Dirección Gerencia

Conforme al art. 98 del Texto Refundido de Ley General de la Seguridad Social (RD Legislativo 8/2015 de 30 de octubre) la Ley General de la Seguridad Social y los Estatutos de la entidad, nombrado por la Junta Directiva y ratificado por el Ministerio competente, el **Director Gerente** de MUTUALIA ejerce la dirección ejecutiva; le corresponde desarrollar sus objetivos generales y la dirección ordinaria de la entidad; sin perjuicio de estar sujeto a los criterios e instrucciones que, en su caso, le impartan la Junta Directiva y su Presidente; incluyendo las de seguridad de la información.

El Director Gerente es el máximo responsable de la implantación del ENS en la entidad. De la Dirección Gerencia depende el compromiso de la entidad con la seguridad y su adecuada implantación, gestión y mantenimiento.

Es responsable de fijar los objetivos estratégicos, organizar adecuadamente sus elementos constituyentes, sus relaciones internas y externas, y dirigir su actividad, incluyendo la competencia de **aprobar/revisar la presente Política de Seguridad de la Información**, facilitando los recursos adecuados para alcanzar los objetivos propuestos, velando por su cumplimiento.

Es función de la Dirección Gerencia de la entidad **NOMBRAR/DESIGNAR**:

- Al **Responsable de la Información**; que podrá ser un cargo unipersonal o desempeñar tal función un órgano colegiado integrado en el Comité de Seguridad de la Información

- Al **Responsable del Servicio**, que podrá ser también un cargo unipersonal o desempeñar tal función un órgano colegiado

- Al **Responsable de la Seguridad**, que debe reportar directamente a la Dirección Gerencia y al Comité de Seguridad de la Información

Por otro lado, corresponde al responsable de la Seguridad la designación de:

- Al **Responsable del Sistema**, que, en materia de seguridad, reportará al Responsable de la Seguridad

Estas designaciones serán permanentes siempre y cuando la persona que ocupe dicho rol pertenezca a MUTUALIA y/o cuando Dirección contemple su cese de dicho rol. La dirección ha acordado realizar las siguientes designaciones:

Responsable de la Información	Comité de Seguridad
Responsable del Servicio	Direcciones de Seguimiento de Gestión
Responsable de la Seguridad	Iratxe Ijalba Izaguirre
Responsable del Sistema	Roberto Rueda Maiso

Así mismo, el Director Gerente, como máxima persona directiva es el representante de la entidad y personifica a la misma como **Responsable del Tratamiento de los datos personales**.

Responsable de la Información: Comité de Seguridad de la información

el Comité de Seguridad de la Información de MUTUALIA está formado por las siguientes personas:

- Responsable de los Sistemas de Información - Responsable de Seguridad
- Responsable de Organización y Gestión de Riesgos
- Delegado de Protección de Datos (*)

- De forma puntual o habitual, otras personas responsables/representantes y/o técnicas de las áreas/procesos que gestionen servicios o información de la organización que, deban participar/reportar/asesorar a la Comisión
- De forma puntual, cualquier otra persona de cualquier área de la Organización (consultora/asesora externa), cuando se precise su asesoramiento o aportación informativa/técnica

*Cuando el Comité de Seguridad de la Información actúe también como Comité de *Protección de Datos*, el DELEGADO DE PROTECCIÓN DE DATOS en el ejercicio de sus funciones, conforme a su posición prevista en el art. 38.3 de la RGPD, no podrá recibir instrucciones, debiendo responder directamente al más alto nivel jerárquico de la entidad (Dirección Gerencia) y no podrá participar en las decisiones relativas a los FINES Y MEDIOS del tratamiento.

Serán <u>funciones</u> y responsabilidades del Comité de Seguridad de la Información de MUTUALIA**:**

1. Ejercer las funciones que, como órgano colegiado le atribuya esta Política de Seguridad de la Información en sus diferentes roles, o la Política de Protección de Datos
2. Apoyar, informar y asesorar (en todas las actividades, dudas y cuestiones relacionadas con la seguridad de los sistemas de información y Protección de Datos) a:
   - La Dirección Gerencia en su calidad de Responsable de Tratamiento
   - La Responsable de Seguridad
   - Al Delegado de Protección de Datos
   - y al resto de personas responsables de Procesos y Áreas funcionales de la Organización
3. Proponer la aprobación/revisión por la Dirección Gerencia esta Política de Seguridad de la Información
4. Aprobar la Normativa de Seguridad de la información
5. Informar regularmente del estado de la seguridad de la información a la Dirección Gerencia
6. Asesorar y proponer resolución de los conflictos de responsabilidad entre los diferentes responsables y/o áreas de la organización o elevar a la Dirección Gerencia los casos en los que no tenga suficiente autoridad para decidir
7. Apoyar y asesorar a las áreas/procesos en la elaboración y/o implementación de controles y medidas en la 1ª línea de defensa de Gestión de Riesgos
8. Supervisar, como 2ª línea de defensa en el Sistema de Gestión de Riesgos, el mapa de riesgos y la implementación de los controles y demás medidas para la eliminación o mitigación de los riesgos de seguridad de la información y de Protección de Datos
9. Monitorizar los principales riesgos residuales asumidos por la organización y recomendar posibles medidas de control
10. Asesorar y alentar la elaboración de normas, procedimientos, instrucciones, guías de buenas prácticas internas para la gestión de la Seguridad de la Información y Protección de Datos
11. Promover la mejora continua del sistema de gestión de la seguridad de la información (SGSI)
12. Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar actuaciones respecto de ellos. Velar por la coordinación en la gestión de tales incidentes.
13. Alentar y supervisar las auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información y Protección de Datos
14. Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación.
15. Informar/analizar novedades normativas, guías/criterios administrativos y/o jurisprudenciales
16. Promover una adecuada concienciación, divulgación de la normativa y formación en materia de seguridad de la información y Protección de Datos
17. Asesorar para la contestación al ejercicio de los derechos de Protección de Datos
18. Informar, deliberar, hacer propuestas técnicas e intercambiar información con los procesos/áreas sobre medidas de seguridad técnica
19. Informar, asesorar y efectuar seguimiento de PIA-EIPD en el diseño, desarrollo y ejecución de proyectos que afecten directamente a la seguridad de la información y de datos personales
20. Emitir directrices/recomendaciones internas sobre áreas de su competencia

Para ejercer estas funciones y responsabilidades el Comité de Seguridad de Mutualia se reunirá al mínimo trimestralmente, pudiendo establecer otras reuniones si sus funciones y/o responsabilidades así lo requieren.

La persona **Responsable de la Seguridad** (con la ayuda que precise de los demás miembros en los que puede delegar funciones, o recabar apoyo administrativo de otras áreas) será el SECRETARIO del Comité de Seguridad de la Información y como tal:

a) Convoca sus reuniones;
b) Prepara los temas a tratar en las reuniones, aportando información para la toma de decisiones;
c) Elabora el acta de las reuniones;
d) Es responsable de la ejecución, directa o delegada, de las decisiones del Comité.

En este rol de Responsable de la Información, el COMITÉ DE SEGURIDAD DE LA INFORMACIÓN:

1. Conforme al art. 13 del RD 311/2022, el Responsable de la Información determina los requisitos de la información en materia de seguridad, y sobre la base del establecimiento previo de los niveles de seguridad en cada dimensión de los sistemas, según los parámetros del Anexo I del ENS (aunque la aprobación formal de los niveles corresponda al Responsable de la Información, se podrá recabar una propuesta del Responsable de la Seguridad y se escuchará la opinión del Responsable del Sistema)
2. Evaluará y supervisará de forma continua, como 2ª línea de defensa, el estado de la seguridad de la información y la eficacia del sistema de gestión de la seguridad de la información implantado en la organización, derivado este del cumplimiento del ENS, el estándar ISO27001 en el que se encuentra certificada la entidad; y de la protección de datos personales según normativa vigente (RGPD y LOPDGDD).
3. Coordinará la seguridad de la información a nivel de organización para, entre otros aspectos, racionalizar la implantación de las diferentes medidas de seguridad requeridas por el sistema y evitar disfunciones que permitan fallas de seguridad al dejar al sistema con puntos débiles donde pudieran ocurrir accidentes o se pudieran perpetrar ataques.
4. Tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección. Es el responsable último de cualquier error o negligencia que conlleve un incidente de confidencialidad o de integridad (en materia de protección de datos) y de disponibilidad (en materia de seguridad de la información).

Responsable del Servicio: Direcciones de Seguimiento de Gestión

El ENS asigna al Responsable del Servicio la potestad de establecer los requisitos del servicio en materia de seguridad: la potestad de determinar los niveles de seguridad de los servicios, pudiendo ser una persona física concreta o un órgano colegiado.

Su función es trabajar en colaboración con el Responsable de Seguridad y el Responsable del Sistema en la valoración de los servicios en las diferentes dimensiones de seguridad y en el mantenimiento de los sistemas.

En MUTUALIA los responsables del servicio serán **las personas responsables de las diferentes áreas, servicios y procesos** (Direcciones de Seguimiento de Gestión) de la organización que gestionan la prestación de los diferentes servicios en los que tratan una información determinada**.**

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 prestación de un servicio siempre debe atender a los requisitos de seguridad de la información que maneja, a los que se suele añadir requisitos de disponibilidad, accesibilidad, interoperabilidad, etc.

Responsable de Seguridad

La facultad para determinar la categoría del sistema (art. 41.2 RD 311/2022) le corresponde a la función de Responsable de la Seguridad. Las tareas de la persona responsable de seguridad serán:

Determinará las **decisiones para satisfacer los requisitos de seguridad de la información y de los servicios** (art. 13 RD 311/2022), entre las cuales están:

- **Mantener la seguridad de la información manejada y de los servicios prestados** por los sistemas de información en su ámbito de responsabilidad, de acuerdo a 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.
- Decisión, firma y responsabilidad en actos ordinarios de **tratamiento, gestión, acceso, conservación y seguridad** en la información digital.
- Decisión, firma y responsabilidad en **comunicación y resolución de incidencias en tratamiento, gestión, conservación y seguridad en la información digital**.
- **Coordinar y controlar las medidas de seguridad**, aplicables y definidas en los **procedimientos** de aplicación.
- Controlar directamente los mecanismos que permiten el **registro de accesos** no permitiendo la desactivación ni la manipulación de los mismos.
- Revisar la **información de control** registrada y elaborar informes de las revisiones realizadas y los problemas detectados.
- Decidir sobre la **adquisición de productos y contratación de servicios** relacionados con la seguridad (En la **adquisición de productos de seguridad de las tecnologías de la información y comunicaciones** se utilizarán, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen **a juicio del Responsable de la Seguridad** - art.19 RD 311/2022)
- Dar **cumplimiento a los requisitos mínimos de seguridad aplicables a la categoría del sistema** según ENS y sin perjuicio del cumplimiento de lo requerido por lo dispuesto en el RGPD.
- **Analizar los informes de auditoría** del ENS y presentar las conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.
- **Mantener la seguridad de la información gestionada y de los servicios** prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo con lo establecido en la presente *Política de Seguridad de la Información*.
- Promover la **formación y concienciación** en materia de seguridad de la información dentro de su ámbito de responsabilidad
- **Las medidas del Anexo II del ENS**, así como aquellas otras necesarias para garantizar el adecuado tratamiento de datos personales **podrán ser ampliadas** por causa de la concurrencia indicada o del **prudente arbitrio del Responsable de la Seguridad** del sistema, habida cuenta del estado de la tecnología, la naturaleza de los servicios prestados y la información manejada, y los riesgos a que están expuestos (art. 28.2 RD 311/2022)
- La relación de medidas seleccionadas del Anexo II se formalizará en el documento **DECLARACIÓN DE APLICABILIDAD**, firmado por la persona **Responsable de la Seguridad** (art. 28.2 RD 311/2022)
- Las **medidas de seguridad** referenciadas en el Anexo II podrán ser reemplazadas por otras compensatorias siempre y cuando se justifique documentalmente que protegen igual o mejor el riesgo sobre los activos (Anexo I) y se satisfacen los principios básicos y los requisitos mínimos previstos en los capítulos II y III del real decreto. Como parte integral de la Declaración de Aplicabilidad se indicará de forma detallada la correspondencia entre las medidas compensatorias implantadas y las medidas del Anexo II que compensan y el conjunto será objeto de la **aprobación formal por parte del responsable de seguridad** (art. 28.3 RD 311/2022)

Además de ello, conforme al **Real Decreto-ley 12/2018, de 7 de septiembre**, de seguridad de las redes y sistemas de información y el **Real Decreto 43/2021, de 26 de enero**, por el que se desarrolla el anterior (que transponen al ordenamiento jurídico español la Directiva 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) en lo que sea de aplicación a la organización, la figura del Responsable de la Seguridad del ENS podrá desplegar las siguientes funciones:

- 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 ciber incidentes 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 RD-Ley 12/2018 y de su Reglamento de desarrollo.
- Constituir el punto de contacto especializado para la coordinación con el CSIRT de referencia.
- 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.

Responsable del sistema

Tiene las siguientes funciones:

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad.
- Recibir los informes de auditoría y adoptar las medidas correctoras adecuadas con las conclusiones aportadas por el responsable de seguridad.
- El Responsable del Sistema puede proponer la suspensión del tratamiento de una cierta información o la prestación de un determinado servicio si aprecia deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. La decisión final, que será tomada por la Dirección Gerencia de la entidad, debe ser acordada con los responsables de la información y los servicios afectados y el Responsable de la Seguridad.

Delegado de protección de datos

MUTUALIA tiene nombrado su Delegado de Protección de Datos, y comunicado en tiempo y forma su designación ante la Agencia Española de Protección de Datos (autoridad de control competente), para que participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales, en general con la **posición** y para el desempeño de las **funciones** que tiene legalmente establecidas por los **arts. 38 y 39 del RGPD y art. 36 y 37 de la LOPDGDD**.

Las personas interesadas, por lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos al amparo del RGPD y la LOPDGDD, podrán ponerse en contacto a través de la cuenta de correo: dpd@mutualia.eus/es

CUADRO DE REGISTRO DE REVISIONES

	FECHA	CONTENIDO DE LA REVISIÓN
	04/02/2022	Edición
	21/12/2023	Actualización conforme al RD 311/2022