ÍNDICE

1. INTRODUCCIÓN

La Dirección de **GHENOVA,** entiende que el sistema de información es un activo fundamental, razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad de la información.

El objetivo de **GHENOVA** es prestar un servicio a sus clientes cumpliendo los requisitos establecidos, de forma que obtengan la máxima satisfacción con nuestros servicios y se garantice la máxima privacidad y seguridad de la información de nuestra empresa.

Dicho objetivo de satisfacción de nuestros clientes y confidencialidad de la información es la piedra angular de nuestra política, entendiendo la satisfacción como el cumplimiento de los compromisos contraídos de la forma más eficiente posible, a la vez que se procura cumplir con las expectativas no contractuales derivadas de las necesidades descubiertas en la ejecución del servicio y relacionadas con el mismo, que el propio cliente nos comunica.

Como punto fundamental de la política está la implantación, operación y mantenimiento del Esquema Nacional de Seguridad.

Mediante la aplicación de una serie de medidas basadas en los requisitos del Esquema Nacional de Seguridad conforme al RD 311/2022 , se persigue una mejora continua en la calidad de los servicios y continuidad de los mismos de las actividades que desarrolla nuestra organización, así como un compromiso continuo de mejora técnica de nuestros sistemas, activos y procesos y el de nuestros proveedores, para procurar una continua adaptación a las necesidades tecnológicas de nuestros clientes.
Para ello, **GHENOVA**, considera la base de esta Política como pilares básicos de la organización para alcanzar la mejora continua de la eficacia de dicho sistema de Gestión, las siguientes directrices, que servirán de base al establecimiento de nuestros objetivos anuales:

- Lograr que la **seguridad de la información** y el respeto a los **datos personales** sean una constante:
    - Preservando la confidencialidad de la información y evitando su divulgación y el acceso por personas no autorizadas.
    - Manteniendo la integridad de la información procurando su exactitud y evitando su deterioro
    - Asegurando la disponibilidad de la información en todos los soportes y siempre que sea necesaria.
- Cumplir todos los requisitos legales aplicables que le son de aplicación, así como con aquellos requisitos que la organización suscriba evaluando continuamente dicho cumplimiento, en todas sus áreas de actividad
- Tener un plan de continuidad que permita recuperarse de un desastre en el menor tiempo posible.
- Velar por una **continua y permanente actualización de nuestros recursos**, tanto **tecnológicos** como, sobre todo, de nuestro **personal**, fomentando políticas de información y formación continua profesional que les permitan avanzar en sus conocimientos al ritmo que lo hace nuestro sector, fomentando la conciencia de la seguridad de la información, a fin de incrementar la competencia de los empleados
  Todos los empleados son informados de sus funciones y obligaciones de seguridad y son responsables de cumplirlas.
- Garantizar la **mejora continua**, manteniendo el Sistema de forma eficaz y efectiva para constatar el compromiso con los clientes, buscando para ello una mejor organización interna del trabajo y en la forma en que tratamos la información de nuestros clientes. Hay un responsable de seguridad encargado del SGSI de la organización.
- Gestionar adecuadamente todas las incidencias ocurridas, evaluando de forma concienzuda los **riesgos de la organización**, analizando los posibles riesgos de todos y cada uno de los procesos de la organización y de los activos de información, previendo y evitando de esta manera desviaciones, tomando las oportunas decisiones para minimizar posibles no conformidades.

- Comunicar a todo el personal y todo aquel que trabaje en su nombre, el obligado cumplimiento de esta Política, incluyendo contratistas y visitantes a nuestras instalaciones.
- Asegurar la **satisfacción de sus clientes** basándose en un trato siempre correcto y en un esfuerzo continuo en la prestación del servicio en base a sus requisitos y a nuestros compromisos de actualizaciones y mejoras.
- Cumplir con los **requisitos de los clientes y de sus grupos de interés**, así como con los requisitos legales y reglamentarios que afecten a la realización y prestación de los servicios prestados
- **Establecer procesos operacionales** que salvaguarden a las personas, la propiedad, la información, los datos y las aplicaciones o sistemas de uso para las instancias establecidas por la organización.
- Establecer y revisar regularmente los Objetivos, acordes con los compromisos que se asumen en esta declaración, fortaleciendo el **compromiso y participación de todo el personal** en el desarrollo y consecución de los Objetivos.
- La Dirección, por su parte, valora especialmente y establece como criterio principal para la estimación de sus riesgos la valoración de la disponibilidad, confidencialidad e integridad de su información y aún más la de sus clientes

2. ALCANCE

La organización establece para ENS RD 311/2022 esta política que se aplica a…

“Sistemas de información que dan soporte a las actividades realizadas con información clasificada de servicios de:

- *A) Servicios de ingeniería, consultoría, asistencia técnica y dirección de obra para proyectos del sector naval, industrial y energía (incluidos los proyectos de energía renovables), civil, en materia de agua e infraestructura del transporte.*

- *B) Consultoría, diseño, desarrollo, implantación y mantenimiento de soluciones digitales en las áreas de: Tecnologías de la información y comunicación (transformación digital, desarrollo de aplicaciones e integración de sistemas);*

Inteligencia Artificial e ingeniería de sistemas avanzada (machine learning, simulación dinámica, sistemas de control y bancos de pruebas inteligentes); y Sistemas navales (sistemas de control, monitorización embarcada, navegación autónoma e integración IoT marítima).

- *C) Servicios de ingeniería y consultoría para apoyo al ciclo de vida y apoyo logístico integrado en el mantenimiento y sostenibilidad de activos e instalaciones.*

- *D) Servicios de ingeniería y consultoría para proyectos de energías renovables marinas y sector eólico offshore.*

3. MISIÓN

La misión de **GHENOVA** es ser un proveedor estratégico para nuestros clientes, fomentando la integración de sus departamentos y dando soluciones de mejora a sus procesos de gestión.

4. MARCO NORMATIVO

GHENOVA se esfuerza en cumplir con toda la legislación aplicable a su actividad, ya sea de carácter general (Código Civil, Código de comercio, etc.) o específico, como por ejemplo la siguiente:

- **Real Decreto 311/2022, de 3 de mayo**: Regula el Esquema Nacional de Seguridad (ENS) y establece principios y requisitos de ciberseguridad en el sector público.
- **Guías de la serie 800 CCN-STIC**: Serie de guías del Centro Criptológico Nacional que orientan sobre seguridad y estructuración documental en el cumplimiento del ENS.
- **Ley Orgánica 3/2018, de 5 de diciembre**: Relativa a la Protección de Datos Personales y garantía de los derechos digitales, complementa y desarrolla el Reglamento General de Protección de Datos (RGPD).

- **Reglamento (UE) 2016/679 del Parlamento Europeo (RGPD)**: Relativo a la protección de datos personales de las personas físicas en la UE y su libre circulación.
- **Reglamento (UE) nº 910/2014 (eIDAS)**: Regula la identificación electrónica y los servicios de confianza en el mercado interior, derogando la Directiva 1999/93/CE.
- **Reglamento (UE) 2019/881 (Reglamento de Ciberseguridad)**: Relativo a la ciberseguridad y certificación de tecnologías de la información, regula la Agencia de la UE para la Ciberseguridad (ENISA) y sustituye al Reglamento (UE) n.o 526/2013.
- **Real Decreto Legislativo 1/1996, de 12 de abril**: Aprueba el texto refundido de la Ley de Propiedad Intelectual, armonizando las disposiciones legales sobre la materia. Actualizada por **Ley 23/2006**.
- **Ley 11/2022 de 28 de Junio**: Ley General de Telecomunicaciones

5. ROLES: FUNCIONES Y RESPONSABILIDADES

5.1. RESPONSABLE DE INFORMACIÓN

- Determina los requisitos (de seguridad) de la información tratada, según los parámetros del Anexo I del ENS.
- Formar parte y tomar decisiones en el Comité de Seguridad de la Información.
- Aprobación de los niveles de seguridad de la información.
- Proteger los activos.
- Cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos.

5.2. RESPONSABLE DEL SERVICIO

- Determina los requisitos (de seguridad) de los servicios prestados, según los parámetros del Anexo I del ENS.
- Formar parte y tomar decisiones en el Comité de Seguridad de la Información.
- Aprobación de los niveles de seguridad de los servicios.
- Proteger los activos.

- Cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos

5.3. RESPONSABLE DE SEGURIDAD

- Determina las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por los responsables de la información y de los servicios.
- 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 Información de la organización.
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.
- Convoca las reuniones del Comité de Seguridad de la Información.
- Junto con el Responsable de Sistema, vela por el cumplimiento del ENS, especialmente en términos de actualización de controles y categorización de activo.
- Prepara los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elabora el acta de las reuniones.
- Es responsable de la ejecución directa o delegada de las decisiones del Comité.
- Elaborar y proponer para aprobación por la organización las políticas de seguridad, que incluirán las medidas técnicas y organizativas, adecuadas y proporcionadas, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados y para prevenir y reducir al mínimo los efectos de los ciberincidentes que afecten a la organización y los servicios.
- Desarrollar las políticas de seguridad, normativas y procedimientos derivados de la organización, supervisar su efectividad y llevar a cabo auditorías periódicas de seguridad.
- Elaborar el documento de Declaración de Aplicabilidad.
- Actuar como capacitador de buenas prácticas en seguridad de las redes y sistemas de información, tanto en aspectos físicos como lógicos.
- Constituirse como punto de contacto con la autoridad competente en materia de seguridad de las redes y sistemas de información y responsable ante aquella del

cumplimiento de las obligaciones que se derivan del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información y de su Reglamento de Desarrollo.

- Constituir el punto de contacto especializado para la coordinación con el CSIRT (Computer Security Incident Response Team – Equipo de Respuesta ante Emergencias Informáticas) de referencia (CCN-Cert, INCIBE..).

- Notificar a la autoridad competente, a través del CSIRT de referencia y sin dilación indebida, los incidentes que tengan efectos perturbadores en la prestación de los servicios.
- Recibir, interpretar y aplicar las instrucciones y guías emanadas de la Autoridad Competente, tanto para la operativa habitual como para la subsanación de las deficiencias observadas
- Recopilar, preparar y suministrar información o documentación a la autoridad competente o el CSIRT de referencia, a su solicitud o por propia iniciativa

5.4. RESPONSABLE DEL SISTEMA

- Formar parte y tomar decisiones en el Comité de Seguridad de la Información.
- Desarrollar, operar y mantener del Sistema durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y política de gestión del Sistema estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Definir la política de conexión o desconexión de equipos y usuarios nuevos en el Sistema.
- Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.
- Junto con el Responsable de Seguridad, vela por el cumplimiento del ENS, especialmente en términos de actualización de controles y categorización de activo.
- Decidir las medidas de seguridad que aplicarán los suministradores de componentes del Sistema durante las etapas de desarrollo, instalación y prueba de este.

- Implantar y controlar las medidas específicas de seguridad del Sistema y cerciorarse de que éstas se integren adecuadamente dentro del marco general de seguridad.
- Determinar la configuración autorizada de hardware y software a utilizar en el Sistema.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del Sistema.
- Llevar a cabo el preceptivo proceso de análisis y gestión de riesgos en el Sistema.
- Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y determinar las medidas de seguridad que deben aplicarse según se describe en el Anexo II del ENS.
- Elaborar y aprobar la documentación de seguridad del Sistema.
- Delimitar las responsabilidades de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del Sistema.
- Investigar los incidentes de seguridad que afecten al Sistema, y en su caso, comunicación al Responsable de Seguridad o a quién éste determine.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
- Puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los responsables de la información afectada, del servicio afectado y el responsable de seguridad, antes de ser ejecutada.

6. DATOS DE CARACTER PERSONAL

GHENOVA, trata los datos de carácter personal, por lo que mantiene un “registro de actividades de tratamiento”, al que tendrán acceso sólo las personas autorizadas, en el que se recogen los datos afectados y los responsables del tratamiento. Todos los sistemas de información de GHENOVA se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado registro.

7. OBLIGACIONES DEL PERSONAL

Todos los trabajadores de GHENOVA, tienen la obligación de conocer esta Política de Seguridad de la Información, que es de obligado cumplimiento dentro del alcance identificado, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Se establecerá un programa de concienciación continua para atender a todos los miembros de GHENOVA, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC dentro del alcance 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, por el contrario se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

8. TERCERAS PARTES

Las terceras partes relacionadas con GHENOVA, dentro del alcance, firman con la empresa un acuerdo que protege la información intercambiada.

Cuando GHENOVA, utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad. Dicha tercera parte, quedará sujeta a las obligaciones establecidas en dicha Política, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

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 Seguridad que precise los riesgos en que se incurre y la forma de tratarlos.

9. HISTORIAL DE REVISIONES

Esta Política será revisada para su continua adecuación anualmente por la Dirección, así como los objetivos y metas de la empresa, y comunicada a todo el personal de la organización encontrándose a disposición del público bajo solicitud de cualquier parte interesada.

Revisión	Fecha	Razón Modificación
1.0	10/01/2025	Creación del Documento

La Gerencia se asegura que la Política de Seguridad de la Información es entendida, implantada y mantenida al día en todos los niveles de la Organización.

En Sevilla, a diez de Enero de 2025

Fdo.: *Natalia González Hereza*
Dirección de Sostenibilidad y Organización