POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

ÍNDICE

1. INTRODUCCIÓN

La información es uno de los principales activos de Cáritas diocesana de Madrid (en adelante, CM) y, como tal activo, está expuesto a riesgos y amenazas que pueden provenir desde dentro o fuera de la organización, y pueden ser intencionales o accidentales. La ocurrencia de dichos riesgos puede provocar pérdidas materiales y/o económicas, daños en la imagen institucional y eclesial y en la confianza de los donantes y financiadores, incumplimiento o infracciones legales, vulneración de los derechos de los usuarios o beneficiarios de su actividad, así como los de los voluntarios, colaboradores, trabajadores o de terceros. Por tanto, es importante proteger adecuadamente los activos de información de CM.

La política de seguridad describe las directrices globales de seguridad de la información de CM definidas por sus órganos de gobierno y, en particular de la Secretaría General, así como los criterios para proteger los activos de información. CM, tiene como valores la centralidad de la persona, la persona como centro de la acción de CM y la defensa de su dignidad, y la transparencia, como apertura de la información a todos los interesados en la labor de CM. Con el fin de amparar estos valores se diseñan estas reglas y orientaciones.

Esta Política está basada en ISO/IEC 27001:2022 - Tecnología de la Información y el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Estas directrices incluyen la adopción de una serie de medidas organizativas y normas que se presentan en este documento y se desarrollan en sus documentos asociados y cuya finalidad es la de proteger los recursos de información de CM y los sistemas de información utilizados para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

En vista de lo anterior, el órgano de gobierno de CM establece unos objetivos estratégicos de Seguridad de la Información, alineados con las estrategias y los objetivos de su actividad.

Esta Política de Seguridad sigue las indicaciones de la guía CCN-STIC-805 del Centro Criptológico Nacional, centro adscrito al Centro Nacional de Inteligencia.

1.1. Prevención

CM debe 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 se implementarán las medidas mínimas de seguridad determinadas en los requisitos establecidos por la norma UNE-EN ISO/IEC 27001:2022 y la Ley Orgánica de Protección de Datos, asegurando la confidencialidad, integridad y disponibilidad de la información, así como la continuidad de sus servicios. Así como, por el Real Decreto 311/2022, de 3 de mayo, por el que se regula el

Esquema Nacional de Seguridad, RGPD y la LOPD, 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, van a estar claramente definidos y documentados. Para garantizar el cumplimiento de la política, CM debe: 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.

1.2. Detección

Dado que los servicios pueden verse afectados por incidentes de seguridad de la información, es necesario monitorizar su operación de forma continua para detectar anomalías en los niveles de prestación y actuar en consecuencia, conforme a los controles establecidos por la norma UNE-EN ISO/IEC 27001:2022. Se implementarán mecanismos de detección, análisis y reporte que permitan informar a los responsables tanto de forma periódica como cuando se produzcan desviaciones significativas respecto a los parámetros definidos como normales.

1.3. Respuesta

CM: Establece mecanismos para responder eficazmente a los incidentes de seguridad. Designa un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros Departamentos o en otros organismos.

1.4. Recuperación

Para garantizar la disponibilidad de los servicios críticos, CM ha desarrollado planes de contingencia de sistemas TIC como parte de su plan general de continuidad del servicio y actividades de recuperación.

2. ÁMBITO DE APLICACIÓN

Estas medidas de seguridad se aplican a CM, y a las siguientes entidades, a las que ofrece soporte entre otras cuestiones en materia de Seguridad, Comunicaciones y Gestión de la Información:

- Fundación de Caridad La Constructora Benéfica - G78077716
- Fundación Pilar de la Mata - Q8745313
- Fundación Santa Lucía - NIF Q88001553
- Fundación LABORAFIT - NIF B88644588
- Fundación para el Fomento del Empleo Labora - NIF G81016917
- Carifood SLU - NIF B88009774
- Asiscar SLU - NIF B81247025
- Textil Empleo SLU - NIF B88164322

3. OBJETIVOS

La Política de Seguridad de la Información tiene como objetivos:

- Implementar el sistema de gestión de seguridad de la información.
- Establecer las normas, procedimientos, compromisos y documentación formativa en materia de seguridad de la información y, especialmente, en los relacionados con la protección de datos de carácter personal.
- Proteger los activos tecnológicos.
- Minimizar el riesgo en las funciones más importantes del sistema de gestión de la información de CM.
- Cumplir con los principios de seguridad de la información.
- Mantener la confianza de sus donantes, empleados, voluntarios, colaboradores y demás partes interesadas.
- Fortalecer la cultura de seguridad de la información de los empleados, voluntarios, colaboradores y proveedores de CM.
- Garantizar la continuidad de los servicios frente a incidentes.

4. COMPROMISOS PARA LA SEGURIDAD DE LA INFORMACION

CM, con el afán de garantizar la seguridad de la información y de los datos de carácter personal que trata en el desarrollo de su actividad, establece los siguientes compromisos:

a. CM protegerá contra el riesgo la información generada, procesada o almacenada por los diferentes procesos, su infraestructura tecnológica y activos que se genera de los accesos otorgados a terceros (ej.: proveedores), o como resultado de un servicio interno o externo.

b. CM protegerá la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información generada, procesada o almacenada por los diferentes procesos, con el fin de minimizar impactos financieros, operativos o legales debido a su uso incorrecto. Para ello, dentro de los límites legalmente establecidos, velará por el uso adecuado de los equipos y dispositivos electrónicos de CM puestos a disposición de sus agentes.

c. CM protegerá su información y sus activos tecnológicos contra las amenazas de origen interno o externo a la organización.

d. CM garantizará el cumplimiento de los derechos y las obligaciones legales enunciadas en la introducción, y en concreto, por lo que se refiere a la seguridad y transparencia de la información. Asimismo, observará el cumplimiento de otras normas regulatorias y contractuales establecidas.

e. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por todas las partes interesadas.

5. ALCANCE

5.1. Agentes

La Seguridad de la Información requiere la implicación y participación de todos los miembros de la organización, esto es, todos los trabajadores, voluntarios y colaboradores que trabajan en CM. Por ello, cada agente debe cumplir los requerimientos de la Política de Seguridad y su documentación asociada. Se establecerán las medidas adecuadas ante el incumplimiento deliberado o por negligencia de la presente Política de Seguridad.

5.2. Sistemas de Información

Esta Política afecta a todos los activos de Información de la organización, tanto a equipos personales o servidores, redes, aplicaciones, sistemas operativos y procesos de la organización que pertenecen y/o son administrados por CM.

5.3. Otras partes interesadas

La presente Política de Seguridad es de conocimiento y cumplimiento extensible para cualquier persona externa perteneciente a terceras organizaciones que realice cualquier tipo de tratamiento sobre la información propiedad de CM. Asimismo, esta Política y sus procedimientos asociados serán de obligado cumplimiento para las organizaciones terceras proveedoras contratadas para la ejecución de servicios profesionales en los ámbitos que se consideren oportunos, en el caso de que realicen cualquier actividad que implique acceso o tratamiento a cualquier sistema o información propiedad de CM y así se definirá contractualmente.

6. MARCO NORMATIVO

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, establece y regula las bases del régimen jurídico de las Administraciones Públicas, los principios del sistema de responsabilidad de las Administraciones Públicas y de la potestad sancionadora, así como la organización y funcionamiento de la Administración General del Estado y de su sector público institucional para el desarrollo de sus actividades.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- 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.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley 34/2002 de Servicios de la Sociedad de la Información (LSSI).
- Ley 22/11, de 11/11/1987, de Propiedad Intelectual.
- Ley 17/2001, de Marcas.
- REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

• Ley 6/2020, de 11 de noviembre, reguladora de Asesoría Jurídica determinados aspectos de los servicios electrónicos de confianza.

• Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

• Ley 10/2021, de 9 de julio, de trabajo a distancia.

7. ORGANIZACIÓN DE LA SEGURIDAD

7.1. Comité de Seguridad de la Información.

El Comité de Seguridad de la Información (en adelante CSI) se ha constituido a fecha de 21 de mayo de 2026, estando formado por los siguientes integrantes:

• Responsable de Seguridad.

• Responsable de Servicio.

• Responsable de Sistemas de Información.

• Responsable de Sistemas.

• Responsable de Protección de datos.

• Administrador del Sistema.

• Administrador de Seguridad (SOC).

Las funciones de esté comité, en relación con el Sistema de Gestión de la Seguridad e la Información (SGSI), pasarán por:

• Atender las inquietudes del Equipo Directivo y de las diferentes Áreas.

• Informar regularmente del estado de la seguridad de la información al Equipo Directivo.

• Promover la mejora continua del SGSI.

• Elaborar la estrategia de evolución de CM en lo que respecta a la seguridad de la información.

• Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.

• Elaborar (y revisar regularmente) la Política de Seguridad de la información para que sea aprobada por la Dirección.

• Aprobar la normativa de seguridad de la información.

• Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.

• Monitorizar los principales riesgos residuales asumidos por CM y recomendar posibles actuaciones respecto de ellos.

• Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.

• Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.

• Aprobar planes de mejora de la seguridad de la información de CM. En particular, velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.

• Velar por que la seguridad de la información se tenga en cuenta en todos los proyectos TIC 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.

• Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la Organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir. Recabará regularmente del personal técnico propio o externo, la información pertinente para tomar decisiones. Se asesorará de los temas que tenga que decidir o emitir una opinión. Este asesoramiento se determinará en cada caso, pudiendo materializarse de diferentes formas y maneras:

- Grupos de trabajo especializados internos, externos o mixtos.
- Asesoría interna y/o externa. Asistencia a cursos u otro tipo de entornos formativos o de intercambio de experiencias.

• Aprobará el Plan de Mejora de la Seguridad, con su dotación presupuestaria correspondiente, en caso de ocurrencia de incidentes de seguridad de la información.

7.2. Roles: funciones y responsabilidades

7.2.1 Responsable de seguridad

• Implantación, desarrollo y mantenimiento de seguridad.

• Coordinar la gestión de la seguridad de la información en toda la institución.

• Definir y desarrollar un conjunto de procedimientos de gestión de seguridad y sus estándares.

• Ofrecer asesoramiento en todos los aspectos de la gestión de la seguridad de la información.

• Identificar cualquier problema que influya en la Seguridad de los productos y del servicio.

• Investigar todos los incidentes de seguridad que sucedan.

• Iniciar acciones para prevenir y/o corregir las no conformidades relativas a la seguridad de la información y asegurarse de que se llevan a cabo estas acciones.

• Asegurarse que se promueve la toma de conciencia de los requisitos del cliente en cuanto a seguridad de la información en todos los niveles de la institución.

• Conservar y revisar el Manual de Seguridad, los Procedimientos documentados y las Instrucciones de Trabajo.

• Informar a la Dirección sobre el desempeño del Sistema de la Seguridad de la Información y cualquier necesidad de mejora.

• Desarrollar los programas de concienciación y formación de la Seguridad para los empleados de la institución.

• Monitorizar la efectividad de los controles para garantizar la seguridad de la información.

• Propondrá los Planes de Mejora y solicitará la aprobación de las inversiones que posiblemente conlleven.

Contará con el apoyo de la Dirección y con los recursos necesarios, tecnológicos y de personal.

Debe proporcionar soporte a las siguientes actividades:

• Análisis de riesgos.

• Proyectos relacionados con la seguridad.

• Implementación y mantenimiento de los procesos necesarios para gestión de la Seguridad.

• Auditorías.

• Incorporación de requerimientos de seguridad de la información en contratos y acuerdos.

• Desarrollo de planes de continuidad de negocio en la institución.

• Confeccionar el Plan Anual de Formación, relacionado con la seguridad de la Información, en función de las necesidades de la institución.

Mantenerse al día en novedades tecnológicas, nuevas amenazas o vulnerabilidades, estándares internacionales, legislación o regulación relacionada con la seguridad de la información; mantener contacto con consultores expertos en el sector y con proveedores.

7.2.2 Responsable del servicio

• El ENS asigna al responsable del servicio la potestad de establecer los requisitos del servicio en materia de seguridad. O, en terminología del ENS, la potestad de determinar los niveles de seguridad de los servicios.

• La prestación de un servicio siempre debe atender a los requisitos de seguridad de la información que maneja.

• Desarrollar, operar y mantener el Servicio de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento. Definir la topología y servicio de Información estableciendo los criterios de uso y los servicios disponibles en el mismo. Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad. El responsable del servicio puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los responsables de la información afectada.

7.2.3 Responsable de la información

• Persona que tiene la potestad de establecer los requisitos de una información en materia de seguridad.

• El Responsable de la Información es el responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad. El ENS asigna al 'Responsable de la Información' la potestad de establecer los requisitos de la información en materia de seguridad. O, en terminología del ENS, la potestad de determinar los niveles de seguridad de la información.

• El Responsable de la Información puede ser una persona concreta o puede ser un órgano corporativo, que revestirá la forma de órgano colegiado de acuerdo

con la normativa administrativa. Aunque la aprobación formal de los niveles corresponda al Responsable de la Información, se puede recabar una propuesta al

Responsable de la Seguridad y conviene que se escuche la opinión del Responsable del Sistema. La determinación de los niveles de seguridad en cada dimensión de seguridad debe realizarse dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad. Se recomienda que los criterios de valoración estén respaldados por la Política de Seguridad en la medida en que sean sistemáticos, sin perjuicio de que puedan darse criterios particulares en casos singulares.

7.2.4 Responsable del sistema

• Persona que se encarga de la explotación del Sistema de Información.

• El ENS asigna al 'Responsable del Sistema' la potestad de establecer los requisitos del sistema en materia de seguridad.

• Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento. Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo. Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

• El Responsable del Sistema puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los responsables de la información afectada.

7.2.5 Responsable de protección de datos

• Persona que tiene la potestad y autoridad de establecer los requisitos del servicio en materia de protección de datos.

• Establecer las pautas para el cumplimiento de la protección de datos en base a lo establecido en la LOPD-GDD 3/2018 de 5 de diciembre, y en el 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).

7.2.6 Administrador de sistemas

Es responsable de la explotación diaria de los sistemas informáticos, aplicando la seguridad operativa, controlando el acceso a los recursos y garantizando el correcto funcionamiento y el cumplimiento de las políticas de seguridad establecidas por la Institución.

• Explotación y Mantenimiento o Supervisión operativa: Monitorización constante del estado de los servidores, redes y servicios para asegurar su disponibilidad.

- Gestión de incidencias: Ejecutar acciones diarias de operación y resolver problemas técnicos o incidentes reportados.
- Actualización y parches: Mantener el hardware, software y sistemas operativos al día para mitigar vulnerabilidades.

• Implementación de la Seguridad o Gestión de accesos y privilegios: Controlar quién accede a la información y recursos. Aplicar estrictamente el principio de mínimo privilegio (el usuario solo tiene los permisos imprescindibles).

- Aplicación de salvaguardas: Desarrollar de forma práctica las medidas de seguridad organizadas por el Responsable de Seguridad.
- Intervención rápida: Suspender servicios o accesos de inmediato si detecta deficiencias graves o riesgos críticos que puedan ser explotados por terceros.

• Copias de seguridad (Backups): Gestionar y verificar la correcta ejecución de los backups periódicos y asegurar la capacidad de recuperación ante desastres.

• Protección de instalaciones: Garantizar que la infraestructura física y lógica resida en áreas controladas y seguras.

7.2.7 Administrador de seguridad

Es la figura encargada de implementar, operar y mantener diariamente las medidas de seguridad del sistema. Su objetivo es ejecutar los controles técnicos y asegurar que no existan vulnerabilidades que comprometan la información.

• Implementación técnica: Desplegar y mantener operativas las herramientas, políticas y medidas de seguridad dispuestas en el sistema de información.

• Vigilancia y respuesta: Asegurar el cumplimiento estricto de los controles y detener servicios de inmediato si se detectan deficiencias graves o brechas explotables por terceros.

• Reporte de incidencias: Informar al Responsable de Seguridad y al CSI sobre cualquier anomalía o vulnerabilidad detectada.

• Asesoramiento: Apoyar a los responsables de la institución en la clasificación de los sistemas y la evaluación continua de riesgos.