1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 13 de Julio de 2021 por Salvador Mercé, CEO de MERCÉ V. ELECTROMEDICINA S.L. Esta Política se Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

2. TÉRMINOS Y DEFINICIONES UTILIZADOS EN ESTA POLÍTICA

SGSI: Son las siglas del Sistema de Gestión de la Seguridad de la Información (regulado por la Norma UNE-ISO/IEC 27001), que es un conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.
TIC: Son las siglas de Tecnologías de la Información y la Comunicación. Este concepto hace referencia a las teorías, las herramientas y las técnicas utilizadas en el tratamiento y la transmisión de la información: informática, internet y telecomunicaciones.
Parte interesada: Persona o grupo que tiene un interés en el desempeño o éxito de la organización.
Confidencialidad: Propiedad de la información de no ponerse a disposición o ser reveladas a personas y o empresas no autorizadas.
Integridad: Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
Disponibilidad: Propiedad de la información de estar accesible y utilizable en el momento que se requiera por la persona y o empresa autorizada.
Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.
Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
Análisis de riesgos: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
Tratamiento de riesgos: Proceso de modificar el riesgo, mediante la implementación de controles.

3. INTRODUCCIÓN

MERCÉ V. ELECTROMEDICINA S.L. 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 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 prontitud y diligencia a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, 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 la norma UNE ISO/IEC 27001, 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 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 conformidad con la normativa de seguridad.

3.1. 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 la norma UNE ISO/IEC 27001, 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:

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

3.2. 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 control sobre la revisión de las políticas para la seguridad de la información (A.5.1.2).

La monitorización es especialmente relevante cuando se establecen líneas de defensa. 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.

3.3. RESPUESTA

Los departamentos deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en terceros a los que preste servicios.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con el centro de respuesta a incidentes de seguridad (INCIBE-CERT).

3.4. 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.

4. ALCANCE

El Alcance General de los sistemas de información asociados a los procesos de negocio que están sujetos a certificación de la norma UNE ISO/IEC 27001 es el siguiente: "***Sistemas de información que sustentan y dan soporte a los servicios de ventas, distribución, instalación y servicio posventa de productos sanitarios***

estériles y no estériles, en los campos de la cardiología, cirugía cardíaca, cirugía y radiología vascular, neurorradiología vascular intervencionista y cirugía oncológica".

5. MISIÓN, COMPROMISO Y LIDERAZGO

La Dirección de MERCÉ V. ELECTROMEDICINA S.L. se compromete a facilitar y proporcionar los recursos necesarios para el establecimiento, implantación, mantenimiento y mejora del Sistema de Gestión de la Seguridad de la Información, así como a demostrar liderazgo y compromiso respecto a este, a través de la constitución del Comité de Seguridad, de sus funciones y responsabilidades. Es misión de esta Dirección:

- Mantener el pleno cumplimiento legal
- Fomentar los planes de formación y concienciación
- Mantener unos óptimos niveles reputacionales
- Gestionar de forma eficaz y efectiva los incidentes de seguridad
- Desarrollar una adecuada política comunicativa y transparente
- Con carácter general, preservar la confidencialidad, integridad y disponibilidad de la información

Este compromiso se extiende a las partes interesadas descritas en el contexto del SGSI, para satisfacer sus intereses y expectativas en seguridad de la información.

6. MARCO NORMATIVO

MERCÉ V. ELECTROMEDICINA S.L. está sujeto, a título enunciativo y no limitativo, a las siguientes normativas y regulaciones:

- 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)
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico
- Real Decreto Legislativo 1/1996, de 12 de abril, Ley de Propiedad Intelectual
- Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo
- 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
- Directiva 93/42/EEC: Directiva relativa a los productos sanitarios (modificada por Directiva 2007/47/EC)
- Reglamento (EU) 2017/745 sobre Productos Sanitarios: Reglamento (EU) sobre Productos Sanitarios (MDR)
- Circular nº 3/2012: Asistencia Técnica de Productos Sanitarios
- MEDDEV 2.12/1 rev.8: Medical devices vigilance system. Manufacturer incident report. Field Safety Corrective Action. + List of contact points (01/2013) & Additional guidance on MEDDEV 2.12/1 rev.8 (07/2019)

7. OBJETIVOS DE SEGURIDAD DEL SGSI

MERCÉ V. ELECTROMEDICINA S.L., para lograr el cumplimiento de su cuerpo principal y de su anexo A, que recogen los principios básicos y de los requisitos mínimos, ha implementado diversas medidas de seguridad proporcionales a la naturaleza de la información y los servicios a proteger y teniendo en cuenta su análisis de riesgos y su declaración de aplicabilidad.

Seguridad como un proceso integral y seguridad por defecto
La seguridad constituye un proceso integrado por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. La aplicación de la norma UNE ISO/IEC 27001 en MERCÉ V. ELECTROMEDICINA S.L. estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuente de riesgo para la seguridad.

Los sistemas se diseñarán de forma que garanticen la seguridad por defecto, del siguiente modo:

a) El sistema proporcionará la mínima funcionalidad requerida para que la organización alcance sus objetivos.
b) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde emplazamientos o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso facultados.
c) En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que no sean de interés, sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue.
d) El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

Reevaluación periódica e integridad y actualización del sistema
MERCÉ V. ELECTROMEDICINA S.L. ha implementado controles y evaluaciones regulares de la seguridad, (incluyendo evaluaciones de los cambios de configuración de forma rutinaria), para conocer en todo momento el estado de la seguridad de los sistemas en relación con las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos. Antes de la entrada de nuevos elementos, ya sean físicos o lógicos, estos requerirán de una autorización formal.

Así mismo, solicitará la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

Gestión de personal y profesionalidad
Todos los miembros de MERCÉ V. ELECTROMEDICINA S.L., dentro del ámbito de la norma UNE ISO/IEC 27001, atenderán a una sesión de concienciación en materia de seguridad al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros, 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.

Gestión de la seguridad basada en los riesgos y análisis y gestión de riesgos
Todos los sistemas afectados por esta Política de Seguridad, así como todos los tratamientos de datos personales, deberán ser objeto de un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos cada una vez al año.
- Cuando cambien la información manejada y/o los servicios prestados de manera significativa.
- Cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.

El Responsable de Seguridad será el encargado de que se realice el análisis de riesgos (con asesoramiento externo), así como de identificar carencias y debilidades y ponerlas en conocimiento del Comité de Seguridad de la Información.

Incidentes de seguridad, prevención, reacción y recuperación
MERCÉ V. ELECTROMEDICINA S.L. ha implementado un proceso integral de detección, reacción y recuperación frente a código dañino mediante el desarrollo de procedimientos que cubren los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

Para que la información y/o los servicios no se vean perjudicados por incidentes de seguridad, MERCÉ V. ELECTROMEDICINA S.L. implementa las medidas de seguridad establecidas por la norma UNE ISO/IEC 27001, así como cualquier otro control adicional, que haya identificado como necesario, a través de una evaluación de amenazas y riesgos. Estos controles, así como los roles y responsabilidades de seguridad de todo el personal, están claramente definidos y documentados.

Cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales, se establecerán los mecanismos de detección, análisis y reporte necesarios para que lleguen a los responsables regularmente.

MERCÉ V. ELECTROMEDICINA S.L. establecerá las siguientes medidas de reacción ante incidentes de seguridad:

- Mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con el centro de respuesta a incidentes de seguridad (INCIBE-CERT).
- Para garantizar la disponibilidad de los servicios, MERCÉ V. ELECTROMEDICINA S.L. dispone de los medios y técnicas necesarias que permiten garantizar la recuperación de los servicios más críticos.

Líneas de defensa y prevención ante otros sistemas interconectados
MERCÉ V. ELECTROMEDICINA S.L. ha implementado una estrategia de protección basada en múltiples capas, constituidas por medidas organizativas, físicas y lógicas, de tal forma que cuando una de las capas falle, el sistema implementado permita:

- Ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse.
- Reducir la probabilidad de que el sistema sea comprometido en su conjunto.
- Minimizar el impacto final sobre el mismo.

Esta estrategia de protección ha de proteger el perímetro, en particular, si se conecta a redes de terceros. En todo caso se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión.

Función diferenciada y organización e implantación del proceso de seguridad
MERCÉ V. ELECTROMEDICINA S.L. ha organizado su seguridad comprometiendo a todos los miembros de la corporación mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas, tal y como se recoge en el apartado de “ORGANIZACIÓN DE LA SEGURIDAD” del presente documento.

Autorización y control de los accesos
MERCÉ V. ELECTROMEDICINA S.L. ha implementado mecanismos de control de acceso al sistema de información, limitándolos a los estrictamente necesarios y debidamente autorizados.

Protección de las instalaciones
MERCÉ V. ELECTROMEDICINA S.L. ha implementado mecanismos de control de acceso físico, previniendo los accesos físicos no autorizados, así como los daños a la información y a los recursos, mediante perímetros de seguridad, controles físicos y protecciones generales en áreas.

Adquisición de productos de seguridad y contratación de servicios de seguridad
Para la adquisición de productos, MERCÉ V. ELECTROMEDICINA S.L. tendrá en cuenta que dichos productos tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen, a juicio del responsable de Seguridad.

Protección de la información almacenada y en tránsito y continuidad de la actividad
MERCÉ V. ELECTROMEDICINA S.L. ha implementado mecanismos para proteger la información almacenada o en tránsito, especialmente cuando esta se encuentra en entornos inseguros (portátiles, tablets, soportes de información, redes abiertas, etc.).

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.

Se han desarrollado procedimientos que aseguran la recuperación y conservación a largo plazo de los documentos electrónicos producidos en el ámbito de las competencias de MERCÉ V. ELECTROMEDICINA S.L. De igual modo, se han implementado mecanismos de seguridad en base a la naturaleza del soporte en el que se encuentren los documentos, para garantizar que toda información relacionada en soporte no electrónico esté protegida con el mismo grado de seguridad que la electrónica.

Registros de actividad
MERCÉ V. ELECTROMEDICINA S.L. ha habilitado registros de la actividad 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. Todo ello con la finalidad exclusiva de lograr el cumplimiento del objeto del presente real decreto, 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.

8. ORGANIZACIÓN DE LA SEGURIDAD

8.1. COMITÉS: FUNCIONES Y RESPONSABILIDADES

El Comité de Seguridad estará formado por: Dirección de la Entidad (CEO), Director de Operaciones, Director TIC, Delegado de Protección de Datos.

El Comité de Seguridad celebrará sus sesiones en las dependencias de MERCÉ V. ELECTROMEDICINA S.L. con periodicidad anual (salvo convocatoria extraordinaria), previa convocatoria al efecto realizada por el Presidente de dicho Comité.

Las funciones del Comité de Seguridad serán las siguientes:

- *Atender las solicitudes, en materia de Seguridad de la Información, de MERCÉ V. ELECTROMEDICINA S.L. y de los diferentes roles de seguridad y/o áreas informando regularmente del estado de la Seguridad de la Información*
- *Asesorar en materia de Seguridad de la Información*

- *Resolver los conflictos de responsabilidad que puedan aparecer entre las diferentes áreas o departamentos*
- *Promover la mejora continua del sistema de gestión de la Seguridad de la Información. Para ello se encargará de:*
    - *Coordinar los esfuerzos de las diferentes áreas en materia de Seguridad de la Información, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades*
    - *Proponer planes de mejora de la Seguridad de la Información, con su dotación presupuestaria correspondiente, priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados*
    - *Velar porque la Seguridad de la Información se tenga en cuenta en todos los proyectos desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC*
    - *Realizar un seguimiento de los principales riesgos residuales asumidos por MERCÉ V. ELECTROMEDICINA S.L. y recomendar posibles actuaciones respecto de ellos*
    - *Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos*
    - *Elaborar y revisar regularmente la Política de Seguridad de la Información para su aprobación por el CEO*
    - *Elaborar la normativa de Seguridad de la Información para su aprobación en coordinación con la Dirección General*
    - *Verificar los procedimientos de seguridad de la información y demás documentación para su aprobación*
    - *Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de Seguridad de la Información y en particular en materia de protección de datos de carácter personal*
    - *Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de Seguridad de la Información*
    - *Promover la realización de las auditorías internas anuales y de protección de datos que permitan verificar el cumplimiento de las obligaciones de MERCÉ V. ELECTROMEDICINA S.L. en materia de seguridad de la información*

8.2. ROLES: FUNCIONES Y RESPONSABILIDADES

- Dirección de la Entidad: CEO de MERCÉ V. ELECTROMEDICINA S.L.
    - *Asegurarse que el sistema de gestión de la seguridad de la información es conforme con los requisitos de la norma UNE ISO/IEC 27001*
    - *Informar a otras partes de la alta dirección (si existe) sobre el comportamiento del sistema de gestión de la seguridad de la información*

- Responsable de Seguridad[1] de la Información, cuya figura recae en la Dirección TIC, y tendrá como funciones, las siguientes:
    - *Notificar la presente política al personal de la entidad y de los cambios que en ella se produzcan*
    - *Coordinar las acciones de implantación, mantenimiento y mejora del SGSI de la entidad, y de sus auditorías*
    - *Supervisar el cumplimiento de la presente Política, de sus normas, procedimientos derivados y de la configuración de seguridad de los sistemas*
    - *Promover las actividades de concienciación y formación en materia de seguridad en su ámbito de responsabilidad*

[1] Debido a la estructura organizativa, Responsable de Seguridad y Responsable del Sistema recae en la misma persona.

- *Realizar con la colaboración del Responsable del Sistema, los preceptivos análisis de riesgos, de seleccionar las salvaguardas a implantar y de revisar el proceso de gestión del riesgo. Asimismo, aceptar los riesgos residuales calculados en el análisis de riesgos*
- *Proponer a la Dirección para su aprobación la documentación del SGSI*
- *Mantener la documentación organizada y actualizada, gestionando los mecanismos de acceso a la misma*
- *Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad*
- *Realizar ejercicios y pruebas sobre los procedimientos operativos de seguridad y los planes de continuidad existentes*
- *Seguimiento del ciclo de vida de los sistemas: especificación, arquitectura, desarrollo, operación, cambios*
- *Implantar las medidas necesarias para garantizar la seguridad del sistema durante todo su ciclo de vida*
- *Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema*
- *Ordenar suspender el manejo de una determinada información o la prestación de un servicio electrónico si es informado de deficiencias graves de seguridad*

- Delegado de Protección de Datos, cuya figura recae en GESPRODAT S.L. (proveedor externo), y tendrá como funciones, las siguientes:
  - *Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del Reglamento General de Protección de Datos (RGPD) y de otras disposiciones de protección de datos de la Unión o de los Estados miembros*
  - *Supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes*
  - *Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35 RGPD*
  - *Cooperar con la autoridad de control*
  - *Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36 RGPD, y realizar consultas, en su caso, sobre cualquier otro asunto*

- Todo el personal de MERCÉ V. ELECTROMEDICINA S.L. será responsable de:
  - *Cumplir la presente política dentro de su área de trabajo*
  - *Aplicar toda la información documentada del SGSI de la entidad en sus actividades laborales que afecta a su desempeño en seguridad de la información*
  - *Transmitir cualquier información relevante sobre seguridad al responsable de Seguridad de la Información*
  - *Proteger y custodiar la información de la empresa, evitando la revelación, emisión al exterior, modificación, borrado o destrucción accidental o no autorizadas o el mal uso independientemente del soporte o medios por el que haya sido accedida o conocida*

8.3. PROCEDIMIENTOS DE DESIGNACIÓN

El Responsable de Seguridad de la Información será nombrado por el CEO de MERCÉ V. ELECTROMEDICINA S.L. a propuesta del Comité de Seguridad. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

8.4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del Comité de Seguridad 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 el CEO de MERCÉ V. ELECTROMEDICINA S.L. y difundida para que la conozcan todas las partes interesadas.

9. DATOS DE CARÁCTER PERSONAL

MERCÉ V. ELECTROMEDICINA S.L. trata datos de carácter personal. Los procedimientos de protección de datos, al que tendrán acceso sólo las personas autorizadas, recoge los tratamientos afectados y los responsables correspondientes. Todos los sistemas de información de MERCÉ V. ELECTROMEDICINA S.L. 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 procedimientos.

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

11. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información complementa las políticas de seguridad de MERCÉ V. ELECTROMEDICINA S.L. en diferentes materias:

- Políticas de Sistemas de Gestión de la Calidad en Productos Sanitarios, según norma ISO 13485

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 carpeta ISO 27001 dentro del Portal Empleado (sitio SharePoint) en la Intranet.

12. OBLIGACIONES DEL PERSONAL

Todos los miembros de MERCÉ V. ELECTROMEDICINA S.L. 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 disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de MERCÉ V. ELECTROMEDICINA S.L. 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 MERCÉ V. ELECTROMEDICINA S.L., 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.

13. TERCERAS PARTES

Cuando MERCÉ V. ELECTROMEDICINA S.L. preste servicios a terceros, 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 y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando MERCÉ V. ELECTROMEDICINA S.L. subcontrate servicios con terceros o ceda información a terceros, en el marco de una prestación de servicios 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.

14. FIRMA

Revisado por: **Nombre y Apellidos**	**Cargo**	**Fecha**
JESÚS GARCÍA PÉREZ	Responsable de Seguridad	12/07/2021
Aprobado por: **Nombre y Apellidos**	**Cargo**	**Fecha**
SALVADOR MERCÉ CERVELLÓ	CEO	13/07/2021
Sistema de firma	**[X] Electrónica**	**[ ] Manual**

22625017D SALVADOR IGNACIO MERCE (R: B96056023)

Firmado digitalmente por 22625017D SALVADOR IGNACIO MERCE (R: B96056023)
Fecha: 2021.07.13 12:30:26 +02'00'