Mutua Universal

Política de Seguridad de la Información

1. Introducción 2
2. Misión de la Entidad 2
3. Marco regulatorio 2
4. Principios básicos y requisitos mínimos de seguridad 2
5. Organización de la seguridad de la información 4
   5.1. Estructura de comités para la gestión y coordinación de la seguridad 4
   5.2. Roles o funciones de seguridad 4
6. Estructuración y gestión de la normativa de seguridad 5
7. Gestión de riesgos del tratamiento de datos personales 6
8. Incumplimientos 7
9. Aprobación y entrada en vigor 7

ANEXO 1. Glosario de términos 8
ANEXO 2. Listado del marco regulatorio aplicable a Mutua Universal 10
ANEXO 3. Principios básicos del Esquema Nacional de Seguridad 11
ANEXO 4. Objetivos, funciones y composición de los comités 12
   A. Comité de Gobierno de Seguridad Corporativa (CGSC) 12
   B. Comité de Seguridad de la Información 13
ANEXO 5. Responsabilidades de los roles y comités de seguridad de la información 15

1. Introducción

Mutua Universal reconoce la importancia que tiene la seguridad de la información para la correcta realización de sus actividades. Por ello, desarrolla esta Política de Seguridad de la Información, en adelante PSI, donde se establecen el conjunto de directrices que rigen la forma en que la organización gestiona y protege la información que trata y los servicios que presta.

Mutua Universal depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar la misión de la Entidad. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la **confidencialidad**, **integridad**, **disponibilidad**, **autenticidad** o **trazabilidad** de la información tratada o a los servicios prestados.

La presente política aplica a todas las actividades relacionadas con el uso, la administración y la protección de la información de la Entidad, y afecta a todo el personal, propio y externo, que presten servicios o dispongan de acceso a la información o a los activos relacionados con ésta, como consecuencia del ejercicio de sus funciones o de la ejecución de un contrato.

En el ANEXO 1. Glosario de términos se encuentran los principales conceptos relacionados con la seguridad de la información que se utilizarán en este documento de política, por lo que se recomienda su lectura para la mejor comprensión de este documento.

2. Misión de la Entidad

Velar por la salud y el bienestar de nuestros Mutualistas, gestionando los servicios y las prestaciones con rigurosidad y excelencia, comprometidos con la sociedad y la sostenibilidad del sistema.

3. Marco regulatorio

La regulación que afecta al desarrollo de las actividades y competencias de Mutua Universal sobre medios digitales, y la implantación de medidas de seguridad en los correspondientes sistemas de información, está constituida por la legislación identificada en el ANEXO 2. Listado del marco regulatorio aplicable a Mutua Universal.

El conjunto de principios básicos y directrices a los que la organización se compromete en esta PSI están alineados con el marco del Esquema Nacional de Seguridad (en adelante, ENS), regulado por el Real Decreto 311/2022, de 3 de mayo, que ofrece un marco común de principios básicos, requisitos y medidas de seguridad para una protección adecuada de la información tratada y los servicios prestados.

Mutua Universal tendrá en cuenta en su operativa habitual las guías de seguridad del Centro Criptológico Nacional (CCN) así como las actualizaciones de dichas guías que sean de aplicación para alinearse con el cumplimiento de lo establecido en el ENS.

4. Principios básicos y requisitos mínimos de seguridad

Mutua Universal vela por disponer de las medidas de seguridad proporcionales a la naturaleza de la información y los servicios a proteger de acuerdo con los **principios básicos** señalados en el capítulo II del Real Decreto 311/2022 (ver ANEXO 3. Principios básicos del Esquema Nacional de Seguridad) y se desarrollará aplicando los siguientes **requisitos mínimos** (capítulo III de dicho RD):

a) **Organización e implantación del proceso de seguridad**, comprometiendo a todos los miembros de la organización con la seguridad de la información e identificando a los responsables de velar por ella.

b) **Análisis y gestión de los riesgos**, que se llevará a cabo en base a metodologías reconocidas internacionalmente y tomando medidas que permitan mitigar o suprimir los riesgos identificados.

c) **Gestión de personal**, formando e informando al personal relacionado con la información y los sistemas sobre sus deberes y obligaciones en materia de seguridad, de tal modo que dicho personal sea capaz de aplicar los principios de seguridad en el desempeño de su cometido.

d) **Profesionalidad**, revisando y auditando la seguridad de la información con perfiles capacitados, formando al personal en materia de seguridad y contratando servicios que cuenten con profesionales cualificados.

e) **Autorización y control de los accesos**, controlando el acceso a los sistemas de información de tal modo que solo puedan acceder los usuarios, procesos, dispositivos u otros sistemas debidamente autorizados.

f) **Mínimo privilegio**, proporcionando únicamente los permisos mínimos necesarios por perfil para que la organización alcance sus objetivos.

g) **Protección de las instalaciones**, implantando controles de acceso físico basados en gestión de identidades y controles de protección frente a amenazas físicas y ambientales.

h) **Adquisición de productos de seguridad y contratación de servicios de seguridad**, contratando e integrando productos o servicios que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición o contratación, y de forma proporcionada a la categoría del sistema y el nivel de seguridad determinados. Salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen, a juicio del responsable de Seguridad de la Información (ver CISO en apartado Roles o funciones de seguridad), bajo la óptica de alineamiento con el ENS.

i) **Integridad y actualización del sistema de información**, aplicando mecanismos formales para la instalación de cualquier elemento físico (como servidores o equipamiento de red) o lógico (como software) en el sistema, así como los parches de seguridad y actualizaciones garantizando su procedencia legítima y debida diligencia.

j) **Protección de la información almacenada y en tránsito**, prestando especial atención a la información en dispositivos periféricos, comunicaciones en redes abiertas o con cifrado débil, asegurando el correcto funcionamiento de los procedimientos de copia de seguridad y restauración.

k) **Prevención ante otros sistemas de información interconectados**, protegiendo el perímetro, en particular, en conexiones con redes públicas y analizando riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, controlando su punto de unión.

l) **Registro de la actividad**, habilitando registros de la actividad de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades ilegítimas, indebidas o no autorizadas, así como permitiendo identificar en cada momento a la persona que actúa.

m) **Detección de código dañino**, implementando medidas para identificar y contener software malicioso que pueda comprometer la seguridad de los sistemas y la información.

n) **Incidentes de seguridad**, estableciendo medidas de detección y respuesta que permitan cubrir los plazos requeridos para el negocio y normativa aplicable.

o) **Continuidad de la actividad**, disponiendo de copias de seguridad y estableciendo los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales de trabajo.

p) **Mejora continua del proceso de seguridad**, actualizando y mejorando de forma continua el proceso de la gestión de la seguridad de la información.

5. Organización de la seguridad de la información

5.1. Estructura de comités para la gestión y coordinación de la seguridad

El Comité de Dirección (CD) de Mutua Universal es responsable de crear el Comité de Seguridad de la Información y el de Gobierno de Seguridad Corporativa, así como de nombrar a los responsables de estos comités. Estas decisiones se comunican a las partes involucradas.

Comités	Misión
Comité de Seguridad de la Información (CSI)	Tiene como finalidad tratar los temas concernientes a la seguridad de la información de la organización, velar por la seguridad de sus servicios y activos de información, asegurando y facilitando la correcta coordinación e integración de todas las actuaciones en esta materia. Coordina y resuelve conflictos sobre la interpretación y aplicación de esta Política, escalándolos al Comité de Gobierno de Seguridad Corporativa si fuese necesario.
Comité de Gobierno de Seguridad Corporativa (CGSC)	Tiene como finalidad aprobar las medidas de seguridad propuestas por el Comité de Seguridad de la Información (CSI), supervisar su implementación, asignar recursos necesarios y asegurar el cumplimiento de las normativas en Mutua Universal y constituirse como **comité de crisis** ante ciberincidentes muy graves o críticos.

Se presenta más detalle sobre objetivos, funciones y composición de los comités en *ANEXO 4.* Objetivos, funciones y composición de los comités

5.2. Roles o funciones de seguridad

La organización de la seguridad de la información en Mutua Universal se establece en la forma y reparto de roles y responsabilidades que se indica a continuación:

Roles de seguridad de la información	
DG: Director Gerente	Máximo responsable de la organización en aspectos de seguridad corporativa, incluyendo la responsabilidad sobre el desarrollo de las competencias de la seguridad de la información y la implantación del ENS.
Responsables de la Información **(RINFO): DF's**	Los **directores funcionales** son los responsables finales del uso de los Activos de Información[1] del sistema y de su protección. Se encargan de validar los requisitos y niveles de seguridad de la información dentro del marco establecido en el ENS, previa propuesta del Comité de Seguridad de la Información. Algunos Directores Funcionales tienen activos de información directamente vinculados a ellos, mientras que otros activos pueden depender de varios Directores Funcionales. Esta relación se refleja en el documento de Categorización del Sistema[2] acorde al ENS.
Responsables de los servicios **(RSERV): CGSC**	Directores de servicio, responsables de aprobar las medidas de seguridad, supervisar su implementación, asignar los recursos necesarios y asegurar el cumplimiento de las normativas en Mutua Universal. Tienen la competencia de decidir sobre la finalidad y prestación de los servicios y determinar sus niveles

[1,2] Ver ANEXO 1. Glosario de términos.

	de seguridad dentro del marco del ENS, previa propuesta del CSI (ver Estructura de comités para la gestión y coordinación de la seguridad). Este rol corresponde al **Comité de Gobierno de la Seguridad Corporativa**.
Responsable de Seguridad de la Información **(RSI): CISO**	Determina las decisiones de seguridad para satisfacer los requisitos establecidos por los Responsables de los Servicios y de la Información, vela por la coherencia y armonización de las normas, procedimientos y actuaciones de la organización en los diferentes ámbitos. Este rol recae en el **Director de Ciberseguridad (CISO).**
Responsable del Sistema de Información **(RSIS): CTO**	Se encarga de la operación de los sistemas de información, atendiendo a las medidas de seguridad determinadas por el Responsable de la Seguridad. Este rol recae en el **Director de Tecnología de Mutua Universal (CTO).**
DPD: Delegado de Protección de Datos	Vela por la adecuada aplicación de la normativa vigente en materia de protección de datos, a través del asesoramiento, supervisión continua de su cumplimiento y cooperación con la autoridad de control correspondiente.
ASI: Administrador de Seguridad de la Información	Miembro de la estructura organizativa que trabaja bajo la supervisión del CISO, y que es designado por el propio CISO.
ASIS: Administrador de sistemas de Información	Miembro de la estructura organizativa que trabaja bajo la supervisión del CTO, y que es designado por el propio CTO.
RSF: Responsable de Seguridad Física	Miembro de la estructura organizativa que vela por la implementación y gestión de controles de la seguridad de la información en el ámbito de la seguridad física, licitando, contratando y supervisando los servicios de seguridad física para prevenir, detectar y responder a amenazas físicas y medioambientales.

En el ANEXO 5. Responsabilidades de los roles y comités de seguridad de la información se definen detalladamente las funciones de estos perfiles.

6. Estructuración y gestión de la normativa de seguridad

Mutua Universal diseña, mantiene e impulsa un cuerpo normativo interno aplicable al ámbito de la seguridad de la información, y a los órganos de dirección y gestión, empleados y proveedores externos. El cuerpo normativo se desarrolla en cinco niveles con diferente ámbito de aplicación, nivel de detalle técnico y obligatoriedad de cumplimiento, estando cada elemento normativo fundamentado o alineado en las normas de nivel superior:

Nivel 1	La presente **política de seguridad de la información (PSI)**
Nivel 2	**Normas de seguridad de la información**. Son de obligado cumplimiento en toda Mutua Universal, en los elementos que apliquen a cada centro de trabajo.
Nivel 3	**Procedimientos generales**, de aplicación sobre la organización en su conjunto. Describen las acciones a realizar en un proceso relacionado con la seguridad.

Nivel 4	**Procedimientos específicos**. Describen las acciones a realizar en un proceso relacionado con la seguridad, responsabilidad de una unidad organizativa, dentro de un mismo centro de trabajo.
Nivel 5	**Informes, registros, evidencias electrónicas y plantillas**. Los informes son documentos de carácter técnico que recogen el resultado y las conclusiones de un estudio o de una evaluación. Los registros de actividad o alertas de seguridad son documentos de carácter técnico que recogen amenazas y vulnerabilidades a sistemas de información y son responsabilidad del equipo de seguridad. Las evidencias electrónicas se generan durante todo el ciclo de vida de los sistemas de información, pudiendo abarcar uno o más sistemas en función del aspecto tratado.

El Comité de Seguridad de la Información (CSI) establecerá los mecanismos necesarios para compartir la documentación derivada del desarrollo normativo con el propósito de normalizarlo, en la medida de lo posible, en todo el ámbito de aplicación de la PSI.

La siguiente tabla resume el marco normativo y la responsabilidad de su propuesta, revisión y aprobación.

Nivel Normativo	Documento	Propone	Revisa	Aprueba
Primero.	Política de Seguridad de la información.	CISO	CGSC	DG
Segundo.	Normas de Seguridad de la información.	CISO	CTO	CSI
Tercero.	Procedimientos generales de seguridad de la información.	CTO/CISO	CSI	CISO/CTO
Cuarto.	Procedimientos específicos e instrucciones técnicas de seguridad de la información.	ASI/ASIS	CISO/CTO	CTO/CISO
Quinto.	Informes, registros, evidencias y plantillas.	ASI / ASIS	CTO / CISO	CISO /CTO

Para la mejor comprensión de la tabla, se recomienda revisar el apartado Roles o funciones de seguridad.

7. Gestión de riesgos del tratamiento de datos personales

Mutua Universal dispone de dos políticas con relación a la gestión de riesgos relativos al tratamiento de datos personales:

- la Política de Gestión de Riesgos, que abarca todos los riesgos corporativos entre los que se encuentran:
  - Riesgos de Seguridad Informática (operacional),
  - Riesgo sobre la protección de datos y seguridad de la información (de información),
  - Riesgo sobre la normativa de protección de datos y seguridad de la información (de cumplimiento)

- la política del Sistema Interno de Gestión de Protección de Datos, que regula los riesgos derivados de las evaluaciones de impacto -PIA- y los derivados de los incidentes de seguridad (de acuerdo con los correspondientes articulados del RGPD).

8. Incumplimientos

Ningún usuario deberá atender a solicitudes, instrucciones u órdenes contrarias a la PSI o a normativa de seguridad de la información de Mutua Universal, ni podrán ampararse en ellas como justificación de cualquier incumplimiento. Únicamente por motivos excepcionales y debidamente justificados, como los requerimientos de autoridades administrativas, inspectoras o judiciales, cabe la posibilidad de contravenir lo establecido en ella.

Cualquier incidencia o situación relacionada con esta política se deberá comunicar a través de la dirección de correo: *ciberseguridad@mutuauniversal.net*

Los incumplimientos por parte del personal sobre lo establecido en la presente política y la normativa de seguridad de la información asociada podrán ser sancionados con arreglo a la normativa vigente, sin perjuicio de otras responsabilidades en el que el infractor hubiera podido concurrir.

9. Aprobación y entrada en vigor

Texto aprobado el día 9 de octubre del 2024 por el Director Gerente y el Director de Digitalización y Tecnología.

Esta PSI es efectiva desde su fecha de publicación y hasta que sea reemplazada por una nueva.

ANEXO 1. Glosario de términos

- **Activo / Activo de Información**: componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.
- **Amenaza:** Cualquier circunstancia o evento con el potencial de causar daño a un sistema de información, afectando la confidencialidad, integridad, disponibilidad, autenticidad o trazabilidad de la información.
- **Amenazas físicas y medioambientales**: Factores externos que pueden causar daño a los sistemas de información y a los activos de la organización. Incluyen riesgos como incendios, inundaciones, terremotos, robos, vandalismo, fallos en el suministro eléctrico y otras condiciones ambientales adversas.
- **Autenticación:** Proceso de verificar la identidad de un usuario, dispositivo o entidad antes de permitir el acceso a un sistema de información.
- **Autorización:** Proceso de conceder permisos a un usuario, dispositivo o entidad para acceder a recursos específicos dentro de un sistema de información.
- **Categoría de seguridad de un sistema**: es un grado, dentro de la escala Básica-Media-Alta, con el que se adjetiva un sistema de información a fin de seleccionar las medidas de seguridad necesarias para el mismo. La categoría de seguridad del sistema recoge la visión holística del conjunto de activos como un todo armónico, orientado a la prestación de unos servicios.
- **Categorización del sistema**: Proceso de clasificación de un sistema de información según su nivel de seguridad requerido (Básica, Media, Alta), basado en una evaluación integral de sus activos y su importancia para la organización. Esta categorización determina las medidas de seguridad necesarias para proteger el sistema, alineándose con las directrices del Esquema Nacional de Seguridad (ENS).
- **Dimensiones de seguridad:** Propiedades de los activos del sistema de información que requieren protección. En el ENS se consideran las siguientes:
    - **Autenticidad**: propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
    - **Confidencialidad:** propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.
    - **Disponibilidad**: propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.
    - **Integridad**: propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
    - **Trazabilidad**: propiedad o característica consistente en que las actuaciones de una entidad (persona o proceso) pueden ser trazadas de forma indiscutible hasta dicha entidad.
- **Incidente de seguridad (ciberincidente o incidente):** suceso inesperado o no deseado con consecuencias en detrimento de la seguridad de las redes y sistemas de información.
- **Medidas de seguridad:** Conjunto de controles, procedimientos y mecanismos implementados para proteger los sistemas de información contra amenazas y vulnerabilidades.
- **Naturaleza de la información:** Conjunto de cualidades de la información que determinan su grado de criticidad para la organización.

- **Política de seguridad:** Conjunto de directrices y normas establecidas por una organización para proteger sus sistemas de información y garantizar el cumplimiento de las regulaciones aplicables.
- **Principios básicos de seguridad:** fundamentos que deben regir toda acción orientada a asegurar la información y los servicios.
- **Proceso de seguridad:** método que se sigue para alcanzar los objetivos de seguridad de la organización. El proceso se diseña para identificar, medir, gestionar y mantener bajo control los riesgos a que se enfrenta el sistema en materia de seguridad.
- **Riesgo de seguridad:** Posibilidad de que una amenaza explote una vulnerabilidad causando un impacto negativo en un sistema de información.
- **Seguridad de la información:** Preservación de la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información y de los sistemas de los que esta depende.
- **Servicio:** Organización, procesos, sistemas de información y personal destinados a cubrir unas necesidades con la entidad beneficiaria.
- **Sistema de información:** cualquiera de los elementos siguientes:
    - Las redes de comunicaciones electrónicas que utilice la organización sobre las que posea capacidad de gestión.
    - Todo dispositivo o grupo de dispositivos interconectados o relacionados entre sí, en el que uno o varios de ellos realicen, mediante un programa, el tratamiento automático de datos digitales.
    - Los datos digitales almacenados, tratados, recuperados o transmitidos mediante los elementos contemplados en los puntos anteriores, incluidos los necesarios para el funcionamiento, utilización, protección y mantenimiento de dichos elementos.
- **Vulnerabilidad:** Debilidad en un sistema de información que puede ser explotada por una amenaza para causar un impacto negativo.

ANEXO 2. Listado del marco regulatorio aplicable a Mutua Universal

ENS y Seguridad de la información:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.
- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.
- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.

Protección de datos personales:

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, RGPD).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Otros:

- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.
- Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.

ANEXO 3. Principios básicos del Esquema Nacional de Seguridad

En materia de gestión de la seguridad de la información Mutua Universal contempla los siguientes principios básicos del Esquema Nacional de Seguridad:

a) **Seguridad como proceso integral** constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información. Asimismo, se prestará la máxima atención a la concienciación de perfiles que intervienen en el proceso de seguridad para evitar la exposición a fuentes de riesgo para la seguridad.

b) **Gestión de la seguridad basada en los riesgos** como actividad continua y permanentemente actualizada. Esta gestión permitirá minimizar los riesgos a niveles aceptables, mediante la aplicación de medidas de seguridad de manera equilibrada y proporcionada a la naturaleza de la información tratada, los servicios prestados y los riesgos a los que se exponen.

c) Aplicación de medidas de **prevención, detección, respuesta y conservación** para minimizar las vulnerabilidades y lograr que las amenazas no se materialicen o al menos, no afecten gravemente a la información o servicios.

d) **Existencia de líneas de defensa** compuesta por múltiples capas de seguridad de forma que el compromiso de una de las capas no suponga el compromiso del sistema en su conjunto o minimice el impacto final. Las líneas de defensa contemplan medidas de naturaleza organizativa, física y lógica.

e) **Vigilancia continua y reevaluación periódica** para la detección de actividades o comportamientos anómalos y su oportuna respuesta. Así como la evaluación permanente del estado de la seguridad y actualización periódica de las medidas aplicadas.

f) **Diferenciación de responsabilidades** en los sistemas de información distinguiendo el responsable de la información, el responsable del servicio, el responsable de la seguridad y el responsable del sistema. Contemplando la diferenciación de la responsabilidad de la seguridad de los sistemas de información y la responsabilidad sobre su explotación.

ANEXO 4. Objetivos, funciones y composición de los comités

A. Comité de Gobierno de Seguridad Corporativa (CGSC)

Su propósito es establecer la colaboración formal en las funciones de gobierno para alcanzar una gestión eficaz en cumplimiento de los objetivos siguientes:

a) Mantener las políticas de ciberseguridad para Mutua Universal.

b) Mantener un marco de Gobierno de la Seguridad que alinee la estrategia y actuaciones en ciberseguridad con los objetivos de Mutua Universal.

c) Asegurar que las medidas de ciberseguridad estén alineadas con la misión y objetivos estratégicos de Mutua Universal.

d) Establecer una visión común sobre los riesgos específicos de ciberseguridad en la organización que permita integrar la gestión de riesgos de ciberseguridad en todas las áreas y actividades de Mutua Universal.

e) Asegurar la implementación y operación adecuada de las medidas de mitigación de riesgos de ciberseguridad.

f) Garantizar el cumplimiento de los requerimientos legales y regulatorios en materia de ciberseguridad.

g) Fomentar una cultura corporativa de ciberseguridad.

Son funciones de este comité de gobierno las siguientes:

a) Definir y aprobar políticas de ciberseguridad.

b) Aprobar niveles de riesgo de ciberseguridad y riesgos residuales, y aceptar el riesgo no tratado.

c) Aprobar planes de protección en ciberseguridad para mantener bajo control los riesgos identificados.

d) Asignar roles en los distintos ámbitos de ciberseguridad, garantizando la segregación de tareas.

e) Asignar recursos, atender incidentes de ciberseguridad y dirigir la planificación y entrenamiento de la continuidad de las actividades relacionadas con la ciberseguridad.

f) Asegurar que el Comité de Seguridad de la Información (CSI) cuente con los recursos necesarios para su actividad.

g) Supervisar los planes de contingencia en ciberseguridad y su correcta ejecución en caso de materialización de riesgos.

h) Evaluar información sobre peligros de ciberseguridad y revisar los límites de exposición a las amenazas.

i) Supervisar las acciones de prevención y cumplimiento de los objetivos de ciberseguridad.

El Comité debe contar, como mínimo, con miembros que tengan responsabilidades de alta gerencia o, en su caso, delegadas, para disponer de la potestad de aprobar inversiones y tomar decisiones al más alto nivel de la empresa. Como la responsabilidad última recae en Mutua Universal y sus apoderados, el Comité debe incluir al menos representación de la dirección, de la gerencia y de aquellos miembros de la dirección cuya función esté relacionada con la gestión y protección de la información de Mutua Universal.

El Comité de Gobierno de la Seguridad Corporativa se constituye con los siguientes **cargos permanentes:**

- Comité de Dirección

- Responsable del Sistema – Director de Tecnología
- Delegado de Protección de Datos - DPD
- Responsable de Seguridad – CISO
- Responsable de Seguridad física

B. Comité de Seguridad de la Información

El Comité de Seguridad de la Información es el comité ejecutivo competente para las decisiones que satisfacen los requisitos de seguridad de la información, y de los servicios y las tecnologías relacionados, bajo las directrices generales marcadas por el Comité de Gobierno de Seguridad Corporativa. Además, supervisa dichas decisiones, con la delegación funcional en administradores y operadores bajo su control. El comité tiene las siguientes funciones:

a) Garantizar y aprobar las normativas que se desarrollan a partir de la Política de Seguridad de la Información de Mutua Universal.

b) Impulsar el cumplimiento de la Política de Seguridad de la Información de Mutua Universal y su desarrollo normativo.

c) Apoyar la coordinación, cooperación y colaboración con otras Mutuas, Administraciones Públicas y Grupos de Interés en materia de Seguridad de la Información.

d) Tomar aquellas decisiones que garanticen la seguridad de la información y de los servicios digitales de Mutua Universal.

e) Resolver los conflictos de competencia que pudieran aparecer entre los diferentes responsables, órganos de dirección y gestión, y entre diferentes áreas de Mutua Universal, en materia de seguridad de la información, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

f) Compartir experiencias de éxito en materia de seguridad entre sus miembros para velar por el cumplimiento de la Política de Seguridad de la Información y su normativa de desarrollo.

g) Definir, dentro del marco establecido por la Política de Seguridad de la Información de Mutua Universal, la asignación de roles y los criterios para alcanzar las garantías que estime pertinentes en lo relativo a la segregación de tareas.

h) Coordinar y aprobar, en su caso, las propuestas de proyectos recibidas del ámbito de la seguridad de la información y tecnologías de la información, encargándose de gestionar un control y presentación regular del progreso de los proyectos y anuncio de las posibles desviaciones al Comité de Dirección de Mutua Universal.

i) Recibir las inquietudes de cualquier miembro de la organización o parte interesada en cuanto a seguridad de la información y tecnología de soporte, analizar y recabar las correspondientes respuestas y soluciones.

j) Recabar, a través de los responsables de seguridad y de servicios TI de Mutua Universal, informes regulares del estado de la seguridad de la organización y de los posibles incidentes, para poder adoptar las decisiones oportunas.

k) Promover la mejora continua en la gestión de la seguridad de la información.

l) Fijar y proponer los niveles de riesgos y los riesgos residuales, para cualquier esfera de seguridad, y aceptar el riesgo no tratado.

m) Fijar y proponer los planes de protección que evalúan y mantienen bajo control los riesgos identificados.

n) Definir y asignar los roles en los distintos ámbitos de seguridad, en base a criterios de garantía en lo relativo a la segregación de tareas, y en cumplimiento de las normativas de Protección del

ENS, y cualquier otra norma o necesidad que Mutua Universal requiera la designación para el desarrollo de una función relacionada con la seguridad.

o) Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.

p) Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.

El Comité de Seguridad de la Información se constituye con los siguientes **cargos permanentes**:

- Director/a de Digitalización y Tecnología, (CIO) quien será el PRESIDENTE.
- Director/a Técnico de Ciberseguridad (Responsable de Seguridad o CISO), quien será el SECRETARIO.
- Director/a de Tecnología (Responsable del Sistema, CTO).
- Delegado de Protección de Datos, (DPO)

Serán **miembros transitorios** (convocados a criterio, individual o colegiado, de los miembros permanentes):

- Director/a de Análisis y Desarrollo
- Director/a de Digitalización
- Responsable de Seguridad física.

ANEXO 5. Responsabilidades de los roles y comités de seguridad de la información

A continuación, se exponen las funciones principales en el ámbito de la seguridad de la información y el ENS a través de la matriz RACI de asignación de responsabilidades:

- R (Responsable): Realiza la tarea y es responsable de su ejecución.
- A (Autoriza): Autoriza y aprueba la tarea a ejecutar. Debe asegurar que se ejecutan las tareas.
- C (Consultado): Se le consulta para la toma de decisiones asociadas a la tarea.
- I (Informado): Se le informa sobre las decisiones tomadas.

FUNCIONES	DG	CGSC	DFs	CISO	ASI	CTO	ASIS	DPD	CSI	RSF
Niveles de seguridad requeridos por la información		I	A	R		C		C	C	
Niveles de seguridad requeridos por el servicio		A	I	R		C		C	C	
Determinación de la categoría del sistema		I	I	R		C		C	A	
Análisis de riesgos		I	I	R		C		C	A	
Declaración de aplicabilidad		I	I	R		C		C	A	
Medidas de seguridad adicionales		I	I	R		C		C	A	
Configuración de la seguridad				A	C	C	R	C	I	
Aceptación del riesgo residual		A	A	R		I		I	I	
Política de seguridad de la información	A	C	C	R		C		C	C	
Normativa de seguridad de la información				R		C		C	A	
Procedimientos generales de seguridad de la información				C		A	R	C	I	
Procedimientos específicos e instrucciones técnicas de seguridad de la información				C		A	R	C		

FUNCIONES	DG	CGSC	DFs	CISO	ASI	CTO	ASIS	DPD	CSI	RSF
Implantación de medidas de seguridad de la información				C		A	R		I	
Contratación de la implantación y supervisión de medidas y servicios de seguridad físicas				C					I	R/A
Supervisión de las medidas de seguridad de la información				A	C	I	R		I	
Estado de seguridad del sistema				A	C	I	R		I	
Planes de mejora de la seguridad de la información				A	R	C			I	
Planes de concienciación y formación				A	R	C			I	
Planes de continuidad				C		A	R		I	
Suspensión cautelar del servicio		A		C		C	R	C		
Seguridad en el ciclo de vida de sistemas de información				C		A	R		I	