GESTIÓN DE RIESGOS PARA EL TRATAMIENTO DE DATOS PERSONALES SENSIBLES EN EL MOVIMIENTO DE MUJERES DE EL ORO

RISK MANAGEMENT FOR THE PROCESSING OF SENSITIVE PERSONAL DATA IN THE WOMEN'S MOVEMENT OF EL ORO

Darwin Daniel Chávez Vega [1*]

[1] Carrera de Tecnologías de la Información, Facultad de Ingeniería Civil, Universidad Técnica de Machala. Ecuador. ORCID: https://orcid.org/0009-0007-2714-5831. Correo: dchavez7@utmachala.edu.ec

Kevin Anthony Burgos Ramírez [2]

[2] Carrera de Tecnologías de la Información, Facultad de Ingeniería Civil, Universidad Técnica de Machala. Ecuador. ORCID: https://orcid.org/0009-0008-0832-4364. Correo: kburgos2@utmachala.edu.ec

Nancy Magaly Loja Mora [3]

[3] Carrera en Tecnologías de la Información, Facultad de Ingeniería Civil, Universidad Técnica de Machala. Ecuador. ORCID: https://orcid.org/0000-0002-5583-4278. Correo: nmloja@utmachala.edu.ec

Harold Patricio Loján Alvarado [4]

[4] Carrera de Derecho, Facultad de Ciencias Sociales, Universidad Técnica de Machala. Ecuador. ORCID: https://orcid.org/0009-0008-6869-261X. Correo: hlojan@utmachala.edu.ec

*** Autor para correspondencia: dchavez7@utmachala.edu.ec**

Resumen

El presente estudio examinó los riesgos relacionados con el manejo de datos personales en el Movimiento de Mujeres de El Oro (MMO), organización que gestiona información sensible sobre mujeres en situación de violencia de género. El objetivo fue proponer controles de seguridad conforme a la norma ISO 27001:2022 y la Ley Orgánica de Protección de Datos Personales de Ecuador (LOPDP). La metodología incluyó la identificación y evaluación de actividades, la priorización de amenazas y la evaluación de vulnerabilidades mediante una escala de valores desarrollada por el Comité de Seguridad de Datos del MMO. Los controles de seguridad se establecieron con base en los principios de: confidencialidad, integridad y disponibilidad. Los resultados mostraron que existe un riesgo crítico asociado con los datos de identificación: Sociales, Legales

y Psicológicos, por lo que se recomendaron medidas como el cifrado, la restricción de acceso y auditorías continuas. Se concluye que una adecuada integración entre la normativa vigente y los controles técnicos propuestos fortalece la protección de los datos personales, reduce los niveles de riesgo y mejora la gobernanza de la información en organizaciones que gestionan datos sensibles.

Palabras clave: Protección de datos personales; gestión de riesgos; Ley Orgánica de Protección de Datos Personales de Ecuador; ISO/IEC 27001:2022; Seguridad de la información

Abstract

This study examined the risks associated with the handling of personal data within the Women's Movement of El Oro (MMO), an organization that manages sensitive information about women affected by gender-based violence. The objective was to propose security controls aligned with the ISO/IEC 27001:2022 standard and Ecuador's Organic Law on Personal Data Protection (OLPDP). The methodology involved identifying and assessing data processing activities, prioritizing threats, and evaluating vulnerabilities using a value scale developed by the MMO's Data Security Committee. Security controls were defined based on the principles of confidentiality, integrity, and availability. The findings revealed a critical level of risk associated with the processing of identification data—specifically, Social, Legal, and psychological categories—prompting the recommendation of measures such as data encryption, access restriction, and ongoing audits. The study concludes that effective integration of regulatory frameworks with proposed technical controls strengthens the protection of personal data, reduces risk levels, and improves information governance in organizations that handle sensitive data.

Keywords: *Personal data protection; risk management; Ecuadorian Organic Law on Personal Data Protection; ISO/IEC 27001:2022; Information Security*

Fecha de recibido: 09/02/2025
Fecha de aceptado: 17/04/2025
Fecha de publicado: 26/04/2025

Introducción

Dentro del marco de la transformación digital, la administración y protección de la información personal se ha convertido en una preocupación a escala mundial. Las entidades, ya sean públicas o privadas, se enfrentan a amenazas potenciales como vacíos de seguridad, accesos no autorizados y manejo inapropiado de datos delicados (Alvear et al., 2024; Durán-Ramírez & Zamora-Vázquez, 2023; P. Romansky et al., 2020). Estas dificultades han impulsado a la adopción de normas internacionales como la ISO/IEC 27001:2022, la cual ofrece un esquema estructurado para la administración de riesgos y la implementación de controles de seguridad, promoviendo la confianza de los usuarios en los sistemas de información (Benussi Díaz, 2020; López et al., 2023; Xiong et al., 2024)

Investigaciones recientes han abordado la necesidad de fortalecer los sistemas de protección de datos, especialmente en regiones como Ecuador, donde la promulgación de la Ley Orgánica de Protección de Datos Personales (LOPDP) en 2021 representa un avance normativo significativo. Sin embargo, su aplicación práctica continúa siendo limitada, exponiendo a numerosas instituciones a riesgos críticos (Alvear Richards & Hernández Pesantes, 2023; Gutiérrez Meneses, 2024). Estudios en sectores como el financiero y tecnológico han demostrado que la ausencia de un enfoque sistemático de gestión de riesgos incrementa la probabilidad de incidentes de seguridad (Fuentes Pozo, 2023; Morales Hidalgo, 2024; Rodríguez et al., 2023).

A pesar de estos avances, existe un vacío con respecto a la implementación de Sistemas de Gestión de Seguridad de la Información (SGSI) en organizaciones sociales que manejan información de alta sensibilidad. Tal es el caso del Movimiento de Mujeres de El Oro (MMO), entidad que administra datos personales, socioeconómicos, psicológicos y legales de mujeres en situación de violencia de género. La carencia de un SGSI basado en ISO/IEC 27001 en esta organización implica un alto nivel de exposición a riesgos como accesos indebidos, alteraciones de la información o su divulgación no autorizada (Hornuf et al., 2023; Novoa, 2020; Perugachi Cartagena, 2021; Wiemas N. G. & Suroso, 2024).

A partir de esta problemática, surge la interrogante: ¿cómo puede la aplicación efectiva de la Ley Orgánica de Protección de Datos Personales en Ecuador (LOPDP) fortalecer la seguridad de los datos personales en una organización social como el Movimiento de Mujeres de El Oro (MMO)?

En este sentido, el objetivo del presente estudio es analizar los riesgos asociados al tratamiento de datos personales en el MMO, tomando como eje central los principios, obligaciones y medidas establecidas por la LOPDP. Como soporte metodológico, se empleará la norma ISO/IEC 27001:2022 para estructurar la identificación de amenazas, vulnerabilidades y controles, en función de asegurar el cumplimiento normativo. El enfoque adoptado es exploratorio, con sustento documental y empírico, lo que permitirá comprender el nivel de exposición actual de la organización y proponer un conjunto de medidas que aseguren la confidencialidad, integridad y disponibilidad de los datos, en coherencia con la legislación ecuatoriana vigente.

Materiales y métodos

El presente estudio se fundamenta en el cumplimiento de la Ley Orgánica de Protección de Datos Personales del Ecuador (LOPDP), la cual establece principios, obligaciones y medidas de seguridad aplicables al tratamiento de datos personales. Esta normativa constituye el eje central del análisis de riesgos desarrollado en el Movimiento de Mujeres de El Oro (MMO), organización que gestiona información altamente sensible de mujeres en situación de vulnerabilidad. Para complementar el enfoque legal, se adoptó la norma ISO/IEC 27001:2022 como marco técnico de referencia para la identificación de activos, evaluación de amenazas, análisis de vulnerabilidades y definición de controles de seguridad. La metodología aplicada está representada en la Figura 1, que esquematiza el proceso utilizado por el Comité de Seguridad del MMO para evaluar los riesgos y establecer medidas de mitigación conforme a la normativa vigente.

En la evaluación de riesgos, se siguen varias etapas. Primero, la tasación de activos permite determinar el valor de cada tipo de dato con base en su nivel de confidencialidad, integridad y disponibilidad. Luego, la evaluación de amenazas y vulnerabilidades identifica eventos que pueden afectar la seguridad de la

información, como accesos no autorizados, fallos en el almacenamiento y deficiencias en los controles actuales (Orellana Toledo, 2022).

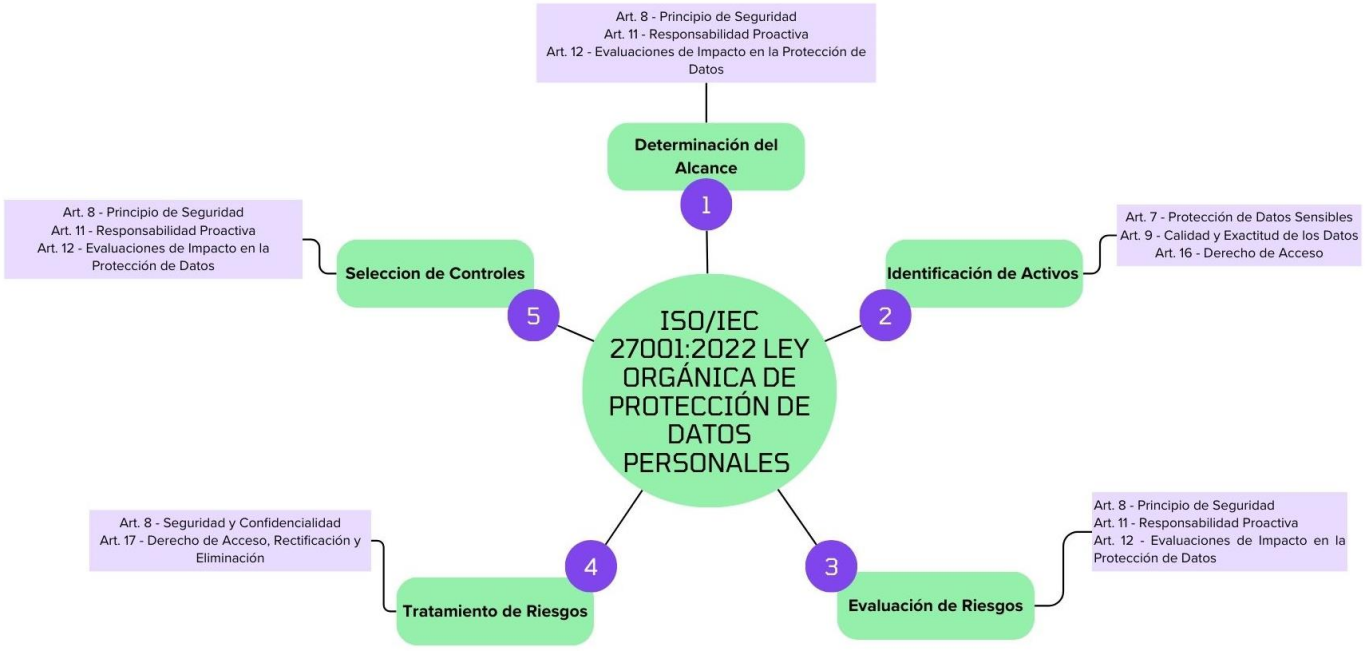

Figura 1. Metodología aplicada para el análisis de riesgos en el MMO
Fuente: Elaboración propia basado en la Ley de Protección de datos Personales en Ecuador & ISO/IEC 27001:2022

Determinación del alcance

Este estudio se enfoca en el análisis de riesgos del tratamiento de datos personales en el Movimiento de Mujeres de El Oro (MMO), aplicando la ISO/IEC 27001:2022. Aunque la organización maneja otros activos como infraestructura tecnológica, redes y documentación física, el Comité de Seguridad del MMO ha identificado los datos personales como el activo más crítico debido a su impacto en la seguridad y privacidad de las usuarias.

La filtración, alteración o pérdida de esta información podría exponer a las víctimas a riesgos significativos, afectando su protección y acceso a servicios legales y psicológicos. Además, la Ley Orgánica de Protección de Datos Personales (LOPDP) exige medidas de seguridad específicas para estos datos.

El alcance de este análisis se limita a identificar amenazas, evaluar vulnerabilidades y proponer controles alineados con la LOPDP e ISO 27001:2022. Esta propuesta servirá como base para futuras estrategias de seguridad dentro del MMO.

Identificación de procesos del MMO

La Tabla 1 presenta los principales procesos en los que se manejan datos personales sensibles durante la atención a víctimas, identificando los tipos de información tratados y la normativa que los respalda conforme

a la LOPDP. Esta organización permite evidenciar la importancia de proteger adecuadamente dicha información en contextos de alta vulnerabilidad.

Tabla 1 Identificación de procesos del MMO

Proceso	Descripción	Datos Tratados	Normativa Aplicable (LOPDP)
Registro de víctima	Captura de datos personales y consentimiento informado.	- Datos de identificación (nombre, cédula, contacto, dirección) - Datos de terceros (agresor, contactos de confianza) - Consentimiento informado.	Art. 7 - Datos Sensibles; Art. 8 - Seguridad y Confidencialidad; Art. 16 - Derecho de Acceso; Art. 12 - Evaluaciones de Impacto
Evaluación socioeconómica	Análisis de información económica y social de la usuaria.	- Datos socioeconómicos (ingresos, empleo, estado civil) - Datos de vivienda y nivel de riesgo social	Art. 7 - Protección de Datos Sensibles; Art. 9 - Calidad y Exactitud de los Datos; Art. 12 - Evaluaciones de Impacto; Art. 16 - Derecho de Acceso
Evaluaciones psicológicas y seguimiento	Evaluación del estado emocional y monitoreo de la usuaria.	- Datos psicológicos (diagnósticos, informes de terapias) - Datos de salud mental	Art. 7 - Protección de Datos Sensibles; Art. 8 - Seguridad y Confidencialidad; Art. 11 - Responsabilidad Proactiva; Art. 16 - Derecho de Acceso y Rectificación
Asesoramiento y gestión legal	Apoyo legal a la usuaria en procesos judiciales y medidas de protección.	- Datos legales (denuncias, medidas de protección, procesos judiciales) - Información de seguimiento del caso	Art. 7 - Datos Sensibles; Art. 8 - Seguridad y Confidencialidad; Art. 12 - Evaluaciones de Impacto; Art. 17 - Derecho de Acceso, Rectificación y Eliminación
Archivo y retención de información	Almacenamiento seguro y eliminación de datos según el marco legal.	- Expedientes físicos y digitales - Historiales de atención de la usuaria	Art. 8 - Seguridad y Confidencialidad; Art. 11 - Responsabilidad Proactiva; Art. 17 - Derecho de Acceso, Rectificación y Eliminación

Fuente: Elaboración propia basado en la Ley de Protección de datos Personales en Ecuador & ISO/IEC 27001:2022

Identificación de activos

La identificación de activos en este estudio se basa exclusivamente en los datos personales sensibles, siguiendo las directrices de ISO 27001:2022 y la Ley Orgánica de Protección de Datos Personales (LOPDP) de Ecuador, se ha categorizado la información de acuerdo con su función, nivel de sensibilidad y área responsable, asegurando un enfoque estructurado para la gestión de riesgos.

Identificación de activos de información por proceso

Proceso: Registro de víctima

Tabla 2 Identificación de activos: Registro de victima

Categoría de Dato	Datos Identificados (Activos)	Área Responsable
Datos de Identificación	Nombre completo, cédula de identidad, fecha de nacimiento, dirección de residencia, número de contacto.	Coordinación General, Área Social.
Datos de Terceros	Información del agresor (si es reportado), datos de contacto de familiares o personas de confianza.	Área Social.
Consentimiento Informado	Documentos físicos y digitales con autorización de uso de datos.	Coordinación y Área Administrativa.

Fuente: Elaboración propia

Proceso: Evaluación Socioeconómica

Tabla 3 Identificación de Activos Evaluación Socioeconómica

Categoría del dato	Datos Identificados (Activos)	Área Responsable
Datos Socioeconómicos	Nivel de escolaridad, ocupación y situación laboral, ingresos económicos, condiciones de vivienda, número de dependientes.	Área Social.
Acceso a Programas Sociales	Beneficios gubernamentales y asistencia social recibida.	Área Social.
Antecedentes de Violencia Familiar	Historial de agresiones previas, denuncias registradas.	Área Social.

Fuente: Elaboración propia

Proceso: Evaluaciones Psicológicas y Seguimiento

Tabla 4 Identificación de Activos Evaluaciones Psicológicas y Seguimiento

Categoría de Dato	Datos Identificados (Activos)	Área Responsable
Evaluaciones Psicológicas	Diagnósticos clínicos, pruebas psicológicas, factores de riesgo psicosocial.	Área Psicológica.
Historial de Atención Psicológica	Fechas de sesiones, evolución del tratamiento, informes de intervención.	Área Psicológica.
Registro de Seguimiento	Notas de terapia, observaciones clínicas, interacciones con la usuaria.	Área Psicológica.

Fuente: Elaboración propia

Proceso: Asesoramiento y Gestión Legal

Tabla 5 Identificación de Activos Asesoramiento y Gestión Legal

Categoría de Dato	Datos Identificados (Activos)	Área Responsable
Datos Jurídicos	Denuncias presentadas, medidas de protección solicitadas y otorgadas.	Área Legal.
Estado de Procesos Legales	Expedientes en curso, resoluciones judiciales.	Área Legal.

Documentación de Casos Archivados	Registro de acciones legales pasadas.	Área Legal.

Fuente: Elaboración propia

Evaluación del Riesgo

Para clasificar los riesgos asociados al tratamiento de datos personales, se adoptó una escala de valoración diseñada por el Comité de Seguridad de Datos del MMO. Esta escala tiene en cuenta dos factores clave:

- Impacto: Nivel de daño que podría causar un incidente en la seguridad de los datos.
- Probabilidad: Posibilidad de que una amenaza explote una vulnerabilidad.

1	1.1	1.2	1.3	1.4	1.5	1.6	1.7	1.8	1.9	2	2.1	2.2	2.3	2.4	2.5	2.6	2.7	2.8	2.9	3
Bajo							**Medio**							**Alto**						

Tasación de activos

La tasación de activos constituye una etapa esencial en el análisis de riesgos, ya que permite determinar el valor de cada activo de información con base en su criticidad. Esta criticidad se evalúa a través de los principios de seguridad de la información: confidencialidad, integridad y disponibilidad. La fórmula utilizada para calcular el valor total del activo es la siguiente:

Valor del Activo = (Confidencialidad + Integridad + Disponibilidad) / 3

Cada uno de estos criterios se califica en una escala del 1 al 3, siendo 3 el nivel más alto de sensibilidad o necesidad de protección. El resultado es un promedio que refleja la importancia del activo dentro del sistema de tratamiento de datos. Esta calificación constituye la base para los cuadros de tasación de activos y priorización del riesgo, permitiendo una gestión objetiva y estandarizada de los niveles de exposición a amenazas.

Tasación de Activos Proceso: Registro de Víctima

Tabla 6 Tasación de activos Proceso de registro de victimas

Activo	Confidencialidad (C)	Integridad (I)	Disponibilidad (D)	Total
Datos de Identificación (Nombre, cedula, dirección, contacto)	3	3	2	**2.67**
Datos de Terceros (Información del agresor, contactos de confianza)	3	3	2	**2. 67**
Consentimiento Informado (Autorización de uso de datos)	3	3	3	**3.00**

Fuente: Elaboración propia

Tasación de Activos Evaluación Socioeconómica

Tabla 7 Tasación de Activos Evaluación Socioeconómica.

Activo	Confidencialidad (C)	Integridad (I)	Disponibilidad (D)	Total
Datos Socioeconómicos (Escolaridad, ocupación, ingresos, vivienda, dependientes)	3	3	2	**2.67**
Acceso a Programas Sociales (Beneficios y asistencia social recibida)	3	3	1	**2.33**
Antecedentes de Violencia Familiar (Historial de agresiones previas, denuncias)	3	3	3	**3.00**

Fuente: Elaboración propia

Tasación de Activos Evaluaciones Psicológicas y Seguimiento

Tabla 8 Tasación de Activos Evaluaciones Psicológicas y Seguimiento

Activo	Confidencialidad (C)	Integridad (I)	Disponibilidad (D)	Total
Evaluaciones Psicológicas (Diagnósticos clínicos, pruebas psicológicas, factores de riesgo psicosocial)	3	3	1	**2.33**
Historial de Atención Psicológica (Fechas de sesiones, evolución del tratamiento, informes de intervención)	3	3	2	**2.67**
Registro de Seguimiento (Notas de terapia, observaciones clínicas, interacciones con la usuaria)	3	3	3	**3.00**

Fuente: Elaboración propia

Tasación de Activos Asesoramiento y Gestión Legal

Tabla 9 Tasación de Activos Evaluaciones Psicológicas y Seguimiento

Activo	Confidencialidad (C)	Integridad (I)	Disponibilidad (D)	Total
Datos Jurídicos (Denuncias presentadas, medidas de protección solicitadas y otorgadas)	3	3	3	**3.00**
Estado de Procesos Legales (Expedientes en curso, resoluciones judiciales)	3	3	2	**2.67**
Documentación de Casos Archivados (Registro de acciones legales pasadas)	3	3	1	**2.33**

Evaluación de Amenazas – Evaluación de Vulnerabilidades – Determinación y Priorización del Riesgo

En esta sección se realiza la evaluación integral de amenazas, vulnerabilidades, controles actuales y la priorización del riesgo para los activos de información sensibles gestionados por el Movimiento de Mujeres de El Oro (MMO). El análisis se ha estructurado por proceso y se ha aplicado una metodología basada en los

principios de la norma ISO/IEC 27001:2022, incorporando una valoración cualitativa de los factores de riesgo. Para cada activo, se determinó la ocurrencia de la amenaza, la posibilidad de explotación de la vulnerabilidad y su valor asociado, permitiendo calcular un promedio final que establece el nivel de criticidad. Esta evaluación permite identificar los puntos críticos en el tratamiento de los datos personales y proporciona una base objetiva para el diseño de controles de seguridad específicos.

Proceso: Registro de Víctima

El proceso de registro de víctima constituye la fase inicial del tratamiento de datos dentro del MMO y, por tanto, presenta una alta concentración de información sensible. En esta etapa se gestionan datos personales, de contacto, de terceros y el consentimiento informado. El análisis evidencia que todos los activos presentan niveles de criticidad altos, debido a la combinación de amenazas frecuentes y vulnerabilidades estructurales, como el almacenamiento físico sin trazabilidad, la ausencia de cifrado y la falta de segmentación de acceso.

Tabla 10 Proceso Registro de Víctima

Activos	Amenazas	Ocurrencia de amenaza	Vulnerabilidad	Explotación	Valor del Activo	Posible Ocurrencia	Total Promedio	Criticidad
Datos de Identificación	Acceso no autorizado	3	Falta de control de acceso	3	2.67	**3.00**	**2.89**	
Datos de Terceros	Filtración de datos sensibles	3	Sin políticas de confidencialidad	3	2.67	**3.00**	**2.89**	
Consentimiento Informado	Alteración o pérdida	3	Manejo físico sin respaldo	3	3.00	**3.00**	**3.00**	

Fuente: Elaboración propia

Proceso: Evaluación Socioeconómica

En el proceso de evaluación socioeconómica se recopilan datos críticos sobre la situación económica y social de las usuarias, incluyendo historial de violencia y beneficios estatales. El análisis revela una alta exposición al riesgo, motivada principalmente por la inexistencia de controles de cifrado, la falta de acuerdos de confidencialidad y el almacenamiento de información en medios no protegidos. Los resultados reflejan una criticidad alta para todos los activos, lo que requiere una intervención inmediata a nivel técnico y organizacional.

Tabla 11 Proceso Evaluación Socioeconómico

Activos	Amenazas	Ocurrencia	Vulnerabilidad	Explotación	Valor del Activo	Posible Ocurrencia	Total Promedio	Criticidad
Datos Socioeconómicos	Acceso indebido	3	Archivos no cifrados	3	2.67	**3.00**	**2.89**	
Programas Sociales	Uso no autorizado	2	Personal sin acuerdos de privacidad	3	2.33	**2.50**	**2.44**	

	por externos							
Antecedentes Violencia	Alteración de historial	3	Sin respaldo ni control de versiones	3	3.00	**3.00**	**3.00**	

Fuente: Elaboración propia

Proceso: Evaluaciones Psicológicas y Seguimiento

Este proceso incluye el manejo de diagnósticos psicológicos, historiales clínicos y registros de seguimiento terapéutico. La evaluación de amenazas y vulnerabilidades muestra que estos activos presentan una combinación crítica de alta sensibilidad de la información y falta de mecanismos de protección adecuados. A pesar de contar con ciertos controles básicos, la ausencia de cifrado, respaldo digital y control de acceso por roles contribuye a un nivel de criticidad alto en todos los casos analizados.

Tabla 12 Proceso Evaluaciones Psicológicas y Seguimiento

Activos	Amenazas	Ocurrencia	Vulnerabilidad	Explotación	Valor del Activo	Posible Ocurrencia	Total Promedio	Criticidad
Evaluaciones Psicológicas	Exposición de diagnósticos	2	Sin cifrado ni respaldo	3	2.33	**2.50**	**2.44**	
Historial Psicológico	Acceso no autorizado	3	Control de acceso compartido	3	2.67	**3.00**	**2.89**	
Registro de Seguimiento	Divulgación de notas privadas	3	Acceso sin segmentación	3	3.00	**3.00**	**3.00**	

Fuente: Elaboración propia

Proceso: Asesoramiento y Gestión Legal

El tratamiento de datos jurídicos y documentos legales en el MMO implica una exposición significativa a amenazas como el acceso no autorizado, la pérdida de expedientes y la alteración de registros. El análisis evidencia vulnerabilidades clave como la falta de bitácoras de acceso, el almacenamiento físico sin respaldo digital y la carencia de segmentación por roles. Todos los activos evaluados alcanzan niveles de criticidad altos, lo que resalta la necesidad de implementar controles estrictos orientados a la confidencialidad, integridad y disponibilidad de la información jurídica.

Tabla 13 Proceso Asesoramiento y Gestión Legal

Activos	Amenazas	Ocurrencia	Vulnerabilidad	Explotación	Valor del Activo	Posible Ocurrencia	Total, Promedio	Criticidad
Datos Jurídicos	Divulgación no autorizada	3	Falta de trazabilidad y bitácoras	3	3.00	**3.00**	**3.00**	
Estado Procesos Legales	Manipulación de expedientes	3	Acceso compartido sin restricciones	2	2.67	**2.50**	**2.56**	
Casos Archivados	Pérdida por deterioro físico	2	Sin respaldo digital	3	2.33	**2.50**	**2.44**	

Fuente: Elaboración propia

Actividades Clave y Correspondencia Normativa ISO 27001:2022 / LOPDP

A continuación, se resumen los procesos del MMO que manejan datos sensibles, vinculando su base legal, normativa aplicable y medidas de seguridad propuestas según la LOPDP e ISO/IEC 27001:2022.

Tabla 14: Actividades clave y correspondencia Normativa ISO 27001:2022 / LOPDP

Proceso	Base Legal	Normativa Aplicable	Categorías de Datos	Medidas de Seguridad (ISO 27001:2022 / LOPDP)
Registro de Víctima	Obligación legal para la atención de víctimas	LOPDP (Art. 7, 8, 12, 16) / ISO 27001 A.5.15, A.8.10	Identificativos, de contacto, legales	Cifrado, Desidentificación parcial, control de acceso, consentimiento informado
Evaluación Socioeconómica	Consentimiento explícito de la titular	LOPDP (Art. 7, 9, 12, 16) / ISO 27001 A.5.24, A.5.20	Económicos, sociales, de vivienda	Contraseña de acceso, respaldo seguro, política de minimización de datos
Evaluación Psicológica	Consentimiento informado de la titular	LOPDP (Art. 7, 8, 11, 16) / ISO 27001 A.8.10, A.8.11	Datos de salud mental, historia clínica	Almacenamiento cifrado, acceso individualizado, Desidentificación en informes
Asesoramiento Legal	Obligación legal derivada de procesos judiciales	LOPDP (Art. 7, 8, 12, 17) / ISO 27001 A.5.30, A.8.9	Jurídicos, antecedentes penales, medidas cautelares	Protección por roles, logs de acceso, firma digital, respaldo y trazabilidad documental

Selección de Controles

Con base en los riesgos identificados y priorizados en las etapas previas del análisis, se procedió a la selección de controles de seguridad conforme al Anexo A de la norma ISO/IEC 27001:2022. Estos controles fueron elegidos para mitigar las amenazas críticas asociadas al tratamiento de datos personales en el Movimiento de Mujeres de El Oro (MMO), especialmente aquellos datos identificados como de alta sensibilidad (identificación, salud mental, antecedentes legales, entre otros).

Tabla 15 Selección de Controles

Código del Control	Nombre del Control	Categoría ISO/IEC 27001	Amenaza Mitigada	Justificación de Aplicación
A.5.15	Control de acceso	Controles Organizacionales	Acceso no autorizado	Permite establecer perfiles y restricciones de acceso a información crítica.
A.5.23	Gestión de políticas de seguridad	Controles Organizacionales	Falta de políticas de confidencialidad	Formaliza y refuerza el cumplimiento de las normas internas de seguridad.
A.8.10	Cifrado de información	Controles Tecnológicos	Filtración de datos sensibles	Evita que los datos expuestos sean legibles por terceros.
A.5.24	Concienciación y formación en seguridad	Controles de Personas	Uso no autorizado	Garantiza que el personal conozca sus responsabilidades sobre el manejo de datos.
A.8.9	Copias de respaldo	Controles Tecnológicos	Pérdida de información por deterioro físico	Respalda los datos críticos para su recuperación en caso de pérdida o daño.
A.5.20	Control de acceso basado en roles	Controles Organizacionales	Acceso indebido o compartido	Limita el acceso a los datos según funciones específicas del personal.
A.8.11	Eliminación segura de información	Controles Tecnológicos	Retención indebida de datos	Asegura que la eliminación de datos se realice de manera segura y conforme a la ley.
A.5.30	Registro y monitoreo de actividades	Controles Organizacionales	Manipulación o alteración de datos	Permite auditar accesos y detectar actividades no autorizadas.

Fuente: Elaboración propia basado en la Ley de Protección de datos Personales en Ecuador & ISO/IEC 27001:2022

El análisis realizado permitió identificar de forma precisa los activos de información sensibles del Movimiento de Mujeres de El Oro (MMO), así como los riesgos asociados a su tratamiento. La tasación de activos, la evaluación de amenazas y vulnerabilidades, y la priorización del riesgo ofrecieron una visión clara sobre los puntos críticos que requieren intervención inmediata, especialmente en procesos donde se maneja información de carácter legal, psicológico y socioeconómico.

A partir de estos hallazgos, se seleccionaron controles específicos de la norma ISO/IEC 27001:2022 que permiten mitigar las amenazas más relevantes, garantizando así la confidencialidad, integridad y disponibilidad de los datos personales. Esta selección, alineada también con la Ley Orgánica de Protección

de Datos Personales (LOPDP), sienta las bases para una gestión técnica y normativa adecuada en entornos de alta sensibilidad como el MMO.

Resultados y discusión

Tratamiento de los Riesgos

El siguiente cuadro identifica y analiza los principales riesgos asociados al tratamiento de datos personales en contextos de atención a víctimas. Se presentan las amenazas detectadas, su nivel de impacto, las vulnerabilidades que las facilitan, así como las medidas propuestas para mitigar cada riesgo. Esta sistematización permite priorizar acciones de seguridad y fortalecer la protección de la información sensible según su criticidad.

Tabla 16 Tratamiento de los riesgos

Amenaza	Nivel de Impacto	Vulnerabilidad	Explotación	Valor del Activo	Posible Ocurrencia	Controles	Artículo
Acceso no autorizado	3	Falta de control de acceso	3	2.67	3	Implementación de acceso restringido y autenticación multifactor	Art. 7 - Protección de Datos Sensibles; Art. 8 - Principio de Seguridad; Art. 11 - Responsabilidad Proactiva; Art. 12 - Evaluaciones de Impacto; Art. 16; Art. 17
Filtración de datos sensibles	3	No existen políticas de confidencialidad	3	2.67	3	Establecer políticas de confidencialidad y encriptación	Art. 7; Art. 8; Art. 9 - Calidad y Exactitud; Art. 11; Art. 12; Art. 16; Art. 17
Alteración o pérdida de datos	3	Manejo físico sin respaldo	3	3.00	3	Implementar respaldo digital y almacenamiento seguro	Art. 7; Art. 8; Art. 9; Art. 11; Art. 12; Art. 16; Art. 17
Uso no autorizado	2	Personal sin acuerdos de privacidad	3	2.33	2	Control de accesos basado en roles y auditorías continuas	Art. 7; Art. 8; Art. 9; Art. 11; Art. 12; Art. 16; Art. 17
Acceso no autorizado a	3	Control de acceso compartido	3	2.67	3	Segmentar accesos y aplicar	Art. 7; Art. 8; Art. 11; Art. 12; Art. 16; Art. 17

información sensible						cifrado en archivos sensibles	
Pérdida de información por deterioro físico	2	Sin respaldo digital	3	2.33	2	Establecer respaldo digital y mantenimiento preventivo	Art. 7; Art. 8; Art. 9; Art. 11; Art. 12; Art. 17

Fuente: Elaboración propia basado en la ISO/IEC 27001:2022

Tratamiento de los datos utilizando la Ley de protección de datos personales

Como complemento al análisis del tratamiento de riesgos en el manejo de datos personales, el siguiente cuadro presenta la correspondencia normativa con los artículos clave de la Ley Orgánica de Protección de Datos Personales (LOPDP). Para cada amenaza identificada previamente, se detalla cómo se aplica la legislación vigente, reforzando las obligaciones en materia de seguridad, prevención, evaluación, y garantía de derechos. Esta asociación permite consolidar un enfoque integral que no solo identifica los riesgos, sino que también fundamenta su tratamiento en el marco legal correspondiente.

Tabla 17 Tratamiento de los datos utilizando la Ley de protección de datos personales

Amenaza	Art. 8 - Principio de Seguridad	Art. 11 - Responsabilidad Proactiva	Art. 12 - Evaluaciones de Impacto	Art. 7 - Protección de Datos Sensibles	Art. 9 - Calidad y Exactitud de los Datos	Art. 16 - Derecho de Acceso	Art. 17 - Derecho de Acceso, Rectificación y Eliminación
Acceso no autorizado	Aplica: Este artículo establece que deben implementarse medidas de seguridad para proteger los datos personales. Esta amenaza afecta directamente la seguridad de los datos.	Aplica: El responsable debe ser proactivo para prevenir el acceso no autorizado mediante medidas de control.	Aplica: Se deben realizar evaluaciones de impacto para identificar los riesgos y mitigarlos.	Aplica: El acceso no autorizado pone en riesgo la protección de datos sensibles.	Aplica: Los datos deben ser precisos y no alterados por accesos no autorizados.	Aplica: El derecho de acceso de los titulares puede verse afectado si hay accesos no autorizados.	Aplica: El derecho de acceso, rectificación y eliminación puede verse comprometido si hay accesos no autorizados a los datos.

Filtración de datos sensibles	Aplica: Este artículo obliga a tomar medidas para evitar la filtración de datos sensibles, mediante protección adecuada.	Aplica: El responsable debe actuar para evitar la filtración mediante medidas preventivas.	Aplica: Se deben hacer evaluaciones de impacto para entender las consecuencias de una filtración.	Aplica: Los datos sensibles deben ser tratados con un nivel más alto de seguridad para evitar filtraciones.	Aplica: Los datos sensibles deben ser precisos y mantenerse protegidos para evitar filtraciones.	Aplica: La filtración puede interferir con el derecho de acceso a los datos de los titulares.	Aplica: El derecho de rectificación y eliminación es fundamental para controlar los datos filtrados.
Alteración o pérdida de datos	Aplica: Este artículo establece la obligación de proteger los datos de alteración o pérdida mediante medidas de seguridad.	Aplica: Se deben tomar medidas proactivas para evitar la alteración o pérdida de datos.	Aplica: Las evaluaciones de impacto deben identificar los riesgos de alteración o pérdida de datos y cómo mitigarlos.	Aplica: La alteración o pérdida de datos sensibles debe ser especialmente vigilada.	Aplica: La alteración de datos compromete su exactitud, lo que requiere medidas correctivas.	Aplica: El derecho de acceso puede ser afectado si los datos son alterados o perdidos.	Aplica: Los titulares deben poder rectificar o eliminar datos alterados o perdidos.
Uso no autorizado	Aplica: Este artículo establece que debe evitarse el uso no autorizado de los datos mediante medidas de seguridad.	Aplica: El responsable debe actuar de forma proactiva para evitar el uso no autorizado de los datos.	Aplica: Las evaluaciones de impacto ayudarán a identificar el riesgo de uso no autorizado y a tomar medidas.	Aplica: El uso no autorizado de datos sensibles compromete su protección y confidencialidad.	Aplica: El uso no autorizado puede afectar la exactitud y calidad de los datos.	Aplica: Los titulares deben tener acceso a sus datos para asegurar que no sean utilizados indebidamente.	Aplica: El uso no autorizado puede interferir con el derecho de acceso, rectificación y eliminación de los titulares.
Acceso no autorizado a información sensible	Aplica: Este artículo aplica en todos los casos donde se accede a datos sin autorización, especialmente datos sensibles.	Aplica: El responsable debe implementar medidas para prevenir el acceso no autorizado a datos sensibles.	Aplica: Es necesario evaluar el impacto de un posible acceso no autorizado a información sensible.	Aplica: La protección de datos sensibles es clave en este caso.	Aplica: Asegurar que la información sensible sea exacta y no alterada es crucial para evitar acceso no autorizado.	Aplica: Los titulares deben poder acceder a sus datos, y si son sensibles, con seguridad adecuada.	Aplica: La protección de la información sensible es crucial para asegurar los derechos de acceso, rectificación y eliminación.

Pérdida de información por deterioro físico	Aplica: Aunque el deterioro físico es una amenaza, se deben aplicar medidas para proteger la integridad de los datos.	Aplica: El responsable debe ser proactivo en proteger los datos ante el deterioro físico de los soportes.	Aplica: Evaluar el impacto de la pérdida de datos es clave para identificar y mitigar este riesgo.	Aplica: Los datos sensibles deben ser especialmente protegidos contra la pérdida por deterioro.	Aplica: El deterioro físico puede comprometer la exactitud de los datos, por lo que deben ser respaldados.	No Aplica: El derecho de acceso no se ve afectado directamente por la pérdida de datos por deterioro físico, pero sí puede necesitar rectificación.	Aplica: El titular debe poder solicitar la eliminación de datos perdidos o deteriorados.

Fuente: Elaboración propia basado en la Ley de Protección de datos Personales en Ecuador

El análisis de las actividades de tratamiento de datos personales en el Movimiento de Mujeres del Oro (MMO) permitió identificar y clasificar los procesos más sensibles según su nivel de riesgo, tipo de información gestionada, base legal y medidas de seguridad implementadas. A continuación, se presentan cuatro actividades clave que ejemplifican el nivel de exposición y la respuesta institucional frente a las exigencias de la Ley Orgánica de Protección de Datos Personales (LOPDP).

Conclusiones

El presente estudio permitió evidenciar que la protección efectiva de los datos personales en el Movimiento de Mujeres de El Oro (MMO) depende, en primer lugar, de una aplicación rigurosa y prioritaria de la Ley Orgánica de Protección de Datos Personales (LOPDP). Esta normativa constituye el eje legal que regula el tratamiento de información sensible y garantiza derechos fundamentales como el acceso, la rectificación, la eliminación y la confidencialidad de los datos.

La implementación técnica de controles respaldados por la norma ISO/IEC 27001:2022 actúa como un complemento operativo que facilita el cumplimiento de los principios establecidos por la ley. A través de la identificación de activos, el análisis de amenazas y vulnerabilidades, y la priorización de riesgos, se estableció una base sólida para proponer medidas de seguridad que respondan tanto a datos de alto riesgo como a las obligaciones legales del responsable del tratamiento.

Este enfoque integrado no solo asegura los principios de confidencialidad, integridad y disponibilidad de la información, sino que también promueve una gestión institucional basada en la responsabilidad proactiva y la prevención. En conjunto, se concluye que la LOPDP debe ser considerada como la columna vertebral de cualquier modelo de protección de datos personales, especialmente en organizaciones que manejan información de alta sensibilidad como el MMO.

Referencias

Alvear, P. A. A., González, V. N. O., Ajila, L. A. A., & Segarra, H. G. G. (2024). Aplicación de la Ley Orgánica de Protección de Datos Personales en el sistema empresarial privado ecuatoriano. *Revista Lex*, *7*(25), Article 25. https://doi.org/10.33996/revistalex.v7i25.201

Alvear Richards, G. E., & Hernández Pesantes, E. A. (2023). *Análisis comparativo de la ley orgánica de protección de datos personales del Ecuador con la legislación peruana desde un enfoque de ciberseguridad y delitos informáticos* [masterThesis]. http://dspace.ups.edu.ec/handle/123456789/25257

Benussi Díaz, C. (2020). Obligaciones de seguridad en el tratamiento de datos personales en Chile: Escenario actual y desafíos regulatorios pendientes. *Revista chilena de derecho y tecnología*, *9*(1), 227-279. https://doi.org/10.5354/0719-2584.2020.56660

Durán-Ramírez, M. F., & Zamora-Vázquez, A. F. (2023). Vulneración de derechos y protección de datos personales en Ecuador. Caso de estudio: Empresa SmartSolutions. *MQRInvestigar*, *7*(1), Article 1. https://doi.org/10.56048/MQR20225.7.1.2023.330-343

Fuentes Pozo, E. A. (2023). *Análisis y diseño de un modelo de gestión de seguridad de la información basado en el estándar ISO 27001:2022 para la Empresa Pc Soluciones de la ciudad de Babahoyo.* [bachelorThesis, Babahoyo: UTB-FAFI. 2023]. http://dspace.utb.edu.ec/handle/49000/14991

Gutiérrez Meneses, D. M. (2024). *Análisis comparativo de la ley orgánica de protección de datos personales del Ecuador con la legislación chilena desde un enfoque de ciberseguridad y delitos informáticos* [masterThesis]. http://dspace.ups.edu.ec/handle/123456789/27616

Hornuf, L., Mangold, S., & Yang, Y. (2023). Players in the Crowdsourcing Industry. En L. Hornuf, S. Mangold, & Y. Yang (Eds.), *Data Privacy and Crowdsourcing: A Comparison of Selected Problems in China, Germany and the United States* (pp. 5-18). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-32064-4_2

López, C. P., Carrillo, J. A., Urgilés, C. F., & Vintimilla, D. O. (2023). Modelo de madurez de ciberseguridad para infraestructuras críticas caso de estudio: Ecuador. *Pro Sciences: Revista de Producción, Ciencias e Investigación*, *7*(48), 39-56. https://doi.org/10.29018/issn.2588-1000vol7iss48.2023pp39-56

Morales Hidalgo, C. G. (2024). *Plan de seguridad basado en la norma de la seguridad de la información para el sector financiero e ISO 27001 para el análisis del sistema informático de la Cooperativa CACPECO* [masterThesis, Quito, Ecuador: Universidad Tecnológica Israel]. http://repositorio.uisrael.edu.ec/handle/47000/4087

Novoa, E. (2020). El derecho a la protección de datos de personales en la prestación de servicios de cloud computing.: Una perspectiva ecuatoriana. *Revista de Derecho: Publicación de la Facultad de Derecho de la Universidad Católica de Uruguay, 22 (Julio-diciembre)*, 64-89.

Orellana Toledo, M. A. (2022). *Elaboración de una guía de implementación de un SGSI para la Corporación Ecuatoriana para el Desarrollo de la Investigación y la Academia—CEDIA* [bachelorThesis]. http://dspace.ups.edu.ec/handle/123456789/22091

P. Romansky, R., S. Noninska, I., 1 Department of Informatics, Technical University of Sofia, Sofia 1000, Bulgaria, & 2 Department of Computer Systems, Technical University of Sofia, Sofia 1000, Bulgaria. (2020). Challenges of the digital age for privacy and personal data protection. *Mathematical Biosciences and Engineering*, *17*(5), 5288-5303. https://doi.org/10.3934/mbe.2020286

Perugachi Cartagena, R. A. (2021). *Propuesta de un ciclo de gestión de riesgos utilizando modelos de amenazas y controles de seguridad ISO/EC 27002 / EGSI / RGPD* [masterThesis, Quito, 2021.]. http://bibdigital.epn.edu.ec/handle/15000/21384

Rodríguez, G. R. D. L. C., Fernández, R. A. M., & Santos, A. C. M. D. L. (2023). Seguridad de la información en el comercio electrónico basado en ISO 27001: Una revisión sistemática. *Innovation and Software*, *4*(1), Article 1. https://doi.org/10.48168/innosoft.s11.a79

Wiemas N. G., K., & Suroso, J. S. (2024). Analysis of Risk Management Information System Applications Using Iso/Iec 27001:2022. *Syntax Literate ; Jurnal Ilmiah Indonesia*, *7*(11), 18372-18391. https://doi.org/10.36418/syntax-literate.v7i11.15426

Xiong, Q., Lan, Q., Ma, J., Zhou, H., Li, G., & Yang, Z. (2024). DRAPE: Optimizing private data release under adjustable privacy-utility equilibrium. *Information Technology and Management*, *25*(2), 199-217. https://doi.org/10.1007/s10799-022-00378-4