Mutua Universal

Declaración de la Política de la Seguridad de la Información

1. Introducción

Mutua Universal tiene como misión velar por la salud y el bienestar de las personas trabajadoras, gestionando los servicios y las prestaciones con responsabilidad y eficiencia, comprometidos con la sociedad y la sostenibilidad del sistema. La seguridad de la información constituye un pilar esencial para garantizar la continuidad, calidad y confianza en los servicios prestados por Mutua Universal.

Mutua Universal adopta el Esquema Nacional de Seguridad (ENS) como marco de referencia para la protección de la información y los servicios electrónicos y garantiza la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información y de los servicios prestados.

2. Objetivo y alcance

La Política de la Seguridad de la Información establece un conjunto de directrices que rigen la forma en que la organización gestiona y protege la información que trata y los servicios que presta, de acuerdo con el marco regulatorio aplicable y vigente en cada momento.

El alcance de la Política de la Seguridad de la Información 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.

3. Principios básicos y requisitos mínimos de seguridad

Mutua Universal dispone 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 y se desarrolla aplicando los siguientes **requisitos mínimos**:

- **Gobernanza de la seguridad**, definiendo responsables e implicando a toda la organización.
- **Gestión de riesgos**, identificando, evaluando y mitigando amenazas con metodologías reconocidas.
- **Gestión de personas**, formando y concienciando al personal en seguridad de la información.
- **Profesionalización**, asegurando la participación de perfiles cualificados y auditorías periódicas.
- **Control de accesos**, limitando el acceso a usuarios, sistemas y dispositivos autorizados.
- **Mínimo privilegio**, asignando únicamente los permisos imprescindibles según el rol.
- **Protección física**, controlando accesos a instalaciones y previniendo amenazas ambientales.
- **Adquisición segura**, incorporando productos y servicios con garantías certificadas de seguridad.
- **Integridad y actualización**, gestionando cambios y aplicando parches de forma controlada.
- **Protección de la información**, asegurando los datos en reposo, en tránsito y en copias de seguridad.
- **Seguridad en interconexiones**, protegiendo el perímetro y controlando conexiones externas.

- **Registro de actividad**, monitorizando y trazando acciones para su análisis e investigación.
- **Protección frente a malware**, detectando y conteniendo software malicioso.
- **Gestión de incidentes**, detectando, respondiendo y resolviendo eventos de seguridad.
- **Continuidad de negocio**, garantizando la operativa ante fallos o incidentes.
- **Mejora continua**, revisando y evolucionando constantemente la seguridad.
- **IA responsable**, aplicando estos principios al diseño, desarrollo y uso de sistemas de inteligencia artificial.

4. Modelo de gobernanza

Mutua Universal dispone de los roles de seguridad definidos por el Esquema Nacional de Seguridad, incluyendo las responsabilidades relativas a la información, los servicios, la seguridad y los sistemas, cuyas funciones y atribuciones se desarrollan en la normativa interna correspondiente.

Asimismo, dispone de un modelo de gobernanza de la seguridad de la información que se articula a través de los siguientes órganos de gobierno:

Comité de Seguridad de la Información (CSI)

Órgano responsable 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 la Política de la Seguridad de la Información, escalándolos al Comité de Gobierno de Seguridad Corporativa si fuese necesario.

Comité de Gobierno de Seguridad Corporativa (CGSC)

Órgano encargado 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.

5. Estructura 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, personal de la entidad/plantilla y proveedores externos. El cuerpo normativo se desarrolla en cinco niveles con diferentes ámbitos de aplicación, nivel de detalle técnico y obligatoriedad de cumplimiento, estando cada elemento normativo fundamentado o alineado en las normas de nivel superior.

6. 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:

- 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)
- 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).

7. Régimen disciplinario e incumplimientos

Los incumplimientos sobre lo establecido en la presente declaración y la política de seguridad de la información asociada podrán ser sancionados con arreglo a la normativa vigente, sin perjuicio de las responsabilidades legales, contractuales o disciplinarias que pudieran corresponder.

Juan Güell Ubillos
Director General
15 de mayo de 2026