POLÍTICA DE SEGURIDAD (ESQUEMA NACIONAL DE SEGURIDAD)

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 03 de Abril de 2024 por la dirección de Mutua Intercomarcal MCSS núm. 39.

Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

2. INTRODUCCIÓN

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

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 presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, trazabilidad e identidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los diferentes departamentos deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad el análisis y la gestión de los riesgos y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes de seguridad según lo establecido en el artículo 8 del ENS

2.1. Prevención

Los departamentos deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello los departamentos deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, los departamentos deben:

1. Autorizar los sistemas antes de entrar en operación.
2. Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
3. Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

2.2. Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 8 del ENS. La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

2.3. Respuesta

Los departamentos deben:

1. Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
2. Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
3. Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias o soporte externo especializado.

2.4. Recuperación

Para garantizar la disponibilidad de los servicios críticos, los departamentos deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

3. ALCANCE

Esta política se aplica a todos los sistemas TIC de Mutua Intercomarcal y a todos los miembros de la organización, sin excepciones.

4. MISIÓN

Preservar la disponibilidad, confidencialidad, integridad, trazabilidad y autenticidad (identidad) de toda la información y servicios vinculados a la actividad de Mutua Intercomarcal, en concreto:

- Servicio de Asistencia Sanitaria (marco de las funciones de las Mutuas de Trabajo).
- Gestión de prestaciones a los mutualistas y/o trabajadores protegidos.
- Gestión de los clientes Mutualistas
- Gestión de la relación y colaboración entre las personas que forman Mutua Intercomarcal.

5. MARCO NORMATIVO

- Ley 35/2014, de 26 de diciembre (Mutuas de Trabajo).
- Real Decreto 1993/1995 de 7 de diciembre (Entidad colaboradora con la Seguridad Social)
- Real Decreto 1060/2022 de 27 de diciembre
- Ley 41/2002, de 14 de noviembre (Ley del paciente).
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
- Real Decreto 311/2022 de 3 de mayo por el que se regula el Esquema Nacional de Seguridad
- Ley Orgánica 3/2018, del 5 diciembre.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016. (a partir del 25 de mayo de 2018).
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y comercio electrónico.

5.1. Instrucciones técnicas de seguridad del CCN

La organización respecto a las instrucciones técnicas de seguridad tendrá en cuenta las normas armonizadas a nivel europeo que resulten de aplicación:

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

6. ORGANIZACIÓN DE LA SEGURIDAD

6.1. Comités: funciones y responsabilidades

El Comité de Seguridad TIC está formado por:

- Director de T.I. y Sistema Integrado de Gestión: Sr. Toni Serra Carbonell
- Responsable de Seguridad y del SGSI: Sr. Jordi Muñoz Nieto
- Responsable Jurídico: Miquel Samper Alonso
- El secretario del Comité de Seguridad TIC es el Sr. Jordi Muñoz Nieto
- El Comité de Seguridad TIC reportará al Comité de Dirección.
- El Comité de Seguridad TIC tendrá las funciones descritas el documento “Comité de Seguridad TIC”.
- El comité es el órgano de resolución de conflictos entre los distintos actores del ENS.

6.2. Roles: funciones y responsabilidades

Los roles y responsabilidades de los diferentes actores se describen en el PRC-265 del sistema de gestión de la seguridad de la información (ISO 27001:2022)

6.3. Procedimientos de designación

El responsable de Seguridad de la Información es nombrado por la Dirección de Mutua Intercomarcal a propuesta del Comité de Seguridad TIC. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.
El Departamento responsable de un servicio que se preste electrónicamente de acuerdo a la Ley

39/2015 de 1 de Octubre, designará al responsable del Sistema, precisando sus funciones y responsabilidades dentro del marco establecido por esta Política. En el caso de Mutua Intercomarcal el responsable de seguridad y del sistema es el mismo.

6.4. Política de seguridad de la información

Será misión del Comité de Seguridad TIC la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por la Dirección de Mutua Intercomarcal y difundida para que la conozcan todas las partes afectadas. (en la intranet y la web de Mutua Intercomarcal).

7. DATOS DE CARÁCTER PERSONAL

Mutua Intercomarcal trata datos de carácter personal. El registro de actividades del tratamiento recoge los ficheros afectados y/o actividades de tratamiento y los responsables correspondientes. Todos los sistemas de información de Mutua Intercomarcal se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en los mencionados documentos.

8. GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

Regularmente, al menos una vez al año:

- Cuando cambie la información manejada
- Cuando cambien los servicios prestados
- Cuando ocurra un incidente grave de seguridad
- Cuando se reporten vulnerabilidades graves

Para la armonización de los análisis de riesgos, el Comité de Seguridad TIC establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad TIC dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

9. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información complementa las políticas de seguridad de Mutua Intercomarcal en diferentes materias:

- Política de Privacidad (para LOPDGDD)
- Política de Seguridad ISO 27001
- Política del SIG (Calidad, Medio Ambiente y ISO 45001)

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos

específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones. La normativa de seguridad estará disponible en la página web de Mutua Intercomarcal.

10. OBLIGACIONES DEL PERSONAL

Todos los miembros de Mutua Intercomarcal tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad TIC disponer los medios necesarios para que la información llegue a los afectados. Todos los miembros de Mutua Intercomarcal atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de Mutua Intercomarcal, en particular a los de nueva incorporación. Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

11. TERCERAS PARTES

Cuando Mutua Intercomarcal preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando Mutua Intercomarcal utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

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. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

12. PROTECCIÓN DE LAS INSTALACIONES

Los sistemas se encuentran en áreas separadas cerrados con llave y con un sistema de seguridad de control de acceso

13. ADQUISICIÓN DE PRODUCTOS

1. La adquisición de productos de seguridad de las tecnologías de la información y comunicaciones, se utilizan de forma proporcionada a la categorización Media del sistema.
2. La certificación indicada en el apartado anterior debe estar de acuerdo con las normas y estándares de mayor reconocimiento internacional en el ámbito de la seguridad funcional.
3. El Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información, constituido al amparo de lo dispuesto en el artículo 2.2.c) del Real Decreto 421/2004, de 12 de marzo, y regulado por la orden PRE/2740/2007, de 19 de septiembre, dentro de sus competencias, determina el criterio a cumplir en función del uso previsto del producto a que se refiera, en relación con el nivel de evaluación, otras certificaciones de seguridad adicionales que se requieran normativamente, así como, excepcionalmente, en los casos en que no existan productos certificados. El proceso indicado, se efectúa teniendo en cuenta los criterios y metodologías de evaluación, determinados por las normas internacionales que recoge la orden ministerial citada.
4. Para la contratación de servicios de seguridad se estará a lo dispuesto en los apartados anteriores y en el artículo 15.

14. PROTECCIÓN DE LA INFORMACIÓN ALMACENADA Y EN TRÁNSITO

1. En la estructura y organización de la seguridad del sistema, se prestará especial atención a la información almacenada o en tránsito a través de entornos inseguros. Tendrán la consideración de entornos inseguros los equipos portátiles, teléfonos móviles, tabletas, dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil.
2. Forman parte de la seguridad los procedimientos que aseguren la recuperación y conservación a largo plazo de los documentos electrónicos producidos por las Administraciones públicas en el ámbito de sus competencias.
3. Toda información en soporte no electrónico, que haya sido causa o consecuencia directa de la información electrónica, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello se aplicarán las medidas que correspondan a la naturaleza del soporte en que se encuentren, de conformidad con las normas de aplicación a la seguridad de los mismos.

15. REGISTRO DE ACTIVIDAD

Con la finalidad exclusiva de lograr el cumplimiento del objeto del 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, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

16. CONTINUIDAD DE LA ACTIVIDAD

Los sistemas dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.

Firmado:
Lluís Gené Torrandell
Director general