INFORME DE EVALUACIÓN DE IMPACTO Y MEDIDAS DE SEGURIDAD.

1. Objeto y alcance:

Objeto: con base a la auditoría realizada, el objeto es lograr definir las medidas de seguridad proporcionales para proteger los derechos de los titulares, garantizar continuidad del servicio público y demostrar cumplimiento ante la Autoridad de Protección de Datos (SPDP).

Alcance: llega a los procesos, personas, tecnología y terceros asociados a los tratamientos en soporte físico y digital. Incluye el sitio web institucional, estaciones de trabajo, almacenamiento externo y documentación de respaldo.

2. Marco normativo aplicable:

- Ley Orgánica de Protección de Datos Personales.
- Reglamento a la Ley Orgánica de Protección de Datos Personales.
- Constitución de la República del Ecuador.

3. Principios y legitimación:

Se verifica la aplicación de los principios de licitud, lealtad, transparencia, minimización, exactitud, limitación de la conservación, integridad, confidencialidad, y responsabilidad proactiva. Las bases legales predominantes se centran en el interés público y las obligaciones legales; el consentimiento aplica para finalidades comunicacionales específicas.

4. Análisis de necesidad y proporcionalidad:

Siempre es necesario que el GAD Parroquial Rural de Manú se limite a la obtención de los datos personales estrictamente pertinentes y no excesivos. Se requiere especial cuidado de transparencia, información clara y, de requerirse, consentimiento informado. Se recomienda anonimizar o pseudonimizar los datos cuando se publiquen resultados o estadísticas.

5. Metodología de evaluación de riesgos:

Con base a las conclusiones y recomendaciones obtenidas mediante la auditoría del año 2025, se emplea una matriz cualitativa 1–5 para Probabilidad (P) e Impacto (I). El Riesgo Inherente (RI) = P × I.

6. Registro de riesgos actuales y medidas propuestas:

ID	Riesgo	Fuente/escenario en el GADPR Manú	P	I	RI	Control existente	Medidas propuestas	Plazo
R1	Malware o virus.	Antivirus desactualizado; usuarios sin inicio de sesión; controles de aplicaciones desactualizados.	4	4	16	Políticas básicas establecidas.	Mantener antivirus actualizado; habilitar inicio de sesión con correo del usuario autorizado en cada equipo; activar control de aplicaciones potencialmente no deseadas. Mantener los equipos actualizados. **Productos entregables:** Reporte de actualización y registro de antivirus activos.	15 días calendario
R2	Acceso no autorizado a equipos.	No existen cuentas únicas por equipo; no se debe otorgar ningún tipo de acceso a ningún usuario que no sea el custodio del equipo.	4	4	16	Políticas de protección establecidas.	Doble usuario (principal/invitado); bloqueo automático; principio de mínimo privilegio. **Productos entregables:** Reporte que evidencie la configuración de usuarios y bloqueo automático.	15 días calendario
R3	Falta de trazabilidad del tratamiento.	Registro de actividades de tratamiento incompleto; consentimientos y solicitudes no registradas.	3	5	15	Existencia de un formato de registro de actividades.	Actualizar el registro de actividades de tratamiento. **Productos entregables:** Registro actualizado con toda la información singularizada en el informe de auditoría.	30 días calendario
R4	Exposición por terceros.	Contratos o convenios sin cláusulas LOPDP o sin adendums.	3	5	15	Políticas de protección establecidas.	Mantener los contratos y/o convenios con cláusulas técnicas específicas. **Productos entregables:** Elaborar un oficio de insistencia al MIES con respecto al Oficio **No. 0413-GADPR-MANÚ-2025**	30 días calendario
R5	Divulgación inexacta de fechas de implementación del formulario en la página web.	Formulario de tratamiento de datos publicado, pero no existe el acta de implementación.	3	4	12	Políticas de protección establecidas.	Elaborar el acta de implementación; monitoreo constante de la página web sobre la publicación del formulario de tratamiento de datos. **Productos entregables:** Acta de implementación con fecha de la publicación del formulario de tratamiento de datos.	30 días calendario
R6	Pérdida o extravío de equipos de computación.	Existe la posibilidad de la destrucción o pérdida de los equipos de computación, y no	4	4	16	Políticas de protección establecidas.	Suscribir las actas de custodia faltantes para los equipos. **Productos entregables:**	15 días calendario

		hay responsables directos de cada equipo.					Actas de custodia de los equipos de computación faltantes.	
R7	Divulgación de información sin poder determinar responsables.	Falta de contratos de confidencialidad/responsabilidad de los encargados del tratamiento de datos personales.	4	4	16	Seguir protocolos.	Elaborar los contratos de confidencialidad y responsabilidades entre los encargados (Presidente y Secretaria-Tesorera) y el responsable (GAD). **Productos entregables:** Copias de los contratos de confidencialidad y responsabilidades entre los encargados y el responsable.	15 días calendario
R8	Posible filtración por soportes físicos.	Puede existir la posibilidad que los archivadores se encuentren sin control de llaves.	3	3	9	Protecciones y barrera físicas.	Mantener un control minucioso de las personas que ingresan a la institución, y las llaves deben permanecer en manos de la Secretaria – Tesorera. **Productos entregables:** Ninguno.	Permanente
R9	Posible almacenamiento de datos excesivos o retención indebida.	Guardar datos no consentidos o en exceso de lo mínimamente requerido.	3	4	12	Seguir protocolos.	Cumplir con lo dispuesto en el Manual de Buenas Prácticas y el Plan de Protección de Datos. **Productos entregables:** Ninguno.	Permanente
R10	Posibilidad de reidentificación de ciudadanos en publicaciones.	Posibilidad de ausencia de anonimización o pseudonimizaciónen documentos internos o públicos.	2	4	8	Seguir protocolos.	Cumplir con los parámetros de anonimización/pseudonimización. **Productos entregables:** Ninguno.	Permanente

10. Evaluación de impacto residual:

Con las medidas propuestas, los riesgos críticos (R1, R2, R6, R7) bajan de Alto a Medio/Bajo. No se aprecia alto riesgo residual que requiera consulta a la Autoridad, siempre que el plan se ejecute en los plazos definidos y se mantenga la mejora continua.

Por su parte, los riesgos medios (R3, R4, R5) bajan de medio a bajo. Esto implica que los riesgos nunca serán de imposible existencia, pero con una buena metodología de gestión de riesgos se puede mantener alejada esa posibilidad.

En cambio, los riesgos permanentes (R8, R9, R10), si bien hoy no existe un riesgo inminente en estos apartados, esto no implica que no puedan ocurrir, así que no existen correcciones de riesgo a corto plazo sino que se amplian permanentemente en el tiempo.

11. Consulta previa a la autoridad:

Si en futuras evaluaciones persiste alto riesgo residual para los derechos de los titulares que no pueda mitigarse con medidas razonables, el GADPR Manú deberá considerar la consulta previa a la Superintendencia de Protección de Datos Personales antes de continuar o iniciar el tratamiento.

12. Decisión sobre la viabilidad:

Con base en la evaluación realizada y el plan de medidas, los tratamientos descritos son viables bajo las condiciones siguientes: (i) ejecución íntegra del plan 1–30 días, (ii) verificación anual de cumplimiento, (iii) actualización de protocolos, y (iv) revisión contractual con terceros críticos.

13. Conclusiones:

La reducción del riesgo depende de cerrar brechas operativas inmediatas. Con el plan de 30 días y las medidas definidas, el nivel de riesgo residual se reduce a umbrales mínimos.

Elaborado y revisado por el equipo auditor.

Firma atentamente,

ANGEL FABIAN CALVA PEÑA

Firmado digitalmente por ANGEL FABIAN CALVA PEÑA
Fecha: 2025.10.28 17:45:02 -05'00'

Abg. Ángel Fabián Calva Peña.
Delegado de Protección de Datos Personales.