistema vigente.

5. MARCO LEGAL Y REGULATORIO

Son de aplicación las leyes y normativas españolas en relación a protección de datos personales, propiedad intelectual y uso de herramientas telemáticas. Por todo ello, **Azigrene Consultores** podrá ser requerida por los órganos administrativos pertinentes a proporcionar los registros electrónicos o cualquier otra información relativa al uso de los sistemas de información.

Esta política se desarrolla dentro del marco normativo:

Real Decreto 311/2022, de 3 de Mayo, por el que se regula el Esquema Nacional de Seguridad

A su vez, esta política se sitúa dentro del marco jurídico definido por los siguientes leyes y Reales Decretos en el ámbito de la seguridad de la información, protección de datos personal, propiedad intelectual, del propio Esquema nacional de seguridad vigentes.

También forman parte del marco normativo las restantes normas, reglamentos y normativa, nacional o internacional, a la que **Azigrene Consultores** está sujeto, están dispuestas en un Registro de Documentación Externa, el cual será actualizado por el responsable de sistema de gestion.

6. PRINCIPIOS BASICOS

La presente política de seguridad se establece de acuerdo con los principios básicos señalados en el capítulo II y se desarrollara aplicando los siguientes requisitos mínimos establecidos por el Articulo 12:

a) Organización e implantación del proceso de seguridad
b) Análisis y gestión de los riesgos
c) Gestión del personal
d) Profesionalidad
e) Autorización y control de los accesos.
f) Protección de las instalaciones.
g) Adquisición de productos.
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 actividad.
m) Incidentes de seguridad.
n) Continuidad de la actividad.
o) Mejora continua del proceso de seguridad

Los requisitos mínimos se exigirán en proporción a los riesgos identificados en nuestro sistema, de conformidad con lo dispuesto en el artículo 28 del ENS. El responsable de los sistemas de gestión será el encargado de consultar la legislación aplicable, registrarlo y mantenerlo actualizado en referencia a las normas relacionadas con la ciberseguridad y la protección de datos.

7. ROLES Y FUNCIONES DE SEGURIDAD

7.1. RESPONSABLE DE PROTECCIÓN DE DATOS

Será una persona con conocimiento especializado en Derecho y en la práctica en materia de protección de datos. Estos conocimientos serán exigibles en relación con los tratamientos que se realicen, así como las medidas que deban adoptarse para garantizar un tratamiento adecuado de los datos personales objeto de esos tratamientos.

El Responsable de Protección de Datos debe desempeñar sus tareas y funciones con total independencia.

Las funciones del **Responsable de Protección de Datos** será:

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones del RPGD y demás normativa aplicable en protección de datos.
- Supervisar el cumplimiento del RGPD y demás normativa aplicable en protección de datos, y de las políticas del responsable o encargado del tratamiento en dicha materia, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en operaciones de tratamiento.
- Ofrecer el asesoramiento que se solicite acerca de la evaluación de impacto relativa a la protección de

datos y supervisar su aplicación conforme al artículo 35 del RGPD.
- Cooperar con la Autoridad de control.

7.2. COMITÉS: FUNCIONES Y RESPONSABILIDADES

El **Comité de Seguridad**, está formado por: el responsable del Sistema de Gestión de Seguridad de la Información (SGSI), el Responsable de Sistemas y el Técnico informático. El Comité de Seguridad tendrá informada a la Dirección.

Las funciones del Comité de Seguridad en relación son:

- Divulgación de la política y normativa de seguridad de la Organización.
- Aprobación de la normativa de seguridad de la Organización.
- Revisión anual de la política de seguridad.
- Desarrollo de los procedimientos relacionados con la Seguridad de la Información
- Designación de roles y responsabilidades.
- Resolución de conflictos en la ejecución de las responsabilidades asignadas.
- Supervisión y aprobación de las tareas de seguimiento del Esquema Nacional de Seguridad:
  - Tareas de adecuación
  - Análisis de Riesgos
  - Auditoría

7.3. ROLES: FUNCIONES Y RESPONSABILIDADES

El **responsable del servicio** será quien determine los requisitos de los servicios prestados, en consonancia, tendrá las siguientes funciones:

- Establecer los requisitos del servicio en materia de seguridad, o, en terminología del ENS, la protestad de determinar los niveles de seguridad de los servicios.
- Clasificar los servicios conforme a los criterios y categorías establecidas en el ENS y en cada una de las dimensiones de seguridad conocidas y aplicables (disponibilidad, autenticidad, trazabilidad, confidencialidad e integridad), dentro del marco establecido en el Anexo I del ENS.
- Atender a los requisitos de seguridad de la información, tales como disponibilidad, accesibilidad, interoperabilidad, etc. que se demanden en la prestación de los servicios.
- Velar por la inclusión de cláusulas sobre seguridad en los contratos con terceras partes que puedan afectar a sus servicios y realizar el seguimiento de su cumplimiento.
- Determinará los requisitos de los servicios prestados

El **responsable de la información** será el propietario de la misma y tendrá las siguientes funciones;

- 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 (disponibilidad, autenticidad, trazabilidad, confidencialidad e integridad), dentro del marco establecido en el Anexo I del ENS.
- Trabajar en colaboración con el responsable de seguridad y el del sistema en el mantenimiento de los servicios de administración electrónica catalogados.
- Apoyar la realización de los análisis de riesgos y valorar las diferentes opciones de gestión del riesgo a implantar.
- Valorar y decidir, junto con los responsables de los Servicios, 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.
- Velar por la inclusión de cláusulas sobre seguridad en los contratos con terceras partes que puedan tener acceso a información de los procedimientos administrativos que gestiona y realizar el seguimiento de su cumplimiento

- Determinará los requisitos de los servicios prestados.

El **responsable de seguridad** será quien tome las decisiones adecuadas para satisfacer los requisitos de seguridad de la información y de los servicios. Dispondrá de las siguientes funciones:

- Supervisar el cumplimiento de la presente Política, de sus normas y procedimientos derivados.
- Asesorar en materia de seguridad a los integrantes Comité de Seguridad que así lo requieran.
- Coordinar la interacción con otros organismos especializados.
- Tomar conocimiento y supervisar la investigación y monitorización de los incidentes de seguridad.
- 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.
- Asesorar, en colaboración con los Responsables de los Sistemas, los Responsables de los Servicios y de la Información, en la realización del análisis y gestión de riesgos, elevando el informe resultante al Comité de Seguridad.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.
- Promover las actividades de concienciación y formación en materia de seguridad en su ámbito de responsabilidad, siguiendo las directrices del Comité de Seguridad.
- Realizar o promover las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones Comité de Seguridad en materia de seguridad.
- Preparar los temas a tratar en las reuniones del Comité de Seguridad, aportando información puntual para la toma de decisiones.
- Elaboración y revisión de la normativa de seguridad Comité de Seguridad.
- Aprobación de los procedimientos de seguridad elaborados por el responsable del Sistema.
- Determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisara la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportara sobre estas cuestiones.

El **responsable de los sistemas de información**, dentro de sus áreas de actuación, tendrán asignadas las siguientes funciones:

- Desarrollo, operación y mantenimiento del sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Garantizar que las medidas de seguridad se integren adecuadamente dentro del marco general de la Seguridad de la Información.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.
- Elaborar procedimientos técnicos de seguridad de los sistemas de información.
- Elaborar planes de continuidad de los sistemas de información.
- Colaborar para la realización del análisis de riesgos de los sistemas de información de los que es responsable.
- Implementar, gestionar y mantener las medidas de seguridad aplicables al sistema de información.
- Gestionar, configurar y actualizar, en su caso, el hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema de información.
- Se encargará (por sí solo, a través de recursos de la empresa o de servicios contratados) de desarrollar la forma concreta de implementar la seguridad en el sistema, de la supervisión de la operación diaria del mismo pudiendo delegar en administradores u operadores bajo su responsabilidad.

El **Administrador de la seguridad**, dentro de sus áreas de actuación, tendrán asignadas las siguientes funciones:

- Formar parte del Comité de Seguridad
- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas TIC en su ámbito de responsabilidad.
- Verificar que las medidas de seguridad establecidas son adecuadas para la protección de la información manejada y los servicios prestados.
- Analizar, completar y aprobar toda la documentación relacionada con la seguridad del sistema.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su

resolución.
- Elaborar el informe periódico de seguridad para el propietario del sistema, incluyendo los incidentes más relevantes del periodo.
- Aprobación de los procedimientos de seguridad elaborados por el responsable del Sistema.
- Elaboración de la normativa de seguridad de la entidad.

El **Delegado de protección de datos**, dentro de sus áreas de actuación, tendrán asignadas las siguientes funciones:

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento, de las obligaciones del RPGD y demás normativa aplicable en protección de datos.
- Supervisar el cumplimiento del RGPD y demás normativa aplicable en protección de datos, y de las políticas del responsable o encargado del tratamiento en dicha materia, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en operaciones de tratamiento, y las auditorías correspondientes.
- Ofrecer el asesoramiento que se solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación conforme al artículo 35 del RGPD.
- Cooperar con la autoridad de control. Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa del artículo 36 del RGPD, y realizar consultas, en su caso, sobre cualquier otro asunto.

7.4. Procedimiento de Designación

El responsable de la información y el responsable del servicio será nombrado por la direccion. El nombramiento será revisado cada 2 años o cuando el puesto quede vacante.
Para la asignación del personal dentro de la empresa para los distintos roles, se han tenido en cuenta las compatibilidades de los roles y sus incompatibilidades.

Por lo que la designación de los roles responsables de la seguridad de **Azigrene Consultores** se realice mediante la presente política y son los siguientes:

Para la asignación del personal dentro de la empresa para los distintos roles, se han tenido en cuenta las compatibilidades de los roles y sus incompatibilidades. Por lo que la designación de los roles responsables de la seguridad de **Azigrene Consultores** son los siguientes:

- **Responsable del servicio:** Dirección general
- **Responsable de la información:** Dirección general
- **Responsable de seguridad:** Responsable de sistemas
- **Responsable de los sistemas de información:** Responsable de sistemas
- **Responsable del sistema:** Responsable de los sistemas de gestión
- **Administrador de la seguridad de sistemas:** Ingeniero de sistemas

7.5. POLÍTICA DE SEGURIDAD

Será misión del Comité de Seguridad la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. En dicha revisión será decisión de la direccion renovar la designación de los responsables de seguridad o la designación de un nuevo personal. La Política será aprobada la Dirección y difundida para que la conozcan todas las partes afectadas.

8. RIESGOS QUE DERIVAN DEL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL

Azigrene Consultores realiza tratamientos en los que hace uso de datos de carácter personal, adoptando las medidas de seguridad adecuadas siguiendo las directrices del Reglamento Europeo de Protección de Datos, las indicaciones del Responsable de Protección de Datos y manteniendo la suficiente diligencia para cumplir con el principio de responsabilidad proactiva y el principio de accountability que establece la actual normativa de seguridad.

9. GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez cada dos años
- Cuando cambie la información manejada
- Cuando cambien los servicios prestados
- Cuando ocurra un incidente grave de seguridad
- Cuando se reporten vulnerabilidades graves
- Cuando así lo indique el Responsable de Protección de Datos.

10. DESARROLLO DE LA POLÍTICA DE SEGURIDAD

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

La normativa de seguridad estará disponible en el portal del empleado de **Azigrene Consultores.**

La Política será revisada como mínimo una vez al año en la revisión por dirección del sistema, o a intervalo más corto en caso de cambios significativos en la organización.

11. DIRECTRICES PARA LA ESTRUCTURACIÓN DE LA DOCUMENTACIÓN DE SEGURIDAD DEL SISTEMA

La documentación relativa a la seguridad de la información estará clasificada en tres niveles, de manera que cada documento de un nivel se fundamenta en los de nivel superior:

- **Primer nivel**: Política de seguridad de la información
  Documento de obligado cumplimiento por todo el personal, interno y externo, de la organización, recogido en el presente documento.
- **Segundo nivel**: normativas y procedimientos de seguridad
  De obligado cumplimiento de acuerdo al ámbito organizativo, técnico o legal correspondiente, desarrollado por **Azigrene Consultores** en el marco de su Sistema de Gestión Integrado en los que se han incluido los aspectos específicos del ENS para cumplir con los requisitos mínimos de seguridad de la información. Para facilitar dicha documentación se ha implementado una declaración de aplicabilidad del ENS en la cual se mapean las medidas de seguridad aplicables con las normativas y procedimientos de seguridad relacionados.
- **Tercer nivel**: informes, registros y evidencias electrónicas
  Documentos de carácter técnico que recogen evidencias generadas durante todas las fases del ciclo de vida del sistema de información, asi como amenazas y vulnerabilidades de los sistemas.

Toda la documentación de **Azigrene Consultores** se clasifica de la siguiente forma:

- Pública
- Interna
- Confidencial

según el procedimiento de Clasificación e intercambio de la información. La documentación será genera por el Comité de Seguridad y aprobada por la Dirección de la empresa.

12. OBLIGACIONES DEL PERSONAL

Todos los miembros de **Azigrene Consultores** tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y el Manual de Políticas y Normas de uso desarrollada a partir de ella, siendo responsabilidad de la Comisión de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Todos los trabajadores de Azigrene Consultores atenderán a una acción de concienciación en materia de seguridad TIC al menos una vez cada dos años. Se establecerá un **programa de acciones en concienciación** continua para atender a todos los miembros de **Azigrene Consultores**, en particular a los de nueva incorporación, teniendo en cuenta siempre las disponibilidades presupuestarias de **Azigrene Consultores**

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.

13. TERCERAS PARTES

Cuando **Azigrene Consultores** preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información.
Cuando **Azigrene Consultores** utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en la mencionada normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de informe 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 Responsable de Sistemas que precise los riesgos en que se incurre y la forma de tratarlos.
El informe debe ser aprobado por los responsables de SGSI y los servicios afectados antes de seguir adelante.

14. ENTRADA EN VIGOR

Esta política de Seguridad de la Información es efectiva desde el día siguiente al de su fecha de aprobación la Dirección de **Azigrene Consultores** y hasta que sea reemplazada por una nueva Política.

València, 20 de septiembre de 2024

AZIGRENE CONSULTORES, S.L.
B-97233092
Avd. Pons y Valero, 188 - 2
Tel. 963301641
46006 VALENCIA

D. Francisco Azara Ballester
Director General de Azigrene Consultores S.L.