Ibermutua
Mutua Colaboradora con la Seguridad Social nº 274

Extracto de la Política de Seguridad de la Información de Ibermutua.

La Política de Seguridad de la Información de Ibermutua, MCSS nº 274, ha sido aprobada el día 26 de junio de 2024, en el transcurso de la sesión del Comité de Seguridad de la Información de Ibermutua, por su Director General, que ha sido ratificada por la Junta General de Ibermutua en fecha 11 de julio de 2024.

Entra en vigor el mismo día de su publicación, siendo revisada periódicamente por el Comité de Seguridad, así como por la Dirección de Ibermutua.

Objeto y contenido.

Plasma el compromiso de la Dirección con el cumplimiento normativo en materia de seguridad de la información, estableciendo las directrices para garantizar la confidencialidad, integridad, disponibilidad y autenticidad de la información, a través de medidas que eviten los riesgos de su alteración, pérdida, indisponibilidad y tratamiento o acceso no autorizado.

Se manifiesta la decidida voluntad de facilitar los recursos necesarios para implantar los controles que se precisen para establecer una estructura de seguridad y, a través de la constitución de un Comité de Seguridad, velar por el cumplimiento de la presente Política y garantizar, con el resto de instrumentos de apoyo y a través de la prevención, reacción y recuperación, la misión y objetivos de la Entidad y el cumplimiento de la legalidad, a través de mecanismos de prevención, reacción y recuperación con objeto de minimizar el impacto de los incidentes de seguridad.

Ámbito de aplicación y alcance.

Es de aplicación a todos los activos de **'Ibermutua Digital'** y obliga a toda la plantilla, a los proveedores o a cualquier persona que acceda a la información o a los sistemas e instalaciones de la Entidad.

Todas las personas son, individual y colectivamente, responsables de entender los riesgos asociados a la información que manejan y de proteger la confidencialidad, integridad y disponibilidad de dicha información en función de su valor, sensibilidad y criticidad

Misión.

Ibermutua es una asociación de empresarios que forma parte del Sector Público estatal, cuya misión es la colaboración con la Seguridad Social en la gestión de determinadas prestaciones públicas para sus empresas y personas trabajadoras protegidas, ejerciendo y desarrollando las competencias legalmente encomendadas, aplicando criterios de eficiencia, innovación, calidad y mejora continua.

Principios básicos.

Para conseguir los logros propuestos con la Política de seguridad de la información, Ibermutua reconoce y adopta los siguientes principios:

a) **Seguridad como proceso integral,** que abarca todos los aspectos humanos, materiales, técnicos, jurídicos y organizativos relacionados con los sistemas de información.

b) **Gestión de la seguridad basada en los riesgos** a través de identificación, análisis y gestión continua de los riesgos.

c) **Prevención, detección, respuesta y conservación.** Con el fin de minimizar las vulnerabilidades y garantizar la conservación de la información y los servicios afectados.

d) **Existencia de líneas de defensa** o capas de seguridad que permitan reaccionar adecuadamente frente a incidentes y minimizar su impacto.

e) **Vigilancia continua.** Se mantiene una vigilancia constante sobre la infraestructuras y sistemas de información, identificando y respondiendo proactivamente a posibles vulnerabilidades y amenazas.

f) **Reevaluación periódica:** Regularmente se revisa la eficacia de las medidas de seguridad.

g) **Diferenciación de responsabilidades:** entre los responsables de la información, el servicio, la seguridad y el sistema.

Marco normativo.

La entidad cuenta con un Procedimiento para la identificación de la legislación aplicable y el registro actualizado de la normativa de seguridad de la información.

Responsabilidades del personal.

Tienen obligación de conocer esta Política y cumplirla:

- Toda la plantilla de Ibermutua.
- Los terceros y personal externo que tengan alguna relación con la información y servicios apoyados en las TIC.

El incumplimiento de la Política de Seguridad podrá ser considerado como una infracción del deber de buena fe, sancionable con las medidas disciplinarias previstas en la legislación y normativa aboral

vigente en cada momento, y sin perjuicio del resarcimiento por daños y perjuicios que les pueda reclamar Ibermutua.

El Comité de Seguridad dispondrá los medios para que esta Política llegue a las personas afectadas.

Desarrollo de la Política y Estructuración de la Documentación de Seguridad.

La Política se desarrollará mediante la elaboración de otras políticas, procedimientos o normativas de seguridad que aborden aspectos específicos e instrucciones técnicas de desarrollo de éstos, que serán elaboradas por el Responsable de Seguridad y aprobadas por el Director General en el seno del CSI, estando disponibles para todo el personal que deba aplicarlas.

Formación y concienciación.

Toda persona con responsabilidad en el uso, la gestión, mantenimiento o explotación de los servicios soportados en las TIC se mantendrá correctamente formado en las tecnologías y procesos propios de su actividad y con relación con la seguridad de la información.

Las acciones formativas deberán ser programadas o a demanda, registradas y medidas, sin perjuicio de las campañas de sensibilización que deban llevarse a cabo.

Gestión de riesgos.

Se hará una determinación del riesgo aceptable por activo. Se analizarán los riesgos de los servicios una vez al año o cuando se produzcan cambios o incidentes graves y se harán Planes de tratamiento para aquellos riesgos que superen el riesgo aceptable.

Clasificación y gestión de activos.

Ibermutua mantendrá un inventario de los activos de información como parte importante de la administración de riesgos. Este inventario estará clasificado de acuerdo con la sensibilidad y criticidad de la información.

Seguridad física y del entorno.

Se mantendrá un inventario de activos de información clasificado, de acuerdo con la sensibilidad y criticidad de la información.

Control de accesos.

Se adoptarán medidas de seguridad para evitar pérdidas, daños, robos o daños que puedan producir la interrupción de la actividad, controlando la identificación de quien haga uso de ellos y la asignación de derechos de acceso.

Se impedirá el acceso no autorizado a través del control de acceso basado en la identificación y los derechos de acceso, en función de la "necesidad de conocer" y "mínimo privilegio".

Comunicación y respuesta a incidentes de seguridad.

Se establecerá un sistema de comunicación, respuesta y registro de incidentes y brechas de seguridad que incluya la comunicación por parte de terceros afectados.

Manejo de datos personales.

Para el manejo de información que incluya datos personales se observarán medidas de seguridad, técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo aceptado, tal y como exige el RGPD y la normativa española vigente asociada a la protección de datos personales.

Terceras partes.

Los terceros relacionados con la gestión, mantenimiento o explotación de los servicios serán partícipes y quedarán obligados por la Política de Seguridad.

Cuando un tercero no pueda cumplir con la Política, el Responsable de Seguridad deberá emitir informe del riesgo que supone, y presentarlo ante el CSI para valorar su aceptación.

Gestión del Personal.

Ibermutua establecerá los recursos necesarios para verificar que todo el personal aplica las normas y procedimientos operativos de seguridad, y evaluará su desempeño y seguimiento.

Adquisición de productos de seguridad y contratación de servicios de seguridad.

La adquisición de nuevos productos, sistemas o servicios de seguridad requerirá analizar los riesgos con proveedores, y obtener las autorizaciones de los responsables del Área funcional implicada y del Área de Contratación de la Mutua.

Mínimo privilegio.

Se aplicará el principio de seguridad por defecto a los sistemas y aplicaciones, que implica: funcionalidad mínima; limitación a la autorización y uso seguro.

Integridad y actualización del sistema.

Se tendrán en cuenta las informaciones sobre vulnerabilidades de los sistemas y productos, y se seguirán las recomendaciones de los fabricantes en cuanto a actualizaciones de seguridad.

Protección de la información almacenada y en tránsito.

Se deberán proteger convenientemente los equipos portátiles que puedan contener información, así como los soportes extraíbles.

Prevención ante otros sistemas de información interconectados.

Se desplegarán las protecciones necesarias para proteger el perímetro de la red corporativa de la Mutua, de forma que se neutralicen las posibles intrusiones.

Registro de actividad y detección de código dañino.

Se generarán registros de actividad para conocer en todo momento qué persona, y sobre qué datos, actúa, y se implementarán medidas de seguridad para detección y radicación de código dañino.

Continuidad de la actividad.

Se diseñará e implantará un plan de Continuidad que evite las interrupciones del servicio y , en su caso, aseguren su inmediata reanudación.

Mejora continua del proceso de seguridad.

Se ha establecido un Sistema de Gestión de la Seguridad que permite conocer en cada momento el estado de la seguridad, si bien se establecerá un proceso de mejora continua que permita nuevas medidas de seguridad, la mejora de las existentes y la incorporación de aquellas que plantee el CSI o el resto de personas de la Mutua.

Organización y seguridad de la información.

Se establece una clasificación por niveles:

- La responsabilidad legal y la especificación de las necesidades o requisitos, que corresponde a la Dirección.
- El gobierno del sistema, que corresponde al Responsable de la Información, al Responsable del Tratamiento y al Responsable del Servicio.
- La supervisión, que corresponde al Responsable de la Seguridad, al Delegado de Protección de Datos y al CSI.
- La operativa del sistema de información, que corresponde al Responsable del Sistema, al Responsable de Seguridad Física y a las demás figuras que gestionan los sistemas (Directores ejecutivos, funcionales y territoriales, etc.).

El detalle y funciones concretas de los diferentes roles y sus responsabilidades, se describe en el procedimiento "*PR Procedimiento general de la gestión de seguridad de la información y modelo organizativo*", al cual se remite esta política, sin perjuicio de lo que disponga la norma en ese punto.