Política de Seguridad de la Información

Grupo Mutua Madrileña

19 de diciembre de 2024

Clasificación: Pública

Índice del contenido

Este documento ha sido elaborado para el uso exclusivo del grupo mercantil encabezado por Mutua Madrileña (en adelante, Grupo societario Mutua Madrileña o el Grupo) y para sus filiales.

Fecha de primera aprobación:	17 de diciembre de 2015
Responsable de edición y revisión	Subdirección General Adjunta de Control de Riesgos
Idiomas disponibles:	Español

Registro de revisiones

Las diferentes revisiones del presente documento serán anotadas en este registro, incluyendo el número de versión, revisión, fecha de publicación, principal causa de la revisión, y los responsables de su aprobación y revisión:

Versión	Fecha	Modificaciones	Revisado Por	Aprobado Por
1.0	27/07/2023	Edición Inicial	Comisión de Auditoría	Órgano de Administración
2.0	24/07/2024	Revisión	Comisión de Auditoría	Órgano de Administración
3.0	19/12/2024	Inclusión de la nueva normativa DORA	Comisión de Auditoría	Órgano de Administración

La revisión de esta política ha sido realizada por:

- Los miembros del Comité de Dirección han revisado y analizado el contenido de esta política.
- Dirección de Control de Riesgos: ha supervisado la coherencia de la política con la estructura del grupo, la dimensión y las particularidades de las entidades que son parte de este.
- Dirección General Adjunta de Tecnología: han revisado la coherencia de la presente política con las políticas de seguridad de la información existentes en el marco de la norma ISO 27001.
- El grupo establecido para la revisión de las políticas ha supervisado que esta política contiene todos los elementos fundamentales que son requeridos por la normativa vigente que le aplica.
- Comité de Riesgos: ha revisado, analizado y dado opinión favorable con carácter previo a su elevación a los Órganos de Administración.

POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN DE MUTUA MADRILEÑA Y SOCIEDADES DE SU GRUPO

I. INTRODUCCIÓN

La presente política se enmarca en el Sistema de Gobierno establecido para Mutua Madrileña y el conjunto de sociedades de su Grupo que se adhieran a la política.

Este documento representa las directrices a más alto nivel relacionadas con la securización de la información de la organización que, posteriormente, serán desarrolladas a través de normativa interna específica del Sistema de Gestión de Seguridad de la Información (SGSI), en la que se detallan, entre otros, aspectos relacionados con la gestión los activos, los roles, la planificación, los recursos y la evaluación de los riesgos y el desempeño del gobierno de la seguridad.

1. Antecedentes

El marco normativo emanado de las Directrices sobre Gobernanza y Seguridad de las Tecnologías de la Información y de las Comunicaciones emitidas por la EIOPA, ESMA o resto supervisores, así como el Reglamento Europeo de Resiliencia Operativa Digital (DORA) han puesto de manifiesto la necesidad de contar con una política de Seguridad que establezca las bases para la gestión de sus medidas de seguridad.

Adicionalmente, cada vez más, los procesos de las entidades financieras se apalancan en la digitalización, el empleo de nuevas tecnologías y en la contratación de proveedores. La tendencia al alza de dicha digitalización deriva en un aumento en los riesgos de seguridad de sus activos de información que obliga a que su dirección, a través del órgano competente, defina los principios a alto nivel y las normas destinadas a proteger la confidencialidad, la integridad y la disponibilidad de la información a fin de respaldar la aplicación de la estrategia de sus tecnologías de información.

En este sentido, el grupo mercantil encabezado por Mutua Madrileña (en adelante, Grupo societario Mutua Madrileña o el Grupo) ha procedido a la redacción de una política de protección de la seguridad de la información.

De forma adicional, existen otras normativas externas, directrices y prácticas de mercado que establecen requerimientos y recomendaciones para la gestión de la seguridad de las tecnologías de la información:

- Normativa estándar UNE ISO/IEC 27001:2023 (en adelante ISO 27001) – Sistemas de Gestión de la Seguridad de la Información.
- Normativa estándar UNE ISO/IEC 27002:2023 (en adelante ISO 27002) – Código de Buenas Prácticas para la Gestión de la Seguridad de la Información.
- Normativa estándar UNE ISO/IEC 27017:2021 (en adelante ISO 27017) – Código de práctica para la seguridad de la información en la nube
- 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 (LOPDGDD)
- Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico (LSSICE).
- Normativa estándar UNE ISO/IEC 27005: 2022 (en adelante ISO 27005) – Gestión del Riesgo de Seguridad de la Información.
- Directrices (BoS-20/002) de EIOPA sobre externalización a proveedores de servicios en la nube
- Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero.

2. Objetivo de la política

El objetivo de la presente política es establecer el marco general necesario, con sus principios y características generales, para garantizar la confidencialidad, integridad y disponibilidad de la información contenida en los activos de la organización.

Todo ello da respuesta, como se ha comentado anteriormente, a la normativa BoS-20/600 de EIOPA sobre Gobernanza y Seguridad de las Tecnologías de la Información y de las Comunicaciones, en su directriz 6 (Política y medidas de seguridad de la información), donde se establece la necesidad de instaurar una política de seguridad de la información que deberá ser aprobada por el órgano de administración de la empresa, que incluya *"una descripción de las principales funciones y responsabilidades para la gestión de la seguridad de la información y en la que se establezcan los requisitos del personal, los procesos y la tecnología en relación con la seguridad de la información, poniendo de manifiesto que el personal de todos niveles tiene responsabilidades a la hora de garantizar dicha seguridad en las empresas*".

De la misma forma, la presente política se alinea con el artículo 5 del Reglamento de Resiliencia Digital (DORA) en cumplimiento de su artículo 5.b: "*adoptará políticas encaminadas a garantizar el mantenimiento de unos niveles elevados de disponibilidad, autenticidad, integridad y confidencialidad de los datos;"*

Así, en la presente política, se establecen como objetivos principales de la organización:

- **Garantizar la confidencialidad, integridad y disponibilidad de toda la información** procesada o albergada en el ámbito de la compañía.
- Establecer las medidas necesarias para **garantizar la continuidad de los servicios TI y minimizar el impacto** que cualquier tipo de incidente de seguridad pueda producir, independientemente de su origen y características
- **Asegurar que el apetito por el riesgo** de la entidad en el marco de los riesgos de seguridad está establecido y **se mantiene dentro los niveles aprobados en el Grupo**, con un seguimiento del riesgo residual, de forma que se vaya acercando a la preferencia de riesgo (riesgo objetivo).

- **Satisfacer y cumplir los aspectos relativos a lo dispuesto en leyes y regulaciones**, así como en los estándares voluntariamente asumidos.

- Llevar a cabo las **sesiones de concienciación y formación específicas** que permitan a cada uno de los diferentes perfiles conocer sus funciones y publicaciones en el ámbito de la Seguridad IT.

- Establecer los **mecanismos oportunos que permitan la mejora continua**.

- **Establecer canales de comunicación e información adecuados entre las filiales y matriz**, para permitir el cumplimiento de sus obligaciones a nivel de Grupo, de forma que, entre otras cosas, las filiales informen a la matriz de cualquier hecho relevante que pudiera afectar a la seguridad de la información del Grupo.

3. Alcance

Respecto al alcance de la presente política dentro del Grupo Mutua, debemos distinguir entre:

- **Mutua Madrileña y filiales y asociadas cuyos activos tecnológicos (sistemas de información) estén integrados con ésta** y estén gestionados desde las áreas de Tecnología de Mutua, en virtud de contratos de apoyo a la gestión.

  Les será de aplicación toda la política, en tanto en cuanto nos refiramos a los activos gestionados desde las áreas de Tecnología de Mutua, ya que en la gestión de estas sociedades participan directamente los departamentos de Mutua Madrileña aprovechando con ello la mayor especialización y economías de escala. La dedicación a estas sociedades se articula a través de contratos de apoyo a la gestión firmados entre la matriz y filiales.

- **Filiales aseguradoras de España y cualquier país europeo:** se unirán a lo desarrollado en la presente política, con las necesarias adaptaciones a las especificidades de cada empresa, en la medida en que se desarrollen sus propias políticas, respetando tanto los principios como las directrices que contienen, basadas en las directrices sobre gobernanza y seguridad de las tecnologías de la información y de las comunicaciones de EIOPA y DORA.

  En este sentido, además de guiarse por los mismos principios, entre otras cosas, deberán seguir una estrategia, procesos y procedimientos similares, que redunde además en un adecuado reporting de grupo, una estructura similar de funciones, asegurándose que se produzca un adecuado sistema de supervisión de los riesgos, con la necesaria separación de funciones entre las diferentes líneas de defensa y que los órganos de administración y control tengan las funciones que se les supone.

- **Las empresas filiales aseguradoras de un país no europeo, así como las empresas filiales reguladas y pertenecientes a otros sectores,** seguirán los principios de esta política, intentando además asimilar sus sistemas al máximo, de forma que permita un reporting de grupo lo más homogéneo posible, si bien contemplando las especificidades que contemple la normativa local o sectorial, respectivamente.

- Respecto **al resto de empresas**, deberán seguir los principios de esta política en la gestión de la seguridad de la información, buscando una adecuada gestión y control de estos.

- El Consejo de Administración de cada una de las entidades deberá aprobar la adhesión, en todo o en parte, a esta política y establecer los canales de comunicación y los órganos y comités encargados de su aprobación en su entidad.

- De igual forma, Mutua Madrileña se obliga a reportar periódicamente al Consejo o Comités específicos de las sociedades que se adhieran a la presente política toda la información que según la normativa deba conocer y en su caso aprobar.

4. Entrada en vigor

Esta política entró en vigor el 27 de julio de 2023. Las actualizaciones de las políticas son de aplicación una vez aprobadas por el Consejo de Administración. La fecha de la entrada en vigor de cada una de las versiones de la política se encuentra recogidas al inicio de la política en el apartado Registro de revisiones, estando la última en vigor también al inicio del documento. Cláusula de Actualización

La política debe ser revisada con una periodicidad mínima anual y, en cualquier caso, siempre que concurran situaciones que modifiquen sustancialmente la naturaleza, estructura o el perfil de riesgos de la entidad.

La coordinación y dirección relativa a la actualización de las políticas es responsabilidad de la Subdirección General Adjunta de Control de Riesgos, perteneciente a la Dirección General Adjunta de Finanzas y Riesgos, quien requerirá a las unidades implicadas en la mismas y elevará al Comité de Riesgos la propuesta de actualización para su revisión previa a la aprobación por el Consejo de Administración.

5. Directrices y principios de la Seguridad de la Información

1. Los procesos de gestión de seguridad de la información se conforman para proporcionar a la organización confianza razonable sobre la idoneidad, eficacia y eficiencia de su estrategia de seguridad, que en cada momento deben adecuarse a las necesidades, riesgos y objetivos de la organización.

2. Para afianzar la gestión de la seguridad de la información, el Grupo cuenta con un Sistema de Gestión de Seguridad de la Información (SGSI) cuyo alcance es el determinado por éste y se adapta a las necesidades de las partes interesadas. Con respecto a este sistema, la presente política supone el compromiso por parte de la dirección de:

a. Establecer, implementar, operar, monitorizar, revisar y mejorar un sistema documentado de gestión de la seguridad de la información basado en la normativa estándar UNE-ISO/IEC 27001 (en adelante ISO 27001).

b. Asignar los recursos adecuados para gestionar el SGSI.

c. Delegar funciones (salvo las aprobaciones) en los integrantes del Comité de Seguridad de la Información y Riesgos Tecnológicos, entre ellos, el Responsable de Gestión de la Seguridad de la Información.

d. Contribuir a la eficacia del sistema de gestión de seguridad.

3. La dirección del Grupo Mutua Madrileña establecerá los siguientes mecanismos para el afianzamiento de la seguridad en la entidad:

a. El establecimiento como encargado de gobernar la Seguridad IT del Grupo Mutua a la figura del CISO (Chief Information Security Officer).

b. El establecimiento de la figura del Responsable de Gestión de Seguridad de la Información, como el encargado del seguimiento y gestión de la Seguridad IT.

c. El desarrollo de un plan de formación y concienciación que garantice la implicación del personal y el cumplimiento de las medidas de seguridad de la información establecidas.

d. La aplicación de los controles necesarios para asegurar un nivel de seguridad adecuado, y mantener el riesgo por debajo de los niveles aceptados.

e. La elaboración e implantación de un conjunto documental que complete, regule y defina las medidas exigidas de seguridad lógica.

f. Facilitar información de manera regular sobre el estado de la seguridad.

g. El tratamiento de los incidentes de seguridad de la información dentro de la metodología de gestión, que asegure tanto su resolución como la vuelta a la normalidad.

h. La definición de los roles y responsabilidades de todo el personal que, de una u otra manera participa en la seguridad del Grupo.

i. La creación de una guía de requisitos y obligaciones respecto a la seguridad de la información, la Normativa de Seguridad, que debe ser leída y aceptada por el personal interno. Esta normativa será recordada a intervalos regulares y planificados.

j. Con el fin de asegurar que la gestión de la Seguridad IT se alinea en todo momento con las necesidades de la organización, se establece una metodología de no conformidades, recomendaciones y mejora continua de todo el sistema de gobierno, siguiendo un ciclo “Plan-Do-Check-Act” (PDCA), que garantiza el mantenimiento continuo de los niveles de seguridad deseados.

4. La dirección de la entidad determina que, conjuntamente y como soporte a la presente política, se deben establecer y documentar un conjunto de reglas que contengan las siguientes directrices mínimas en lo que a seguridad de la información se refiere:

a. Directrices de seguridad en la gestión de accesos.

b. Directrices de copias de seguridad y recuperación de información.

c. Directrices para la gestión del riesgo de seguridad de la Información.

d. Directrices de uso aceptable de los activos de información.

e. Directrices para la gestión de incidentes de seguridad.

f. Directrices para la gestión de la seguridad en terceras partes.

g. Directrices para el aseguramiento de la seguridad en los procesos operativos de la organización.

5. Adicional a las directrices anteriores, la política de seguridad de la información se apoya en otras normas y procedimientos específicos que se encuentran citados más adelante.

6. Todo el personal externo y posibles visitas que accedan a las instalaciones sujetas a esta política, están obligadas a su cumplimiento y esto será supervisado por el personal interno.

II. GOBERNANZA, FUNCIONES Y RESPONSABILIDADES

A continuación, se describen las funciones y responsabilidades específicas de los diferentes órganos y unidades que intervienen de manera relevante en la gestión y control de la seguridad de la información. Estas responsabilidades están referidas, sin necesidad de diferenciarlas, salvo cuando expresamente así se indique, tanto a cada una de las entidades financieras individualmente consideradas, como al Grupo en su conjunto.

1. Consejo de Administración

Descripción – Unidad

El Consejo de Administración (Consejo de Administración en Mutua Madrileña), es el máximo y último responsable de los sistemas de gobernanza y de gestión de la seguridad de la información de la organización; sin perjuicio de poder encomendar algunas funciones a los órganos o comités internos que considere adecuados en función de sus responsabilidades.

A este fin, determina el alcance y la frecuencia de las revisiones internas del sistema de gobernanza, teniendo en cuenta la naturaleza, el volumen y la complejidad de la actividad tanto a nivel individual como a nivel de Grupo, así como la estructura del Grupo.

Responsabilidades

Debe asegurarse de la existencia de medios humanos y técnicos adecuados y suficientes para garantizar el correcto funcionamiento de los sistemas de gestión de la seguridad de la información y de una adecuada segregación de funciones.

De esta manera el Consejo de Administración es el garante de la seguridad de la información del Grupo, siendo:

- El Consejo de Administración como último responsable, define, aprueba y supervisa todas las disposiciones relacionadas con el marco de gestión del riesgo y su actualización relacionado con las TIC.

- Responsable de establecer y aprobar la estrategia de seguridad IT que incluirá las pruebas de resiliencia operativa digital, de las medidas a implantar por incidencias graves TIC y Seguridad de la Información, y recibir comunicaciones acerca del progreso y los riesgos asociados a las pruebas de penetración basadas en amenazas (TLPT). Esta responsabilidad abarca igualmente las disposiciones para el establecimiento del perfil de riesgo de seguridad de la organización y los apetitos de riesgo, aprobando las alertas de tolerancia y límites de exceso. El apetito de riesgo deberá ser comunicado a la Dirección de Seguridad IT/CISO. Responsable de la adopción y cumplimiento de las políticas encaminadas a garantizar el mantenimiento de unos niveles elevados de disponibilidad, autenticidad, integridad y confidencialidad de los datos.

- Responsable de la definición de los cometidos y responsabilidades en lo que respecta a todas las funciones relacionadas con la seguridad de la información. También deberá

establecer los mecanismos de gobernanza adecuados para garantizar una comunicación, cooperación y coordinación efectivas y oportunas entre dichas funciones.

- Responsable de la asignación y revisión periódica del presupuesto establecido para satisfacer las necesidades de la seguridad de la información de la entidad en lo que respecta a recursos, programas de sensibilización y actividades de formación y capacidades.

- La aprobación de los planes de auditoría TIC en aquellos casos en los que no sea responsabilidad de la Comisión de Auditoría y Cumplimiento.

- Atención a la obligación de formación sobre materia TIC.

- Aprobación de los informes de revisión periódicos y puntuales relativos a pruebas de resiliencia operativa digital e incidentes TIC.

Relación con otros órganos

El Consejo de Administración recibe un reporte directo de la Comisión de Auditoría y Cumplimiento (CAC) sobre resultados y propuestas/recomendaciones (revisión y actualización de políticas).

Adicionalmente, recibe de Seguridad IT la propuesta del apetito al riesgo, perfil y estrategia para su aprobación.

2. Comisión de Auditoría y Cumplimiento (CAC)

Descripción – Unidad

Corresponde a la CAC supervisar la eficacia del control interno, la auditoría interna y los sistemas de gestión de riesgos de la entidad, incluyendo los riesgos de seguridad lógica, así como discutir con el auditor de cuentas las debilidades significativas del sistema de control interno detectadas en el desarrollo de la auditoría, todo ello sin quebrantar su independencia. A tales efectos, y cuando lo considere necesario, podrá presentar recomendaciones o propuestas al Consejo de Administración.

La revisión y actualización de todas las políticas deben someterse previamente a la revisión y la opinión de la Comisión de Auditoría antes de su elevación al Consejode Administración.

Responsabilidades

Las responsabilidades principales de la CAC en materia de Seguridad IT son:

- Establecer el calendario de actividad de Auditoría Interna en relación con los riesgos de seguridad así como la aprobación de los planes de auditoría TIC en aquellos casos en los que no sea responsabilidad del Consejo de Administración.

- Reportar al Consejo de Administración de la actividad de auditoría desarrollada y los resultados obtenidos. Se tomarán en cuenta sus consideraciones y opinión sobre los distintos aspectos a reportar al Consejo de Administración desde el Comité de Riesgos, en particular en la propuesta de valoración del apetito de riesgo.

- Adicionalmente, la Comisión de Auditoría y Cumplimiento supervisará la eficacia de esta política

Relación con otros órganos

- La Comisión de Auditoría y Cumplimiento reporta al Consejo los resultados y propuestas/recomendaciones de la revisión y actualización de políticas y del apetito de riesgo, así como sobre la estrategia de seguridad en lo que respecta a su alineamiento con la estrategia de la compañía.

- Auditoría interna: coordinación y supervisión de la actividad del área.

3. Dirección General

Descripción – Unidad

La Dirección General apoya y garantiza el establecimiento y desarrollo del sistema de gestión de seguridad de la información. Para ello, impulsa la aplicación en la entidad de los sistemas de gobernanza de la seguridad eficaces, definiendo las estructuras, líneas y mecanismos de información y reporte y los niveles de autoridad y responsabilidad necesarios para la consecución de los objetivos de la entidad y del Grupo.

Participa en el proceso de elaboración, análisis y propuesta de decisiones a los órganos de dirección y gobierno en esta materia y vela por que exista un adecuado análisis de riesgos en los procesos de toma de decisiones relevantes de la entidad.

Está debidamente informada de la evolución del sistema de gobernanza de la seguridad de la información del Grupo y de las debilidades detectadas en dichos sistemas.

Responsabilidades

Las responsabilidades principales de la Dirección General en materia de Gestión y Control del Riesgo TI son:

- Asegurar el establecimiento del Sistema de Gestión de Seguridad de la Información.

- Asegurar la dotación de recursos requerida por la Organización para la ejecución de las funciones asignadas.

- Asegurar que se establecen estructuras departamentales con una correcta separación de funciones, segregación de tareas, atribución de competencias y delegación de facultades.

- Asegurar el alineamiento y la consistencia entre la estrategia de la organización y la estrategia de seguridad de la información.

Relación con otros órganos

La relación con otros órganos se establece a través de cada uno de los Comités de los que forma parte.

4. Comité de Dirección

Descripción – Unidad

El Comité de Dirección está informado sobre los aspectos esenciales de la evolución de la seguridad, así como de las actualizaciones de las políticas y las distintas responsabilidades recogidas en materia de seguridad si así lo requiere.

Responsabilidades

Es responsabilidad de la Alta Dirección la implementación de los procedimientos de gestión de riesgos en línea con las directrices establecidas por el Consejo de Administración y de una estructura organizativa que permita la adecuada aplicación y desarrollo del sistema de gestión del riesgo tecnológico y de la seguridad de la información. En este sentido:

- Es responsable de la implantación de un sistema de gestión de seguridad de la información, bajo los criterios y parámetros establecidos por el Consejo de Administración, sin perjuicio de la existencia de unidades específicas encargadas de la supervisión y el control de estos.

- Debe estar involucrado en la gestión de la seguridad de la información, garantizar que la estrategia de seguridad se aplica, adopta y comunica a todo el personal y los proveedores de servicios pertinentes, según sea aplicable y relevante, de manera oportuna.

- Garantiza que está establecido y actualizado periódicamente el mapa de procesos y actividades comerciales, así como de sus cargos, funciones y activos de negocio, entre ellos los activos de información y activos de TIC, a fin de identificar su importancia y sus interdependencias con los riesgos de seguridad.

- Aprobar el documento de especificación del alcance que realiza la entidad con la información requerida del TLPT.

- Revisión y visto bueno del Marco de Gestión del Riesgo TIC y sus actualizaciones periódicas, en lo referente a Seguridad de la Información.

- Dar el visto bueno a los informes periódicos de información relativos a pruebas de resiliencia operativa digital e incidentes TIC.

Relación con otros órganos

El Comité de Dirección recibe un reporte directo del Comité de Riesgos sobre resultados y propuestas/recomendaciones en relación con la gestión y control del riesgo de seguridad.

5. Comité de Riesgos

Descripción – Unidad

El Comité de Riesgos es un órgano encargado de facilitar la aplicación y realizar la supervisión de los sistemas de control interno y de gestión de riesgos a nivel del Grupo.

La composición, presidencia y funcionamiento general del Comité de Riesgos se define en el documento “Política de Gestión de Riesgos en el Marco del Sistema de Gobierno”.

Responsabilidades

Las responsabilidades principales del Comité de Riesgos en materia de Gestión de Riesgos de Seguridad de la Información son:

- Ser informado e involucrado en la gestión y control de los riesgos de seguridad de la información mediante la revisión del proceso y resultados de la gestión y control del riesgo.
- Ser informado de la estrategia de seguridad que se propondrá al Consejo de Administración, de forma que en el Comité se pueda realizar su análisis y emitir opinión respecto a su suficiencia desde el punto de vista de la gestión y control de los riesgos y se supervise el seguimiento de su ejecución siempre y cuando se detecten nuevos riesgos o de ejecución en dicha planificación.
- Ser informado de todos los aspectos relevantes relativos a los riesgos se seguridad de la información por las distintas áreas, funciones o comités.
- Proponer, previa opinión de la SDG Adjunta de Control de Riesgos, al Consejo de Administración, a través de la Comisión de Auditoría y Cumplimiento, el apetito por el riesgo de seguridad.
- Promover la adopción de las medidas oportunas para mantener los niveles de riesgo dentro de los límites establecidos por el Consejo de Administración.
- Supervisar periódicamente la gestión y control de los riesgos de seguridad.

Relación con otros órganos

El Comité de Riesgos recibe un reporte directo del Comité de Seguridad de la Información y Gestión de Riesgos Tecnológicos sobre resultados y propuestas/recomendaciones en relación con la gestión del riesgo de seguridad de la información. Adicionalmente la Subdirección General Adjunta de Control de Riesgos reporta las conclusiones de la actividad de control en relación con la gestión del riesgo de seguridad.

Por otro lado, el CISO y la Subdirección General de Tecnología, en caso necesario, puede reportar asuntos concretos relativos a la gestión del riesgo TI y de seguridad de la información según corresponda. Pueden asistir a las convocatorias del Comité de Riesgos como invitados, a solicitud del presidente.

Adicionalmente, el Comité de Riesgos es el responsable de reportar las conclusiones principales sobre el estado de la gobernanza y la gestión y control de Riesgos TI a la Comisión de Auditoría y Cumplimiento y a los Órganos de Administración.

6. Comité de Seguridad de la Información y Riesgos Tecnológicos

Descripción – Unidad

El Comité de Seguridad y Riesgos TIC ejerce las labores de revisión por la dirección obligatoria por la norma ISO 27001 de cara al aseguramiento de la conveniencia, adecuación y eficacia del Sistema de Gestión de Seguridad de la Información del Grupo MM a intervalos planificados.

Responsabilidades

Este comité es responsable, entre otras labores, de:

- Toma de decisiones de todos los aspectos relevantes que puedan afectar al Sistema de Gestión de Seguridad de la Información (SGSI).
- Determinación del alcance y exclusiones del SGSI.
- Proponer objetivos de seguridad y realizar el seguimiento de su cumplimiento.
- Aprobar la documentación de alto nivel del SGSI.
- Proponer al Comité de Riesgos el nivel de riesgo aceptado y su supervisión.
- Aprobar las medidas de seguridad para la reducción del nivel de riesgo.
- Revisar periódicamente:
    - La gestión de la seguridad de la información y el sistema.
    - Los riesgos de seguridad.
    - El plan de tratamiento de riesgo.
    - El estado de aplicabilidad.
    - Incidentes y nivel de incidencias.
    - Medidas de prevención, corrección y mejora.
    - La infraestructura que da soporte a la gestión de la seguridad de la información, tal como herramientas de seguimiento, recursos materiales, equipos de personas, infraestructuras de reporte entre otros.
    - El informe de auditoría sobre el SGSI.
- Velar por el cumplimiento normativo.
- Elevar al Comité de Riesgos las conclusiones del registro de incidentes si así se le requiere.
- Asegurar que se establecen procedimientos, se implantan y se mantienen.
- Promover el conocimiento de los requisitos de seguridad de los grupos de interés a todos los niveles de organización.
- Velar por el cumplimiento de la presente política, instando en su caso acciones correctoras y, si fuera necesario, iniciar acciones disciplinarias o legales.
- Exigir a los empleados, contratistas y terceros, que apliquen la seguridad de acuerdo con las políticas y procedimientos establecidos en Mutua Madrileña.
- Definir y crear la figura del Responsable de Gestión de Seguridad.

La composición y funcionamiento general del Comité de Seguridad de la Información y Riesgos Tecnológicos se definirá con detalle en los estatutos del mismo. En cuanto a la presidencia del Comité, este estará compuesto por:

- Director Gral. Adjunto de Tecnología (Presidencia)
- Subd. Gral. Adj. de Control de Riesgos (Secretaría)

Tanto el presidente como el secretario son los responsables de acordar los asistentes en función del orden del día, asegurando que se encuentran representadas en todo caso las direcciones de las áreas de negocio afectadas y responsables de la gestión de los diferentes ámbitos de riesgo tecnológico. En caso de las reuniones relacionadas con la gobernanza de la seguridad es obligatoria la presencia de:

- Dirección de Tecnología
- Gobierno y estrategia TI
- Seguridad de la información (CISO)
- Continuidad TI
- Responsable de Gestión de la Seguridad de la Información

Relación con otros órganos

- Comité de Riesgos: reporte al Comité de los aspectos relevantes relacionados con el sistema de gestión y control de riesgos TI.
- SDG Adjunta de Control de Riesgos: representada en este Comité, tiene la función de llevar a cabo el Control del Riesgo de Seguridad que se gestiona a través del mismo.
- Seguridad TI/CISO, Subdirección General de Tecnología de quien recibe toda la información relevante de gestión de riesgo TI.

7. Auditoría Interna

La gobernanza, los sistemas y los procesos de las empresas para sus riesgos de seguridad de la información deben ser auditados de manera periódica y en consonancia con su correspondiente plan de auditoría por unos auditores dotados de unos conocimientos, unas competencias y una experiencia suficiente en seguridad de la información, a fin de garantizar de manera independiente su eficacia al Consejo de Administración.

La frecuencia y el objeto de estas auditorías deben ser adecuados a los riesgos de seguridad pertinentes, tal y como se describe en la Política de Auditoría Interna del Grupo Mutua.

8. Dirección General Adjunta de Tecnología.

Descripción – Unidad

Este órgano representa a toda la dirección en lo relacionado con la gestión de la seguridad y de la información y por tanto, es su máximo responsable.

Responsabilidades

A través de la Dirección de Seguridad TI/CISO y de la S.D.G de Tecnología sus principales responsabilidades son:

- Proponer la estrategia TI y de seguridad de la información de la compañía e informar de su evolución al Comité de Riesgos y al Consejo de Administración.

- Asegurar el despliegue de estrategias, políticas, procedimientos, protocolos y herramientas de seguridad adecuadas, fiables y resilientes.

- Facilitar los medios para que, a través de la Dirección Seguridad TI / CISO se realice el diseño, implantación y control del sistema de gestión de la seguridad de la información, bajo los criterios y parámetros establecidos por el Consejo de Administración, sin perjuicio de que requieran la colaboración de otras unidades organizativas del Grupo.

- Garantizar y dotar de recursos a las funciones asignadas a la Dirección de Seguridad TI / CISO.

Relación con otros órganos

La relación con otros órganos se establece a través de cada uno de los Comités de los que este órgano forma parte.

9. Subdirección General de Tecnología

Descripción – Unidad

La Subdirección General de Tecnología es la responsable de la implantación de ciertos ámbitos del marco de gestión y control de la seguridad de la información bajo los criterios y parámetros establecidos en esta política y así como en resto de normativa asociada.

Para ello deberán implantar las medidas de seguridad indicadas por el área de Seguridad IT de acuerdo a los estándares, buenas prácticas y control de los riesgos implantados por ésta.

Responsabilidades

La Subdirección General de Tecnología tiene como principales responsabilidades:

- Contribuir al mantenimiento de las políticas de seguridad de la información.

- Garantizar la puesta en práctica de las políticas, directrices y metodologías relativas a seguridad de la información.

- Identificar los activos de información y los activos TI asociados a los servicios TI y a los procesos de negocio e identificar a los propietarios que deberán ser los responsables de su clasificación.

- Someter a pruebas periódicas los planes y medidas que permitan garantizar la continuidad de las funciones esenciales.

- Custodiar las evidencias que garanticen la ejecución de los controles y los resultados de éstos y ponerlas a disposición de los revisores que las soliciten: Dirección de Seguridad de la Información TI/CISO, SDG Adjunta de Control de Riesgos, áreas de control, auditores internos o externos, supervisores, etc.

- Revisar y ejecutar el marco de gestión del riesgo.

- Ejecutar el análisis de riesgos de TI asociados a los servicios TI y a los procesos de negocio de los que es responsable, y presentar los resultados obtenidos para determinar el tratamiento del riesgo. Para ello se realizará un informe anual de revisión (que incluirá las pruebas de la resiliencia operativa digital, de las medidas a implantar por incidencias graves TIC y de la gestión de proyectos TIC que afecten a las funciones esenciales) además de informes de riesgos cuando se supere el nivel de apetito por el riesgo.

Relación con otros órganos

Comité de Seguridad de la Información y Riesgos Tecnológicos: al que reporta toda la información relevante relacionada con las funciones descritas anteriormente.

Auditoría Interna: recepción de informes de resultados en la ejecución de auditorías. Sobre esto deberá reportar los planes de corrección y mejora que pudiesen resultar.

10. Dirección de Seguridad TI/CISO

Descripción – Unidad

Las principales funciones de la dirección de seguridad TI/CISO (Chief Information Security Officer), en lo relativo a la gestión de riesgos de TI, tal como se describe esta figura en el SGSI del Grupo Mutua, son:

- Garantizar la confidencialidad, integridad y disponibilidad de la información de la Compañía y la seguridad en cualquier ámbito, así como del cumplimiento de las normativas, organismos oficiales y legales en materia de seguridad, minimizando el impacto en los servicios y de acuerdo con las directrices estratégicas.

- Definir y ejecutar todos los procedimientos y políticas técnicos relacionados con la seguridad de la información incluída la política de Seguridad y Procedimientos.

- Definir estrategias de seguridad y controlar su implantación.

- Proteger los activos y evitar daños a la Compañía, minimizando la probabilidad de ocurrencia de los riesgos, mitigando al máximo los impactos en caso de que se materialicen.

- Actuar como interlocutor con la alta dirección a través del Comité de Seguridad donde se comparte información de proyectos e iniciativas, riesgos, amenazas e incidencias, en materia de seguridad de la información.

- Identificar y definir la parte de Seguridad TI del Marco de Gestión del riesgo TI.

- Realizar el análisis de riesgos de Seguridad de la Información asociados a los procesos de negocio de los que es responsable, y presentar los resultados obtenidos para determinar el tratamiento del riesgo. Para ello se realizará un informe anual de revisión (que incluirá las pruebas de la resiliencia operativa digital, de las medidas a implantar por incidencias graves TIC y Seguridad de la Información y generar comunicaciones acerca del progreso y los riesgos asociados a las pruebas de penetración basadas en amenazas (TLPT) además de informes de riesgos cuando se supere el nivel de apetito por el riesgo.

- Elaborar el procedimiento de TLPT que se incluye dentro de la política de Seguridad de la Información.

Responsabilidades

Las responsabilidades del CISO, en lo referente a la Gestión del Riesgo de Seguridad de la Información, son las siguientes:

- Definir la estrategia de Seguridad de la Información, que será aprobada por el Consejo de Administración.

- Contribuir en la definición y mantenimiento de la política de seguridad de la información, así como de controlar su implantación.

- Asegurar que todos los empleados y proveedores de servicios que acceden a la información y los sistemas son adecuadamente informados de la política de seguridad de la información.

- Controlar la implantación de la estrategia de Seguridad de la Información, que actualizará y reportará a los órganos de control y de administración si así se requiere. Dicha estrategia de seguridad se actualizará y concretará periódicamente en un plan anual con los principales proyectos e iniciativas en relación con la seguridad de la información.

- Coordinar el análisis y resolución de los incidentes de seguridad de la información y comunicar los más relevantes de acuerdo al plan de comunicación establecido para los mismos.

- Definir planes de seguridad dirigidos a la protección de los activos y la minimización de daños a la Compañía, reduciendo la probabilidad de ocurrencia y mitigando al máximo los impactos en caso de que se materialicen, proponiendo los planes de respuesta y recuperación para los diferentes tipos de incidentes de seguridad y alineados con el Sistema de Gestión de Continuidad de Negocio. Supervisar la ejecución de dichos planes y reportar el estado.

- Proponer al Comité de Seguridad de la Información y Riesgos Tecnológicos el nivel de apetito por el riesgo de seguridad de la información, dentro del flujo de validación existente (tras la propuesta al Comité de Seguridad de la Información y riesgos Tecnológicos será elevado al Comité de Riesgos y al Consejo de Administración para su aprobación, previo análisis e integración con la propuesta de la Subdirección General de Tecnología, así como su valoración por parte de la SDG Adjunta de Control de Riesgos.)

- Evaluar el cumplimiento de los niveles objetivos de riesgo de seguridad que se establezcan y comunicar sobre ello al Comité de Seguridad de la Información y Riesgos Tecnológicos.

- Liderar el análisis de riesgos de seguridad de información, y presentar los resultados obtenidos para determinar el tratamiento del riesgo, así como proponer las medidas y controles que reduzcan el riesgo al Comité de Seguridad de la Información y Riesgos Tecnológicos.

- Definir KPIs / KRIs relativos a los riesgos de seguridad de la información, para su seguimiento.

- Informar y aconsejar al Consejo de Administración periódicamente y en momentos puntuales sobre la situación de seguridad de la información y su evolución.

- Evaluar si los proveedores de servicios cumplen con los requisitos de seguridad de la información establecidos.

- Promover la “cultura de la seguridad” favoreciendo las respuestas automáticas por parte de los usuarios y colaboradores de la Compañía.

Relación con otros órganos

- Comité de Seguridad de la Información y Riesgos Tecnológicos: reporte de toda la información relevante de Gestión de Seguridad de la Información, en los términos establecidos en el SGSI del Grupo Mutua.

- SDG Adjunta de Control de Riesgos: a quien reporta resultados de la actividad de análisis, evaluación y tratamiento de riesgos de seguridad, así como estado de definición e implantación de planes de seguridad y planes de corrección y mejora resultantes de las auditorías.

- Auditoría Interna: recepción de informes de resultados en la ejecución de auditorías. Sobre esto deberá reportar los planes de corrección y mejora que pudiesen resultar.

11. Seguridad Corporativa

Descripción – Unidad

La Dirección de Seguridad Corporativa vela por la adecuada implantación de las medidas de seguridad física para proteger las instalaciones, centros de datos y áreas sensibles, tanto en lo referente a la gestión de acceso físico a las instalaciones, como en lo relativo al acondicionamiento técnico de dichas instalaciones.

Responsabilidades

Sus principales responsabilidades en lo referente a la gestión de la seguridad de la información son:

- Definir, documentar e instaurar procedimientos para el control del acceso físico o la seguridad física. Dichos procedimientos se deberán instaurar, aplicar, supervisar y revisar periódicamente y, además, habrán de incluir controles para la supervisión de irregularidades

- Coordinar el análisis y gestión de la respuesta de los incidentes de seguridad física, llevando un registro de estos e informando de los relevantes a la mayor brevedad posible al CISO.

Relación con otros órganos

- Seguridad TI/CISO: reporte del estado de situación y evolución de iniciativas en implantación que afecten a la gestión de la Seguridad de la Información y el Riesgo TI.

- Auditoría Interna: recepción de informes de resultados en la ejecución de auditorías. Sobre esto deberá reportar los planes de corrección y mejora que pudiesen resultar.

12. Dirección de Compras Corporativas

Descripción – Unidad

La Dirección de Compras Corporativas (a través de la unidad Vendor Risk Management) vela por la identificación, evaluación y seguimiento de los potenciales riesgos de seguridad asociados a la subcontratación de servicios en terceros.

Responsabilidades

Sus principales responsabilidades en lo referente a la gestión de la seguridad de la información son las establecidas en la Política de externalización Adicionalmente serán relevantes las siguientes obligaciones en relación con todos los proveedores que tengan acceso a los sistemas de la compañía o a datos de esta:

- Asegurar que cumplen con lo establecido en las políticas y procedimientos de seguridad de la información, así como los requisitos en esta materia establecidos en los contratos que les apliquen y en la política de gestión de seguridad en la subcontratación de servicios y proveedores.

- Asegurar que conocen y difunden entre sus empleados las políticas mencionadas y las buenas prácticas de seguridad de la información y recibir concienciación al respecto.

Relación con otros órganos

- Comité de Seguridad de la Información y Riesgos Tecnológicos: al que reporta toda la información relevante en lo relacionado con el riesgo de seguridad de la información en terceras partes.

- Auditoría Interna: recepción de informes de resultados en la ejecución de auditorías. Sobre esto deberá reportar los planes de corrección y mejora que pudiesen resultar.

13. Dirección General Adjunta de Personas, Talento y Cultura

Descripción – Unidad

La Dirección General Adjunta de Personas, Talento y Cultura, velará por la adecuada implantación de las medidas relacionadas con la formación de las personas que forman parte de la organización en materia de gestión de riesgos TIC y Seguridad de la información.

Responsabilidades

Sus principales responsabilidades serán

- Desarrollar e implementar programas de formación periódica de riesgos TIC y Seguridad de la información destinados al órgano de dirección, así como ofrecer al resto de trabajadores de la compañía formaciones de resiliencia operativa de tal manera que permita comprender y evaluar el riesgo relacionado con las TIC. Garantizar la trazabilidad de los cursos realizados por los empleados, incluida la Alta Dirección, de cara a cumplir con los requerimientos que pudieran contener las diferentes normativas aplicables.

- Asegurar que en los procesos de contratación se consideren las competencias necesarias en materia de resiliencia operativa digital para asegurar el correcto nivel de conocimiento de los trabajadores y especialmente de aquellos que usen sistemas de información o tecnologías para el desempeño de sus actividades.

14. Obligaciones de los usuarios (resto de la organización)

De forma general, todo el personal de la Organización tiene el deber de conocer y cumplir la normativa corporativa de gestión de la seguridad.

En concreto, esta obligación supone:

- Informar a las funciones fundamentales de cualquier hecho relevante, presente o futuro, que pudiera afectar de forma significativa a la gestión de la seguridad de la información.
- Cumplir con la presente política, así como con todos los procedimientos asociados a ésta.
- Aprovechar la formación necesaria que le permita conocer las obligaciones y funciones en el ámbito de la presente política y los principios de la seguridad de la información y las TI.

III. ESTRATEGIA, PROCESOS Y PROCEDIMIENTOS

1. Documentación del Sistema de Gestión de Seguridad de la Información

Aunque el SGSI abarca una amplia cantidad de documentación, es importante tener en cuenta los documentos que lo conforman básicamente y que bajo ningún concepto pueden ser excluidos del mismo son:

- Política de Seguridad de la Información
- Alcance del Sistema
- Metodología de evaluación de riesgos de seguridad de la información
- Informe de evaluación de Riesgos
- El plan de tratamiento de dichos riesgos

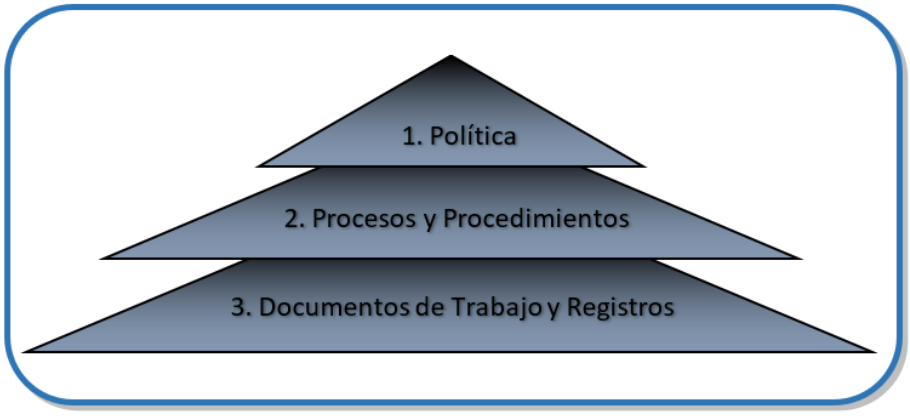
Los procedimientos documentados que necesita la organización para asegurar su correcta planificación, operación, control de sus procesos y eficacia de los controles impuestos.

Como mínimo, dichos procedimientos serán:

- Gestión documental
- Auditoría interna
- No conformidades, recomendaciones y mejora continua
- Medición del desempeño

- Proceso de recursos humanos
- Revisión por dirección
- Monitorización IT
- Objetivos de seguridad
- Seguridad en dispositivos móviles
- Actividades de teletrabajo
- Uso de activos y soportes
- Procedimiento de clasificación y tratamiento de la información
- Procedimiento de gestión de soportes
- Procedimiento de control de acceso físico
- Procedimiento de gestión de accesos
- Procedimiento de uso criptográfico
- Normativa de seguridad
- Procedimiento de operación (todos los del SGSI así como los operativos en posesión de las áreas).
- Procedimiento de códigos maliciosos
- Procedimiento de seguridad de gestión de cambios
- Procedimiento de intercambio de información
- Procedimiento de gestión de incidentes de seguridad
- Los registros requeridos por las normas bajo las cuales se documenta.
- La Declaración de Aplicabilidad

A continuación, se indica mediante el gráfico la jerarquía de dicha documentación dentro del SGSI:



2. Revisión y Actualización de procesos y procedimientos

Todos los documentos internos del SGSI son elaborados por el responsable de la Gestión de Seguridad y aprobados, por:

1. Comité de Seguridad de la Información y Riesgos Tecnológicos, en el que está representada la Dirección de Mutua Madrileña para revisar y aprobar la documentación de alto nivel del Sistema de Gestión de Seguridad de la Información y la Gestión de Riesgos TIC, planificación, alcance,y la normativa interna de Gestión de Riesgos Tecnológicos y roles y responsabilidades relacionadas con la gestión de riesgos y continuidad de los servicios.

2. El CISO para todas aquellas políticas y procedimientos técnicos.

En la aprobación se comprueba siempre la adecuación de este. Las fechas de aprobación y realización aparecen en el documento junto con el estado de revisión.

3. Normativa General de Seguridad

Todo el personal bajo las directrices de la organización tiene la obligación de conocer y cumplir las Normas de Uso y Seguridad de los Sistemas Corporativos.

3.1 Equipos corporativos

- Todos los equipos/dispositivos informáticos, que se conecten a la red de la organización deben ser proporcionados o autorizados por Mutua Madrileña.

- Sólo se debe instalar software suministrado o autorizado por Mutua Madrileña.

- Es obligación de todo el personal de la organización salvaguardar la seguridad de los equipos informáticos, bloquearlos o apagarlos cuando se abandone el puesto de trabajo.

- Se debe mantener la configuración del PC establecida por el Departamento de Sistemas.

- Las operaciones de mantenimiento sólo podrán ser realizadas por el personal del Área del CAU (Centro de Atención al Usuario) o en su defecto, cualquier otro personal de Sistemas autorizado.

- La Compañía podrá realizar auditorías e inspecciones a los PC (a las carpetas de red, SharePoint, Teams, etc.) sin previo aviso, con el fin de verificar que los programas y los ficheros y sus contenidos son los autorizados y su uso conforme se establece en las presentes normas. Para estas auditorías e inspecciones se requiere la autorización previa de la Dirección General de la Compañía o de la Dirección General Adjunta de Tecnología, quiénes podrán autorizar auditorías de inspecciones concretas o categorías de supuestos que podrán dar lugares a las mismas.

- Recuerda que los dispositivos entregados por la compañía son de uso profesional y NO personal:

    - Deben mantenerse en buen estado.

    - No se permite su personalización.

    - Ante pérdida o robo, se debe notificar mediante petición de servicio

    - Devolver todo el material cuando se produzca una desvinculación con la empresa

3.2 Teletrabajo

- El teletrabajo se realiza únicamente a través de los medios permitidos por el área de Tecnología.

- No está permitido utilizar conexiones desde redes no seguras (Wifis públicas y en lugares concurridos).

- Está prohibido almacenar información y documentación de MM en los equipos personales.

- En caso de conexión con equipo personal, éste debe tener un antivirus instalado y actualizado y tener un sistema operativo actualizado y con los últimos parches de seguridad instalados.

3.3 Autenticación y uso de contraseñas

- El código de usuario y la contraseña son personales e intransferibles; no deben ser compartidos.

- La contraseña inicial debe ser cambiada obligatoriamente.

- Se debe usar contraseñas seguras “fuertes”, una contraseña fuerte es aquella que no resulta fácil de adivinar, debe tener las siguientes características:

    - Una longitud mínima de al menos 8 caracteres.

    - Utilizar siempre una mezcla de caracteres diferentes (mayúsculas + minúsculas + números + símbolos).

- No se debe guardar la contraseña en un fichero del equipo, ni escritas en un post-it, cuadernos u hojas que estén a la vista y sean accesibles en el puesto de trabajo.

- No se deben usar identificadores genéricos (no asignados a un usuario concreto).
- Ante sospecha de que nuestra contraseña puede ser conocida, se debe cambiar inmediatamente.

3.4 Dispositivos Móviles y uso responsable de la telefonía

- Todos los dispositivos móviles corporativos llevan un código PIN de protección de mínimo 8 dígitos. No compartas ni dejes escrito dicho PIN.
- No está permitido proporcionar acceso a terceros al dispositivo.
- Únicamente se permite la descarga e instalación de aplicaciones procedentes de fuentes fiables (AppleStore, Play Store, etc).
- En caso de utilización de dispositivo personal para fines laborales es importante:
    - No almacenar información corporativa en el dispositivo.
    - Activar una metodología de bloqueo.
    - Deberá realizar actualizaciones del sistema operativo del teléfono móvil con regularidad.
- Evita el uso de los dispositivos fijos de telefonía para acciones personales.
- No se permite la modificación del sistema de dispositivos móviles “rooteo” o “jailbreak”.
- No se permite la creación de copias de seguridad en nubes no autorizadas por la compañía.

3.5 Procedimiento para la salida segura de datos corporativos

- La extracción de copias de los datos e información almacenados en los sistemas corporativos de la empresa, con la única excepción de aquellos que tengan carácter público, requieren la perceptiva autorización de la Dirección de la compañía, la cual se obtiene conforme se establece en el siguiente procedimiento:
    - El Responsable de solicitar la salida de información debe ponerse en contacto con el Departamento de Seguridad IT que le devolverá un formulario de Salida de Soportes.
    - El citado responsable debe rellenar el formulario y obtener autorización de:
        - El Área de Protección de Datos
        - La D.G.A de Tecnología
    - El formulario cumplimentado deberá ser devuelto a Seguridad IT, que comprobará si está debidamente cumplimentado y autorizado.
    - Si la salida es autorizada, se procederá a hacer la copia de los datos y/o de manera cifrada por el área de Seguridad IT.

3.6 Almacenamiento, transferencia y fuga de información

- No está permitido almacenar información corporativa en el disco duro del equipo de trabajo.
- Toda la información que se guarde en los equipos de Mutua Madrileña debe ser de carácter profesional, no personal.
- El acceso a la información de MM por parte de proveedores estará restringido a la información necesaria para la realización del servicio.
- Para trabajar fuera de la oficina no deben extraerse copias de los datos e información almacenados en los sistemas corporativos de la Entidad.
- No se debe facilitar información corporativa a personas no autorizadas. El envío de la información con terceros se realizará siguiendo el medio dictado por Mutua Madrileña.
- Se debe mantener la mesa de trabajo recogida con la documentación debidamente resguardada en las taquillas y armarios.
- No se debe dejar información confidencial en pizarras y otros tipos de pantallas.
- Se deben desactivar las notificaciones de ventanas emergentes cuando se comparte pantalla.

3.7 Red Interna

- Toda la información corporativa debe ser únicamente almacenada en los directorios corporativos (SharePoint, OneDrive, etc.) evitando el almacenamiento en el disco duro del PC.
- La información almacenada en los directorios corporativos debe ser de carácter profesional.

3.8 Nubes

- No alojes información corporativa en nubes no autorizadas por el área de Tecnología y Seguridad IT.
- Sólo podrán tener acceso a las nubes autorizadas por Seguridad IT, aquellos usuarios que hayan sido autorizados.

3.9 Internet y Correo Electrónico

- Utiliza internet únicamente con fines profesionales.
- No descargues software directamente de páginas de internet. Sólo puede instalar software suministrados o autorizados por Mutua Madrileña.
- Toma las máximas precauciones al bajar ficheros de internet.
- No está permitido el envío masivo de correos y el uso personal del mismo.

- Presta especial atención a la información enviada a los destinatarios de correo externos a la compañía. Recuerda que no se puede sacar información sin autorización.
- No abras y elimina siempre los mensajes y los enlaces sospechosos.
- No aceptes documentos ni archivos adjuntos provenientes de direcciones desconocidas.

3.10 Redes Sociales

- Evita manifestaciones, comentarios o afirmaciones sobre temas de la compañía que no estén autorizados o sean despectivos.
- No está permitido revelar fuentes de información corporativas.
- Evita hacer manifestaciones, comentarios o afirmaciones en contra de algún compañero. cliente o proveedor.
- No se permite el uso de WhatsApp para difundir información profesional.

3.11 Seguridad física

- Todo el personal bajo las directrices de la organización tiene la obligación de conocer y cumplir las normas de seguridad en los edificios corporativos.
- Los sistemas de seguridad y de protección instalados en el edificio, deben ser usados de forma responsable.
- Es obligación de todo el personal seguir en todo momento las indicaciones del personal de seguridad, especialmente las relacionadas a una posible emergencia en el edificio.
- La verificación de identidad mediante sistema biométrico se debe usar en los accesos a través de los tornos de seguridad, así como en las áreas críticas que disponen de este sistema.
- No está permitido acceder al centro de trabajo fuera del horario habitual. En caso de necesidad, se deberá comunicar con la suficiente antelación a la Dirección de seguridad corporativa.
- La tarjeta de acceso es personal e intrasferible.
- Se debe usar en los accesos a través de los tornos de seguridad, así como en las áreas críticas que disponen de este sistema. Además, debe portarse en un lugar visible en el interior de las instalaciones corporativas.
- No se debe prestar la tarjeta a ningún compañero y/o personal externo.
- Se debe resguardar los dispositivos portátiles en las taquillas habilitadas al finalizar la jornada laboral o al ausentarse del puesto de trabajo por un largo periodo.
- Ante el robo o extravío de la tarjeta, avisa al Centro Permanente de Seguridad.

3.12 Comunicación de Incidentes

- Todo el personal debe informar tan pronto como sea posible de cualquier incidente que pueda comprometer la Seguridad de los Sistemas de Información de Mutua Madrileña.

- La gestión de incidencias debe tramitarse de conformidad con el siguiente procedimiento:

    - Incidentes de seguridad relacionados con el uso y seguridad de los equipos: Al identificar una incidencia, se debe dar de alta una solicitud en la aplicación de gestión de Incidencias de la organización (Service Desk).

    - Al transmitir la incidencia deberá aportarse la siguiente información en la apertura de la incidencia:

        - Tipo de incidencia.

        - Categoría.

        - Momento en que se produce

        - Persona que comunica.

        - A quién se le comunica.

        - Efectos derivados de la incidencia

    - Una vez enviada la incidencia, a través de la herramienta, se iniciará el workflow del proceso de gestión de incidencias.

- También se dispone de un correo electrónico directo con el área de seguridad: ciberseguridad@group.mutua.es Si el incidente es de seguridad física, se debe notificar al Centro Permanente de Seguridad, bien a través de correo electrónico (ccp@mutua.es) o llamando al 915 92 25 06.

IV. ANEXO – DEFINICIONES

- Política → Conjunto de instrucciones o normas generales de actuación de una organización.

- Normativa interna → En este documento se hace referencia con estos términos al conjunto de documentos que desarrollan la política y son específicos del departamento, aprobados o en el ámbito del mismo o en algún comité, como el de Seguridad o el de Riesgos Tecnológicos y Continuidad de Negocio.

- Seguridad de la información → Consiste en la preservación de la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio.

- Seguridad → Cualidad de seguro: Libre y exento de todo peligro, daño o riesgo (RAE).

- Confidencialidad → La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

- Integridad → mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

- Disponibilidad → acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

- El apetito por el riesgo: indica el nivel global de riesgo que la entidad está dispuesta a aceptar o evitar con el fin de alcanzar sus objetivos estratégicos, frente a eventos inesperados. Se distinguen 3 niveles: preferencia (nivel deseable); tolerancia (zona de riesgo que marca la necesidad de analizar de forma preventiva un plan de actuación al desviarnos del nivel de preferencia, para evitar alcanzar el nivel de exceso. Valor a partir del cual, salta la alerta) y exceso (área de riesgo que se quiere evitar. Se inicia tras superar el límite).