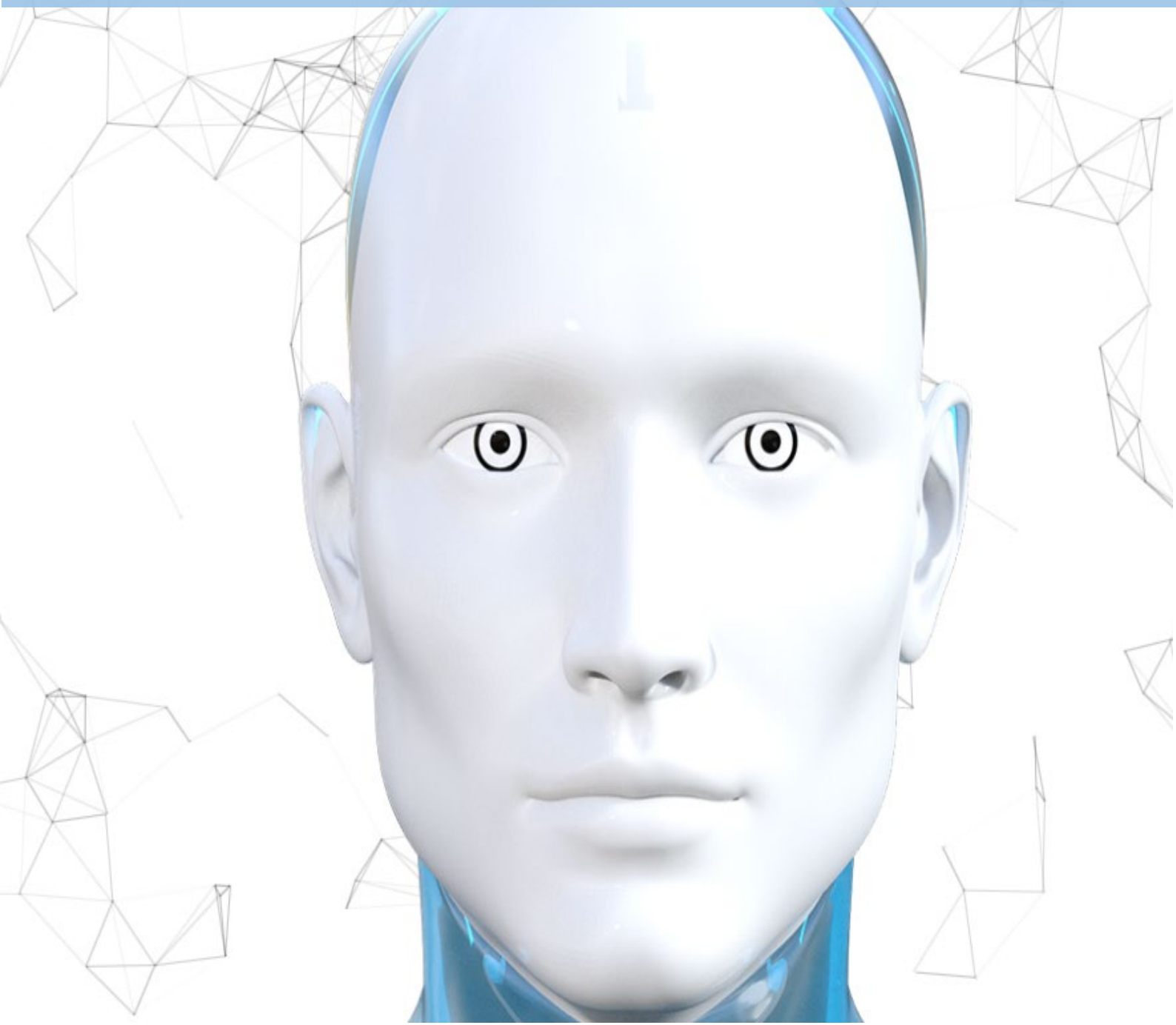
Fecha: 23/05/23
Versión: 1.0

IN1- Difusión Interna
NL2 – Uso Oficial

CIBINAR

MARCO NORMATIVO DE SEGURIDAD

POL_001 POLITICA DE SEGURIDAD - PÚBLICA



CONTROL DE FIRMAS

	FECHA
ELABORADO POR Responsable de Seguridad	17/04/2023
APROBADO POR Comité de Seguridad	23/05/2023

CONTROL DE VERSIONES

VERSIÓN	FECHA	AUTOR	CAMBIOS
1.0	17/04/23	Responsable de Seguridad	Versión inicial del documento

APROBACIÓN Y ENTRADA EN VIGOR

El presente Documento ha sido aprobado por el Comité de Seguridad de CIBINAR, contribuyendo al establecimiento de las directrices generales para el uso adecuado de los recursos de tratamiento de información que CIBINAR pone a disposición de sus usuarios para el ejercicio de sus funciones y que, correlativamente, asumen las obligaciones descritas, comprometiéndose a cumplir con lo dispuesto en los siguientes epígrafes.

Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación por parte de CIBINAR.

Las versiones anteriores que hayan podido distribuirse constituyen borradores que se han desarrollado temporalmente, por lo que su vigencia queda anulada por la última versión de este documento.

1. Introducción

Ponemos en conocimiento de todas las partes interesadas (clientes, proveedores, colaboradores…) la existencia de Directrices de Seguridad de la Información establecidas en nuestra organización para mostrar el compromiso de CIBERSEGURIDAD E INTELIGENCIA ARTIFICIAL, S.L (en adelante, CIBINAR) en la protección y garantía de los principios de: confidencialidad, integridad y disponibilidad de la información manejada en la Organización.

Trabajamos bajo un Sistema de Gestión de Seguridad de la Información, cuyo alcance no sólo afecta al uso de los activos, sino que se extiende a todas las personas y terceros en el conocimiento y cumplimiento de estas Directrices estructuradas acorde a las normas ISO/IEC 27001:2022 y RD 311/2022 por el que se regula el Esquema Nacional de Seguridad (ENS). Tanto la Política como las Directrices de Seguridad de la Información, están en línea con el Reglamento General de Protección de Datos (RGPD).

En cualquier ámbito de la normativa se desarrollan las funciones y responsabilidades desde las diferentes dimensiones de la Seguridad consideradas, entendiendo como tales las dimensiones de:

- ***Disponibilidad***
- ***Confidencialidad***
- ***Integridad***
- ***Trazabilidad***
- ***Autenticidad***

Esta regulación, en materia de seguridad, incide en los siguientes campos de la Organización:

- **Acceso a las instalaciones**. En la que se regulan las normas de acceso, haciendo especial mención a los accesos a áreas seguras y regulación del acceso a personas ajenas a la organización.
- **Acceso a la red corporativa.** Los recursos corporativos son protegidos con los medios de seguridad técnicos necesarios para asegurar la protección de la información, ya sea desde las propias instalaciones o de forma externa. El acceso y el uso de la información están reguladas por normas enfocadas a la protección con especial atención a información sensible o confidencial.
- **Uso de los activos.** Las personas en CIBINAR se comprometen a hacer un uso racional y velar por el cuidado de los equipos proporcionados

por la Organización para el desempeño de sus funciones y tareas. En este sentido se describen normas de actuación y se aplican configuraciones encaminadas a la protección de la información contenida en estos dispositivos.

- **Uso de internet.** Especial atención se realiza en la regulación del uso de internet, correo electrónico y almacenamiento en la nube a usos profesionales con el objetivo de minimizar riesgos que puedan producirse con un uso no regulado de dichas herramientas.
- **Gestión de incidencias.** La implicación de las personas de CIBINAR en materia de seguridad ayuda a detectar posibles problemas que puedan poner en peligro la confidencialidad, integridad y disponibilidad los servicios o activos que soportan.
- **Continuidad de negocio.** Todos los medios implantados para la disponibilidad y continuidad del negocio están en línea con los requerimientos de los esquemas ISO certificados en la organización.
- **Propiedad intelectual.** Protegida con el compromiso de las personas de CIBINAR conforme a las normas de confidencialidad de la organización.

La violación de las Políticas y las directrices de Seguridad está sujetas a sanción de acuerdo con los mecanismos habilitados en la legislación vigente.

Tanto la Política como la Normativa son revisadas periódicamente para alinearlas con las necesidades de la organización.

El Comité de Dirección conoce la importancia de estas Políticas y participa activamente en la revisión de estas.

2. Resumen Ejecutivo - Política de seguridad

Ponemos en conocimiento de nuestros clientes, usuarios y proveedores la existencia de Directrices de Seguridad de la Información establecidas en nuestra organización para mostrar el compromiso de **CIBINAR** con la protección y garantía de los principios de: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información manejada en la Organización.

Trabajamos bajo un Sistema de Gestión de Seguridad de la Información, cuyo alcance no sólo afecta el uso de los activos, sino que se extiende a todas las personas y terceros en el conocimiento y cumplimiento de estas Directrices estructuradas de acuerdo con el Esquema Nacional de Seguridad. Tanto la Política como las Directrices de Seguridad de la Información, están en línea con el Reglamento General de Protección de Datos (RGPD).

Esta regulación en materia de seguridad incide en los siguientes campos de la Organización:

Acceso a las instalaciones

En la que se regulan las normas de acceso, haciendo especial mención a los accesos a áreas seguras y regulación del acceso a personas ajenas a la organización.

Acceso a la red interna

Los recursos tecnológicos están protegidos con los medios de seguridad técnicos necesarios para asegurar la protección de la información, ya sea desde las propias instalaciones o de forma externa. El acceso y el uso de la información están reguladas por normas enfocadas a la protección con especial atención a información sensible o confidencial.

Uso de los activos

Las personas que componen el Ayuntamiento se comprometen a hacer un uso racional y velar por el cuidado de los equipos proporcionados por la Organización para el desempeño de sus funciones y tareas. En este sentido se describen normas de actuación y se aplican configuraciones

encaminadas a la protección de la información contenida en estos dispositivos.

Uso de internet

Especial atención se realiza en la regulación del uso de internet, correo electrónico y almacenamiento en la nube a usos profesionales con el objetivo de minimizar riesgos que puedan producirse con un uso no regulado de estas herramientas.

Gestión de incidencias

La implicación de todos los miembros del Ayuntamiento en materia de seguridad ayuda a detectar posibles problemas que puedan poner en peligro la confidencialidad, integridad y disponibilidad los servicios o activos que soportan.

Continuidad del servicio

Todos los medios implantados para la disponibilidad y continuidad del servicio están en línea con los requerimientos del RD 311/2022 de 3 de Mayo de 2022 por el que se regula el Esquema Nacional de Seguridad.

Propiedad intelectual

Protegida con el compromiso de todos los que componemos el Ayuntamiento conforme a las normas de confidencialidad de la organización.

La violación de las Políticas y las directrices de Seguridad está sujeta a sanción de acuerdo con los mecanismos habilitados en la legislación vigente.

Tanto la Política como las Directrices son revisadas periódicamente para alinearlas con las necesidades de la Organización y estado del arte de la tecnología.

El Comité de Seguridad conoce la importancia de estas Políticas y participa activamente en la revisión de las mismas.

Nuestra principal responsabilidad es ofrecer a nuestros clientes y usuarios soluciones y servicios de confianza con altos estándares de seguridad necesarios.

Como muestra de garantía y confianza para nuestros usuarios, **CIBINAR** se somete periódicamente a auditorías independientes para la certificación de sus sistemas de gestión y producción de acuerdo al Esquema Nacional de Seguridad y Sistema de Gestión de Seguridad de la Información basado en la norma UNE:ISO 27001:2022.