FPC

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Fundación Plaza Castilla
CIF: G84070945 | Constituida: 02/11/2004 | Registro: 732
Ferraz 22, Madrid | Tel: (+34) 652 63 40 40

1. INTRODUCCIÓN Y ALCANCE

1.1 Propósito

La presente Política de Seguridad de la Información establece el marco normativo y las directrices necesarias para garantizar la protección, confidencialidad, integridad y disponibilidad de toda la información gestionada por la Fundación Plaza Castilla en el desarrollo de su misión de combatir el sin hogarismo y proteger la infancia.

1.2 Alcance

Esta política aplica a:

- Todos los empleados, voluntarios, colaboradores y terceros que accedan a los sistemas de información de la Fundación
- Toda la información procesada, almacenada o transmitida por la organización
- Todos los sistemas de información, infraestructura tecnológica y equipos utilizados
- Los procesos y procedimientos relacionados con el tratamiento de datos de beneficiarios vulnerables

Consideración Especial

Dada la naturaleza de nuestra misión, esta política presta especial atención a la protección de datos de menores y personas en situación de vulnerabilidad social, estableciendo medidas reforzadas de seguridad y privacidad.

2. MARCO NORMATIVO APLICABLE

2.1 Normativa Principal

- **Reglamento General de Protección de Datos (RGPD)** - Reglamento (UE) 2016/679
- **Ley Orgánica 3/2018** de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)
- **Ley Orgánica 1/1996** de Protección Jurídica del Menor
- **Ley 50/2002** de Fundaciones
- **Real Decreto 3/2010** Esquema Nacional de Seguridad

2.2 Normativa Específica del Tercer Sector

- Guía de la Agencia Española de Protección de Datos para entidades del Tercer Sector
- Recomendaciones específicas para el tratamiento de datos de colectivos vulnerables
- Protocolos de protección infantil en organizaciones sociales

3. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

3.1 Principios Fundamentales

1. **Confidencialidad:** La información solo debe ser accesible a personas autorizadas
2. **Integridad:** Mantenimiento de la exactitud y completitud de la información
3. **Disponibilidad:** Acceso a la información cuando sea necesario

4. **Trazabilidad:** Capacidad de seguir el rastro de las acciones realizadas
5. **Autenticidad:** Verificación de la identidad de usuarios y origen de datos
6. **No repudio:** Garantía de que las acciones no puedan ser negadas

3.2 Principios Específicos para Colectivos Vulnerables

- **Protección Reforzada:** Medidas adicionales para datos de menores y personas vulnerables
- **Consentimiento Informado:** Explicación clara y comprensible de los tratamientos
- **Minimización de Datos:** Recopilación solo de información estrictamente necesaria
- **Anonimización:** Técnicas para proteger la identidad cuando sea posible

4. CLASIFICACIÓN DE LA INFORMACIÓN

Nivel	Descripción	Ejemplos	Medidas de Protección
CRÍTICA	Datos de menores, historiales clínicos, situaciones de riesgo	Expedientes de protección infantil, datos médicos, ubicaciones de refugio	Cifrado AES-256, acceso restringido, auditoría completa
CONFIDENCIAL	Datos personales de beneficiarios adultos	Información socioeconómica, documentos de identidad	Cifrado, control de acceso, registro de actividad
INTERNA	Información operacional de la fundación	Procedimientos internos, comunicaciones staff	Control de acceso por roles, backup seguro
PÚBLICA	Información destinada a divulgación	Memorias, noticias, información corporativa	Revisión antes de publicación

5. MEDIDAS DE PROTECCIÓN ESPECIALES PARA DATOS SENSIBLES

5.1 Protección de Datos de Menores

Protocolo Especial - Protección Infantil

- Consentimiento de tutores legales obligatorio
- Acceso limitado solo a personal autorizado y formado
- Cifrado de extremo a extremo para toda comunicación
- Pseudonimización obligatoria en reportes estadísticos
- Eliminación segura al alcanzar mayoría de edad (salvo consentimiento expreso)

5.2 Datos de Personas Sin Hogar

- **Ubicaciones de refugio:** Clasificación crítica, acceso ultra restringido
- **Historiales sociales:** Compartimentación por equipos de trabajo
- **Documentación:** Custodia segura de documentos físicos y digitales
- **Contactos familiares:** Protección especial para evitar localización no deseada

5.3 Medidas Técnicas Reforzadas

1. **Cifrado Avanzado:** AES-256 para datos en reposo y en tránsito
2. **Autenticación Multifactor:** Obligatoria para acceso a datos críticos
3. **Segregación de Red:** Redes separadas para datos de diferente clasificación
4. **Monitorización 24/7:** Sistemas de detección de intrusiones

6. CONTROLES DE ACCESO Y AUTENTICACIÓN

6.1 Gestión de Identidades

- **Principio de Menor Privilegio:** Acceso mínimo necesario para desempeñar funciones
- **Segregación de Funciones:** Separación clara entre roles operativos y administrativos

- **Revisión Periódica:** Auditoría trimestral de permisos y accesos
- **Proceso de Alta/Baja:** Procedimientos formales para gestión de usuarios

6.2 Niveles de Acceso por Perfil

Perfil	Nivel de Acceso	Datos Autorizados	Restricciones
Dirección	Nivel 4 - Completo	Todos los datos	Auditoría completa de accesos
Trabajador Social	Nivel 3 - Especializado	Casos asignados + datos agregados	Solo casos bajo su responsabilidad
Personal Administrativo	Nivel 2 - Limitado	Datos administrativos y contacto	Sin acceso a historiales sociales
Voluntarios	Nivel 1 - Básico	Información general no personal	Supervisión continua requerida

7. GESTIÓN DE INCIDENTES DE SEGURIDAD

7.1 Clasificación de Incidentes

Niveles de Gravedad

- **CRÍTICO:** Exposición de datos de menores o ubicaciones de refugio
- **ALTO:** Acceso no autorizado a datos personales de beneficiarios
- **MEDIO:** Fallos de sistema que afecten disponibilidad de servicios
- **BAJO:** Incidentes menores sin impacto en datos personales

7.2 Procedimiento de Respuesta

1. **Detección y Notificación (0-2 horas)**
   - Identificación inmediata del incidente
   - Notificación al Responsable de Seguridad

- Activación del equipo de respuesta

2. **Contención y Evaluación (2-6 horas)**
   - Aislamiento del sistema afectado
   - Evaluación del impacto y alcance
   - Preservación de evidencias

3. **Notificación Externa (24-72 horas)**
   - Notificación a la AEPD si procede
   - Comunicación a afectados según RGPD
   - Coordinación con autoridades competentes

4. **Recuperación y Seguimiento**
   - Restauración segura de servicios
   - Implementación de mejoras
   - Documentación de lecciones aprendidas

8. CONTINUIDAD DEL NEGOCIO Y BACKUP

8.1 Estrategia de Backup

- **Frecuencia:** Backup diario de datos críticos, semanal de datos operacionales
- **Ubicación:** Copias en ubicaciones geográficamente separadas
- **Cifrado:** Todas las copias cifradas con AES-256
- **Pruebas:** Verificación mensual de integridad y restauración

8.2 Plan de Continuidad

Tiempos Objetivo de Recuperación (RTO)

- **Servicios Críticos (protección infantil):** 2 horas
- **Servicios Esenciales (atención directa):** 8 horas
- **Servicios Administrativos:** 24 horas

9. FORMACIÓN Y CONCIENCIACIÓN

9.1 Programa de Formación Obligatoria

- **Personal Nuevo:** Formación en seguridad durante los primeros 15 días
- **Todo el Personal:** Actualización anual en protección de datos y seguridad
- **Personal con Acceso Crítico:** Formación semestral especializada
- **Voluntarios:** Sesión específica sobre manejo confidencial de información

9.2 Contenidos Específicos

1. Normativa RGPD aplicable al tercer sector
2. Protección especial de datos de menores
3. Manejo ético de información de personas vulnerables
4. Procedimientos de seguridad informática
5. Protocolo de respuesta ante incidentes
6. Técnicas de ingeniería social y phishing

10. SUPERVISIÓN Y AUDITORÍA

10.1 Monitorización Continua

- **Sistemas Automatizados:** Alertas en tiempo real para actividades sospechosas
- **Revisión de Logs:** Análisis diario de registros de acceso
- **Métricas de Seguridad:** Dashboard con KPIs de seguridad actualizados

10.2 Auditorías Periódicas

Tipo de Auditoría	Frecuencia	Alcance	Responsable
Auditoría Interna	Trimestral	Cumplimiento de procedimientos	Responsable de Seguridad

Tipo de Auditoría	Frecuencia	Alcance	Responsable
Auditoría Externa	Anual	Evaluación integral RGPD	Consultoría Externa
Pentesting	Semestral	Vulnerabilidades técnicas	Empresa Especializada
Revisión de Accesos	Mensual	Permisos y privilegios	IT + RRHH

11. REVISIÓN Y ACTUALIZACIÓN

11.1 Proceso de Revisión

Esta política será revisada y actualizada según las siguientes circunstancias:

- **Revisión Ordinaria:** Cada 12 meses como mínimo
- **Cambios Normativos:** Actualización inmediata ante nueva legislación
- **Incidentes Graves:** Revisión tras cualquier brecha de seguridad crítica
- **Cambios Organizacionales:** Adaptación a nuevos servicios o estructuras

11.2 Aprobación y Comunicación

Todas las actualizaciones deberán ser aprobadas por la Dirección de la Fundación y comunicadas a todo el personal en un plazo máximo de 15 días desde su aprobación.

> Compromiso de la Dirección
>
> La Dirección de la Fundación Plaza Castilla se compromete a proporcionar los recursos necesarios para la implementación efectiva de esta política y a liderar con el ejemplo en el cumplimiento de las medidas de seguridad establecidas, priorizando siempre la protección y dignidad de las personas a las que servimos.

Fecha de Aprobación: Enero 2025

Fecha de Próxima Revisión: Enero 2026

Versión: 1.0

Fernando Rodríguez Duplá
Presidente
DNI: 00822622G
Fundación Plaza Castilla

Daniel González García
Director
DNI: 52887209C
Fundación Plaza Castilla