1. INTRODUCCION

La información es uno de los principales activos de **CÁRITAS ESPAÑOLA** 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 **CÁRITAS ESPAÑOLA**.

La política de seguridad describe las directrices globales de seguridad de la información de **CÁRITAS ESPAÑOLA** definidas por sus órganos de gobierno y, en particular de la Secretaria General, así como los criterios para proteger los activos de información. **CÁRITAS ESPAÑOLA**, tiene como valores la centralidad de la persona, la persona como centro de la acción de Cáritas y la defensa de su dignidad, y la transparencia, como apertura de la información a todos los interesados en la labor de Cáritas. 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 **CÁRITAS ESPAÑOLA** 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, los órganos de gobierno de **CÁRITAS ESPAÑOLA** establecen 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

CÁRITAS ESPAÑOLA 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, **CÁRITAS ESPAÑOLA** 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

CÁRITAS ESPAÑOLA: 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, **CÁRITAS ESPAÑOLA** ha desarrollado planes de contingencia de sistemas TIC como parte de su plan general de continuidad del servicio y actividades de recuperación.

2. 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 **CÁRITAS ESPAÑOLA**.
- 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 **CÁRITAS ESPAÑOLA**.

- Garantizar la continuidad de los servicios frente a incidentes.

3. COMPROMISOS PARA LA SEGURIDAD DE LA INFORMACION

CÁRITAS ESPAÑOLA, 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. **CÁRITAS ESPAÑOLA** 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. **CÁRITAS ESPAÑOLA** 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 Cáritas Española puestos a disposición de sus agentes.

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

d. **CÁRITAS ESPAÑOLA** 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.

4. ALCANCE

4.1. Agentes

La Seguridad de la Información requiere la implicación y participación de todos los miembros de la organización, esto es, todos los trabajadores, voluntarios, becarios y colaboradores que trabajan en **CÁRITAS ESPAÑOLA**. 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.

4.2. 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 **CÁRITAS ESPAÑOLA**.

4.3. 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 **CÁRITAS ESPAÑOLA**. 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 **CÁRITAS ESPAÑOLA** y así se definirá contractualmente.

5. 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.

6. ORGANIZACIÓN DE LA SEGURIDAD

6.1. Comité de Seguridad de la Información y Protección de Datos

El Comité de Seguridad de la Información y Protección de Datos (en adelante CSIPD) se ha constituido a fecha de 21 de abril de 2026, estando formado por los siguientes integrantes:

- Secretaria general
- Responsable de Seguridad
- Responsable de la Información
- Responsable de Servicio
- Responsable de Sistemas
- Delegada de Protección de Datos
- Responsable de MIS
- Responsable de Desarrollo de Personas
- Consultor de seguridad

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 Cáritas 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 Cáritas 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 Cáritas. 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.

6.2. Roles: funciones y responsabilidades

Secretaria general

- Realizar el seguimiento de los acuerdos y planes de acción aprobados por el CSIPD, informando periódicamente sobre su estado de ejecución.
- Apoyar al Responsable de Seguridad en la preparación de informes, revisiones del sistema de gestión de seguridad de la información y documentación requerida según 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.
- Proporcionar los recursos necesarios para el cumplimiento del SGSI.

Responsable de Seguridad

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, según lo establecido en la Política de Seguridad de la Información de la organización.
- Coordinar la organización y convocatoria de las reuniones del CSIPD de la información y protección de datos, estableciendo el orden del día.
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.
- Aprobar la declaración de aplicabilidad.
- Canalizar y supervisar, tanto el cumplimiento de los requisitos de seguridad del servicio que se presta o solución que provee, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio.

Responsable de la Información

- Responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.
- Responsable último de cualquier error o negligencia que conlleve un incidente de confidencialidad o de integridad (en materia de protección de datos) y de disponibilidad (en materia de seguridad de la información).
- Establecer los requisitos de la información en materia de seguridad.
- Determinar y aprobar los niveles de seguridad de la información.
- Aprobar la categorización del sistema con respecto a la información.

Responsable del Servicio

- Establecer los requisitos del servicio en materia de seguridad.
- Determinar los niveles de seguridad de los servicios.
- Aprobar la categorización del sistema con respecto a los servicios.

Responsable del Sistema

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad.
- Potestad para proponer la suspensión del tratamiento de una cierta información o la prestación de un determinado servicio si aprecia deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.

Delegada de Protección de Datos

- Coordinar todos los aspectos relacionados con la adecuación de las actuaciones de **CÁRITAS ESPAÑOLA** en materia de protección de datos de carácter personal.
- Coordinar, junto con el responsable de Seguridad, el cumplimiento de ISO/IEC 27001:2022 y el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad con respecto a la protección de datos de carácter personal.

Responsable de Desarrollo de Personas

- Colaboración con los requisitos establecidos al departamento de personas exigido por ISO/IEC 27001:2022 y el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad con respecto a la protección de datos de carácter personal.
- Coordinación relativa a los datos de carácter personal de los agentes de **CÁRITAS ESPAÑOLA**

Responsable de MIS (Módulo de Intervención Social)

- Colaboración con los aspectos relacionados con el módulo de intervención social necesarios para cumplir con ISO/IEC 27001:2022 y el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad con respecto a la protección de datos de carácter personal

Consultor de seguridad

- Apoyo 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.

6.3. **Designación y renovación**

El Responsable de Seguridad será nombrado por la Secretaria General y se revisará cada 2 años o cuando el puesto quede vacante. El resto de cargos indicados en el apartado anterior será designado por el CSIPD.

7. Estructuración de la documentación

La documentación relativa a seguridad de la información se clasifica en función de su contenido:

- Políticas: documentos de alto nivel que establecen los principios, compromisos y directrices generales de la organización en materia de seguridad de la información.
- Normas: conjunto de reglas y disposiciones de obligado cumplimiento que desarrollan las políticas de seguridad y establecen los requisitos y controles que deben aplicarse en la organización para garantizar la protección de la información y de los sistemas.
- Procedimientos: documentos que describen de forma detallada las actividades, responsabilidades y pasos a seguir para ejecutar determinados procesos relacionados

con la seguridad de la información, asegurando que se realizan de manera uniforme y controlada.

- Manuales: documentación que proporciona instrucciones prácticas y guías de uso para la correcta aplicación de políticas, normas o procedimientos, facilitando su comprensión y aplicación por parte de los usuarios o personal técnico.
- Registros: evidencias documentales que demuestran la ejecución de actividades, controles o procesos relacionados con la seguridad de la información. Permiten acreditar el cumplimiento de las políticas, normas y procedimientos establecido.

La documentación relativa a seguridad de la información se clasifica en función de su acceso en:

- Secreto: usuario gestiona la información secreta recibida sólo en la medida en que sea necesaria para el desempeño de su cargo y de sus funciones en **CÁRITAS ESPAÑOLA**.
- Confidencial: solo pueden acceder usuarios autorizados.
- Interna: solo pueden acceder usuarios de **CÁRITAS ESPAÑOLA**
- Pública: pueden acceder usuarios ajenos a **CÁRITAS ESPAÑOLA**

8. RESPONSABILIDADES

Cualquier incumplimiento de las políticas y normas de seguridad que suponga un potencial daño, consumado o no a **CÁRITAS ESPAÑOLA**, podría ser sancionada según los mecanismos habilitados en las normativas legal, contractual y corporativa vigentes.

Todas las acciones en las que se comprometa la seguridad de **CÁRITAS ESPAÑOLA** y que no estén previstas en esta política, deberán ser revisadas por los órganos de Dirección y por el Responsable de Seguridad.

8.1. Agentes usuarios de sistemas de la información

Los agentes deben conocer, entender y aplicar las Políticas de Seguridad, procedimientos, estándares y la legislación vigente. En general, cualquier persona que genera información es responsable de su clasificación de acuerdo con el Manual de Seguridad que se apruebe. Asimismo, cualquier agente que utiliza información y los sistemas de información está obligada a gestionarlos con el cuidado necesario, así como a utilizarlos únicamente para realizar las tareas autorizadas y en cumplimiento de las normativas válidas. Esto también es aplicable al personal externo subcontratado si fuera el caso.

8.2. Propietario de los activos de información

CÁRITAS ESPAÑOLA es generalmente el propietario de los activos de Información. Los responsables establecidos en la Política de Adquisición de bienes y servicios deberán adquirir, desarrollar y mantener las aplicaciones informáticas de **CÁRITAS ESPAÑOLA** teniendo en cuenta esta Política de Seguridad de la Información. Estas aplicaciones

deberán servir como sistemas de Soporte a las decisiones y a otras actividades de la organización.

CÁRITAS ESPAÑOLA indicará la clasificación de sus activos que mejor corresponde con su valor crítico, disponibilidad e importancia relativa para la organización. Su clasificación marcará el nivel de riesgo y de protección, así como el nivel de acceso a dicha información o aplicación informática.

8.3. Equipo de Gestión de la Información

Los trabajadores y voluntarios del Equipo de Gestión de la Información son los encargados de salvaguardar tanto la Información de la propia organización como la cedida por terceros.

El Responsable de Seguridad de la Información es el responsable de establecer y mantener las Políticas, Manuales y Procedimientos de Seguridad de la Información de **CÁRITAS ESPAÑOLA,** informando periódicamente a la Dirección de Área correspondiente y a los órganos de gobierno de **CÁRITAS ESPAÑOLA**.

El Sistema de Información contempla disponer de un Administrador autorizado para cada Activo, siendo reconocido como el responsable del mismo. Los miembros del Equipo de Gestión de la Información son los responsables de almacenar la Información, implementar controles de acceso (para prevenir accesos no autorizados) y ejecutar copias de seguridad periódicas (para asegurar la disponibilidad de la información crítica).

Deben asimismo desarrollar, aplicar, mantener y revisar las medidas de seguridad definidas por **CÁRITAS ESPAÑOLA** en el Manual de Seguridad.

9. DIFUSIÓN Y APROBACIÓN DE LA POLÍTICA

La presente Política de Seguridad de la información será accesible a todos los agentes, se entregará a la incorporación de cada nuevo agente y cada vez que sufra una revisión de importancia se tendrá disponible un ejemplar en la INTRANET de **CÁRITAS ESPAÑOLA** o bien se difundirá por correo electrónico o cualquier otro medio a todos los agentes internos y externos subcontratados por **CÁRITAS ESPAÑOLA** que manejen datos y recursos pertenecientes a la entidad para el conocimiento y conciencia de las normas de seguridad dispuestas.

Asimismo, se obtendrá compromiso de la lectura y aceptación de la misma por parte de todos los agentes. Esta política forma parte del "*Manual de Seguridad del Agente*".

Los órganos de gobierno de **CÁRITAS ESPAÑOLA** y, en particular, la Secretaria General es la responsable de la aprobación y publicación de la Política, su difusión a todos los agentes y terceros afectados.

Con carácter general **CÁRITAS ESPAÑOLA** se dotará de procedimientos que permitan la aplicación de estos principios en su gestión habitual, generando los mecanismos de verificación necesarios.

Para conseguir que estos compromisos sean aplicables es necesaria la implicación de las personas que trabajan en Caritas en la búsqueda y aplicación de soluciones que prevengan del uso inadecuado de los activos de la información, por ello animo a todos los que formamos **CÁRITAS ESPAÑOLA** y a nuestros colaboradores, a comprometernos con el cumplimiento y difusión de esta política como contribución para que la acción de Cáritas sea en todo momento coherente con sus valores.

Aprobado:
Secretaria General María González Dyne