UNIÓN DE MUTUAS
Mutua Colaboradora con la Seguridad Social N.º 267

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE UNIÓN DE MUTUAS

UNIÓN DE MUTUAS, mutua colaboradora con la Seguridad Social n.º 267, es una asociación de empresas, sin ánimo de lucro, que colabora en la gestión de la Seguridad Social conforme a lo establecido en la legislación vigente, prestando sus servicios a sus empresas asociadas, trabajadores por cuenta propia adheridos y trabajadores por cuenta ajena protegidos. Todo ello basado en un modelo de gestión de la excelencia y buen gobierno, contribuyendo de esta manera a un mayor bienestar social, en términos de sostenibilidad.

Para sustentar el desarrollo de la presente Política de Seguridad, Unión de Mutuas asume una serie de objetivos estratégicos entre los cuales se encuentra el disponer de los recursos necesarios para analizar, evaluar y tratar los riesgos a los que están expuestos los activos de la organización que afectan a la seguridad de la información en las dimensiones de disponibilidad, integridad, confidencialidad, trazabilidad y autenticidad.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con celeridad a los incidentes. La protección frente a cualquier amenaza identificada requiere la implantación de una serie de medidas de seguridad que deben establecerse conforme a la legislación vigente en materia de protección de datos, el resultado del análisis de riesgos de la entidad y las propias medidas del Esquema Nacional de Seguridad.

Esta Política de Seguridad es de aplicación a todos los procesos estratégicos, operativos y de apoyo, a todos sus sistemas de tecnologías de la información y de las comunicaciones y a todos los centros y personal de Unión de Mutuas, conforme a la Declaración de Aplicabilidad del Sistema de Gestión de la seguridad de la información y a una categorización de los sistemas de nivel ALTO según directrices del Esquema Nacional de Seguridad.

Unión de Mutuas considera estratégico para la entidad que los procesos integren la seguridad de la información como parte de su ciclo de vida. Los sistemas de información y los servicios deben incluir la seguridad por defecto desde su creación hasta su retirada, incluyéndose la seguridad en las decisiones de desarrollo y/o adquisición y en todas las actividades en explotación estableciéndose la seguridad como un proceso integral y transversal.

Unión de Mutuas basa su gestión de la seguridad en la Gestión del Riesgo por lo que todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos que se reevaluará y actualizará periódicamente, en base a metodología de gestión del riesgo reconocida internacionalmente cuya implementación se encuentra desarrollada en el sistema de gestión documental de la entidad y disponible a través de la intranet corporativa para todo el personal.

En Unión de Mutuas se han implementado con carácter preventivo todas aquellas medidas de seguridad derivadas del cumplimiento normativo en protección de datos, las guías de controles de la norma de gestión ISO27001 y las contempladas en el Esquema Nacional de Seguridad según la categorización de los sistemas. La organización ha implementado los controles necesarios para:

- monitorizar los sistemas que dan soporte a los servicios de modo que se pueda obtener una detección temprana de los incidentes de seguridad.
- dar respuesta de forma eficaz a los incidentes de seguridad detectados.
- y aportar continuidad a los servicios dentro del Plan de contingencias y Continuidad de Negocio de la entidad.

La presente Política se desarrollará aplicando los siguientes requisitos mínimos:

a) Organización e implantación del proceso de seguridad.
b) Análisis y gestión de los riesgos.
c) Gestión de personal.
d) Profesionalidad.
e) Autorización y control de los accesos.
f) Protección de las instalaciones.
g) Adquisición de productos.
h) Seguridad por defecto.
i) Integridad y actualización del sistema.
j) Protección de la información almacenada y en tránsito.

k) Prevención ante otros sistemas de información interconectados.

l) Registro de actividad.

m) Incidentes de seguridad.

n) Continuidad de la actividad.

o) Mejora continua del proceso de seguridad.

Estos requisitos se encuentran desplegados en la normativa y procedimientos de seguridad específicos para la implementación de las medidas de seguridad que son de aplicación para el ENS y su desarrollo se encuentra descrito en los documentos de operativa y las normas de aplicación incluidas y estructuradas en la Gestión Documental de la entidad. Esta documentación se encuentra disponible a través de la intranet corporativa para todo el personal, estando en coherencia y conforme a los requisitos de implementación del Reglamento General de Protección de Datos (RGPD) y de otras normas de gestión en las que la entidad está certificada.

Esta Política de seguridad se complementa con la Política de alto nivel de Unión de Mutuas y conforme a los requisitos de certificación de Normas de Gestión.

DATOS DE CARÁCTER PERSONAL

Unión de Mutuas trata categorías especiales de datos personales conforme Art. 9 del RGPD, estando legitimada para el cumplimiento de una obligación legal asumida como responsable (Art. 6 1.c RGPD). La adecuación y cumplimiento conforme requisitos del RGPD queda recogida documentalmente en el procedimiento de Protección de datos de carácter personal que forma parte de la gestión documental de la entidad, y se encuentra disponible a través de la intranet corporativa para todo el personal.

Unión de Mutuas pone a disposición de usuarios e interesados toda la información relacionada con los tratamientos que realiza de datos de carácter personal, en la Política de privacidad y protección de datos, disponible también en esta web.

MARCO LEGAL Y REGULATORIO

Las funciones de las mutuas colaboradoras con la Seguridad Social quedan sujetas a la normativa actual que se encuentra establecida ampliamente en el Mapa Normativo de la entidad. Se incluyen como principales:

Real Decreto Legislativo 8/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley General de la Seguridad Social.
Reglamento general de colaboración en la gestión de las Mutuas de Accidentes de Trabajo y Enfermedades Profesionales de la Seguridad Social.
Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales.
Resolución de 4 de mayo de 2015, de la Secretaría de Estado de la Seguridad Social, por la que se establece el Plan general de actividades preventivas de la Seguridad Social, a aplicar por las mutuas colaboradoras con la Seguridad Social en la planificación de sus actividades para el año 2015.
Real Decreto 625/2014, de 18 de julio, por el que se regulan determinados aspectos de la gestión y control de los procesos por incapacidad temporal en los primeros trescientos sesenta y cinco días de su duración.
Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
Reglamento General de Protección de Datos, (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).
Real Decreto 1541/2011, de 31 de octubre, por el que se desarrolla la Ley 32/2010, de 5 de agosto, por la que se establece un sistema específico de protección por cese de actividad de los trabajadores autónomos.
Ley 32/2010, de 5 de agosto, por la que se establece un sistema específico de protección por cese de actividad de los trabajadores autónomos (BOE 06/08/2010).
Real Decreto 1299/2006, de 10 de noviembre por el que se aprueba el cuadro de enfermedades profesionales en el Sistema de Seguridad Social y se establecen criterios para su notificación y registro.
Resolución de 26 de noviembre de 2002, que regula la utilización del Sistema de Declaración Electrónica de Accidentes de Trabajo (Delta) que posibilita la transmisión por procedimiento electrónico de los nuevos modelos para la notificación de accidentes de trabajo.
Orden ESS/1187/2015, de 15 de junio, por la que se desarrolla el Real Decreto 625/2014, de 18 de julio, por el que se regulan determinados aspectos de la gestión y control de los procesos por incapacidad temporal en los primeros trescientos sesenta y cinco días de su duración.
Orden TAS/1/2007, de 2 de enero, por la que se establece el modelo de parte de enfermedad profesional, dicta normas para su elaboración y crea el correspondiente fichero de datos personales.

ORGANIZACIÓN DE LA SEGURIDAD: FUNCIONES Y RESPONSABILIDADES

En los sistemas de información se diferenciará la persona responsable de la información, del servicio y de la seguridad. Siguiendo uno de los principios básicos del ENS sobre la seguridad como función diferenciada se han establecido en la organización, roles y responsabilidades diferenciadas que se describen a continuación:

Responsable de la información y del servicio

El órgano responsable de la seguridad de la información y del servicio será el Comité de Seguridad de la Información que determinará los requisitos de la información tratada en materia de seguridad y en base al establecimiento previo de los niveles de seguridad en cada dimensión de los sistemas. Además, como Responsable del Servicio determinará los requisitos de los servicios prestados y sus niveles de seguridad.

Responsable de seguridad

La persona líder del Proceso de Gestión de Sistemas de Información de Unión de Mutuas es la Responsable de Seguridad conforme a los requisitos del Esquema Nacional de Seguridad y determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios. Entre las tareas principales del Responsable de Seguridad se encuentran:

- 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 al menos una vez al mes la información de control registrada y elaborar un informe de las revisiones realizadas y los problemas detectados.
- Adoptar decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.
- Decidir sobre la adquisición de productos y contratación de servicios relacionados con la seguridad.
- Dar cumplimiento de 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 Reglamento General de Protección de Datos de carácter personal.
- Formalizar, aprobar formalmente y firmar el cumplimiento de las medidas de seguridad del Anexo II del ENS, incluidas las compensatorias y su justificación, en un documento que se denominará Declaración de Aplicabilidad.
- 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 a 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.

Comité de Seguridad de la Información

El Comité de Seguridad de la Información tiene como objetivo realizar una evaluación continua del 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 éste del cumplimiento del Esquema Nacional de Seguridad, la Norma de Gestión ISO27001 y de la protección de datos de carácter personal según normativa vigente.

De acuerdo con ello, las responsabilidades del Comité de Seguridad de la Información serán, entre otras que se definirán ampliamente en el documento de seguridad, coordinar la seguridad de la información a nivel de organización para, entre otros aspectos,

- racionalizar implantación de las diferentes medidas de seguridad requeridas por el sistema.
- evitar disfunciones que permitan fallas de seguridad al dejar al sistema con puntos débiles donde pudieran ocurrir accidentes o se pudieran perpetrar ataques.

El Comité de Seguridad de la Información está formado por representantes de:

- Estrategia y Gestión Directiva.
- Gestión de Contingencia Profesional.
- Gestión de Prestación Económica.
- Gestión de Afiliación-Cotización.
- Responsable del Sistema (SGSI).
- Gestión de Recursos Humanos.

- Gestión Jurídica.
- Gestión de la Innovación y Mejora.
- Gestión de Edificios e Instalaciones.
- Responsable de Seguridad.
- Responsable de Contratación.
- Responsable de Cumplimiento Normativo.
- Delegado de Protección de Datos.

Responsable del Sistema

La persona líder del Subproceso de Control y Seguridad del Proceso Gestión de Sistemas de Información de Unión de Mutuas es la Responsable del sistema conforme a los requisitos del Esquema Nacional de Seguridad y la Norma de Gestión ISO27001 (Responsable del Sistema de Gestión de los Sistemas de Información) y determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

Entre las tareas principales del Responsable del Sistema se encuentran:

- Recibir los informes de auditoría y adoptar las medidas correctoras adecuadas con las conclusiones aportadas por el Responsable de Seguridad.
- En el caso de los sistemas de categoría ALTA, visto el dictamen de auditoría, el responsable del sistema podrá acordar la retirada de operación de alguna información, de algún servicio o del sistema en su totalidad, durante el tiempo que estime prudente y hasta la satisfacción de las modificaciones prescritas. (Esta decisión debe ser acordada con los responsables de la información afectada, del servicio afectado y el Responsable de la Seguridad, antes de ser ejecutada).
- Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.

Delegado de Protección de Datos

Unión de Mutuas ha designado a su delegado de protección de datos para que participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales.

Los interesados, por lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos al amparo del Reglamento General de Protección de Datos, podrán ponerse en contacto con el delegado de protección de datos de Unión de Mutuas a través de: delegadoprotecciondatos@uniondemutuas.es

El delegado de protección de datos estará obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones, de conformidad con el Derecho de la Unión o de los Estados miembros. El delegado de protección de datos de Unión de Mutuas actuará como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento de los datos de carácter personal de los interesados entre otras funciones establecidas en la actual normativa.

Obligaciones del personal

Todo el Personal de Unión de Mutuas debe conocer y cumplir esta Política de Seguridad de la Información, su Normativa de desarrollo y procedimientos de Seguridad.

Las funciones y obligaciones de todas las figuras vistas en esta Política se encuentran definidas al detalle en la documentación del Proceso de Gestión de los sistemas de información.

Sobre la resolución de conflictos entre los diferentes responsables prevalecerá la decisión del Responsable de Seguridad que deberá estar justificada ante el Comité de Seguridad de la Información.

La Dirección Gerencia de Unión de Mutuas es la encargada de nombrar y aprobar al Responsable de la Información y del Servicio, y al Responsable de la Seguridad mediante la aprobación del Documento de Seguridad, donde se encuentran bien definidos sus responsabilidades y cargos, y mediante la firma de la presente Política.

TERCERAS PARTES

Cuando Unión de Mutuas preste servicios a otros organismos o maneje información de otros organismos, les hará partícipes de esta Política de Seguridad de la Información.

Cuando Unión de Mutuas utilice servicios de terceros o ceda información a terceros, les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte deberá aceptar el quedar sujeta a las obligaciones establecidas en dicha normativa, 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.

Aprobación y entrada en vigor del presente texto el 13 de julio de2017.

Fecha de última actualización: abril 2018.

Juan Enrique Blasco Sánchiz
Director gerente