Fundación Centro de Investigaciones Psicológicas

Manual de procedimientos administrativos

y de seguridad informática

Documento	Manual de Procedimientos Administrativos y de Seguridad Informática
Versión	2.1 (Actualizada con estándares DPIA, fuga digital y almacenamiento estratégico)
Fecha de aprobación	[Pendiente - completar tras reunión de Consejo]
Próxima revisión	Anual
Responsable	Coordinación General / Administración / Responsable de IT

Contenido

PARTE I: PROCEDIMIENTOS ADMINISTRATIVOS

1. Gestión de fondos y caja chica

Concepto	Descripción
Responsable	Una persona designada por Coordinación General (administrador/a).
Monto máximo por operación	Hasta $20.000 ARS (U$14) (ajustable anualmente por inflación).
Monto máximo de reposición	Hasta $80.000 ARS (U$57) (fondo fijo).
Gastos permitidos	Pequeños gastos operativos (taxi, fotocopias, café para reuniones, insumos de oficina urgentes, pequeños refrigerios para reuniones de equipo).
Gastos prohibidos	Combustible, comidas personales, regalos, anticipos de sueldo, compras que superen el monto por operación sin autorización.
Procedimiento de rendición	Cada 15 días o cuando se haya usado el 70% del fondo. Debe incluir: ticket o factura original (con CUIT de la Fundación), detalle del gasto, firma de quien recibió y del responsable de caja chica.
Reposición	Se entrega el monto rendido contra entrega de comprobantes válidos.

---

2. Viáticos y gastos de viaje

- **Solicitud:** Debe realizarse por escrito (mail o formulario Anexo 1) con al menos 48 horas de anticipación, indicando motivo, destino, fechas y presupuesto estimado.
- **Montos diarios permitidos** (por persona, en pesos argentinos, ajustables anualmente por inflación):

Concepto	Monto diario
Alojamiento (hasta)	$35.000 (U$25)
Comidas (desayuno, almuerzo, cena)	$10.000 (U$7)
Transporte local	Según gasto real con comprobante
Combustible (vehículo propio)	$200 (U$0,15) por km (o según tarifa oficial de la Administración Pública)

- **Rendición:** Dentro de los 5 días hábiles posteriores al viaje. Debe incluir:
    - Comprobantes de alojamiento (factura a nombre de la Fundación).
    - Facturas de comidas (cuando sea posible obtenerlas).
    - Comprobantes de transporte (pasajes, remises, peajes).
    - Planilla de kilometraje (fecha, origen, destino, km recorridos, motivo).
- Cualquier sobrante debe ser reintegrado a la caja de la Fundación en el momento de la rendición.
- **Gastos no justificados** serán descontados del próximo viático o del sueldo (si aplica).

---

3. Gestión de activos (inventario)

- Se llevará un **registro actualizado** de todos los bienes duraderos (valor > $80.000 ARS o U$57) adquiridos por la Fundación: computadoras, tablets, impresoras, mobiliario, equipos de grabación, teléfonos, etc.
- Cada activo tendrá una **etiqueta de inventario** con número único y será asignado a un responsable mediante la firma del **Formulario de Recepción de Activos** (Anexo 2).
- **Inventario anual:** En diciembre de cada año se realizará un recuento físico de todos los activos, conciliando con el registro. El resultado se comunicará a Coordinación General.

- **Baja de activos:** Requiere autorización de Coordinación General. Si es por robo, debe presentarse denuncia policial. Si es por obsolescencia o rotura, se documenta y se decide donación, venta como chatarra o destrucción segura (especialmente en el caso de discos duros, que deberán ser destruidos o formateados de manera segura).
- **Préstamo de activos:** Solo se permite a personal de la Fundación y por tiempo limitado (máximo 7 días) con autorización del responsable del área. Debe registrarse en un formulario de préstamo.

---

4. Archivo y documentación

- **Estructura de carpetas digitales (en la nube institucional):**

01_Gobernanza/

  01_Actas/

  02_Estatutos/

  03_Politicas/

02_Financiero/

  01_Balances/

  02_Rendiciones/

  03_Facturas/

  04_Comprobantes_pago/

03_Proyectos/

  [Nombre Proyecto]/

    01_Informes/

    02_Financiero/

    03_Comunicaciones/

    04_Evaluaciones/

04_RRHH/

  01_Contratos/

02_Legajos/

03_Capacitaciones/

05_Comunicacion/

01_Prensa/

02_Redes/

03_Materiales/

06_Redes/

01_Convenios/

02_Contactos/

07_Proteccion_Datos/

01_Consentimientos/

02_Denegaciones_ARCO/

03_Incidentes/

04_DPIA/

05_Fuga_Digital/

- **Respaldo:** Copia de seguridad automática diaria en la nube institucional (Google Workspace, Nextcloud, o servicio similar con cifrado) y copia física externa (disco duro encriptado) actualizada semanalmente.
- **Retención de documentos:**
    - Documentos financieros y legales: **10 años**.
    - Documentos de proyectos (informes, evaluaciones): **5 años**.
    - Documentos de personal (contratos, legajos): **5 años** después del egreso.
    - Consentimientos informados y datos personales: Hasta 5 años después de finalizada la intervención, salvo obligación legal de mayor plazo.
- **Destrucción segura:**
    - Documentos en papel con datos sensibles: se destruirán con máquina trituradora (triturado en partículas, no en tiras).

- Archivos digitales: se borrarán de forma segura utilizando software de borrado que sobrescriba la información (ej: DBAN, Eraser) o se destruirá físicamente el soporte (discos duros).

Novedad: Para los documentos de nivel **Restringido** (denuncias, datos de comunidades originarias, información de salud), se debe garantizar que al menos una copia de respaldo se encuentre en servidores ubicados fuera de la jurisdicción provincial, con proveedor certificado en estándares GDPR o equivalentes, como medida de protección contra coerción política, desastres locales o incautaciones. (Ver sección 12.3)

---

5. Firma de documentos y representación

Tipo de documento	Quién firma	Requiere doble firma
Contratos < $1.000.000 ARS	Coordinación General	No
Contratos > $1.000.000 ARS	Coordinación + Presidente del Consejo	Sí
Convenios institucionales	Coordinación General	Sí (con visto bueno del Consejo en reunión)
Cheques / transferencias	Administración + Coordinación	Sí
Rendiciones a donantes	Coordinación General	No, pero con copia al Consejo
Declaraciones juradas	Administración	No
Notas formales a autoridades	Coordinación General	No

Regla general: Toda firma implica la aceptación de responsabilidad sobre el contenido y veracidad del documento.

6. Gestión de recursos humanos

- **Contratación:** Se realizará mediante concurso abierto o búsqueda dirigida, siempre respetando los principios de no discriminación, igualdad de oportunidades y transparencia. Se aplicará lo establecido en el Código de Ética (punto 12) sobre diversidad e inclusión.
- **Legajo del personal:** Cada empleado, voluntario o pasante tendrá un legajo que contendrá:
    - Contrato o carta de acuerdo.
    - Copia de DNI.
    - CV actualizado.
    - Títulos y certificaciones (si aplica).
    - Certificado de antecedentes penales (para personal que trabaje con poblaciones vulnerables).
    - Formularios de adhesión a políticas (SEAH, Anticorrupción, Código de Ética, Protección de Datos).
    - Registro de capacitaciones recibidas.
- **Licencias y permisos:** Se regirán por la legislación laboral argentina y el reglamento interno de trabajo (documento específico).
- **Salud y seguridad en el trabajo:** La Fundación proveerá un entorno de trabajo seguro y saludable. En caso de trabajo de campo en zonas de riesgo, se aplicará el Manual de Seguridad en Frontera y Territorios Apartados (documento específico).

---

7. Compras y contrataciones

Este manual remite a la **Política de Compras y Contrataciones (versión 2.1)** , que debe ser consultada para todo proceso de adquisición de bienes o servicios. El área administrativa es responsable de asegurar el cumplimiento de dicha política.

---

8. Protección de datos personales en la gestión administrativa

En toda la gestión administrativa, la Fundación cumplirá con la **Ley 25.326 de Protección de Datos Personales** y con los principios establecidos en la **Política de Protección de Datos Sensibles (v1.1)** . En particular:

- **Consentimiento:** Siempre que se recaben datos personales (de beneficiarios, personal, proveedores, aliados), se obtendrá el consentimiento informado correspondiente, explicando la finalidad, el plazo de conservación y los derechos ARCO.
- **Derechos ARCO:** Cualquier solicitud de acceso, rectificación, cancelación u oposición deberá ser respondida en un plazo máximo de **10 días hábiles**. Las solicitudes se registrarán en la carpeta 07_Proteccion_Datos/02_Denegaciones_ARCO.
- **Minimización:** Solo se recabarán los datos estrictamente necesarios para la finalidad perseguida.
- **Seguridad:** Se implementarán las medidas técnicas y organizativas necesarias para garantizar la confidencialidad, integridad y disponibilidad de los datos (ver Parte II de este manual).

La gestión administrativa deberá tener en cuenta los resultados de las **Evaluaciones de Impacto de Protección de Datos (DPIA)** realizadas para proyectos sensibles, y aplicar las medidas de mitigación allí definidas. (Ver Anexo 5)

PARTE II: SEGURIDAD INFORMÁTICA (IT POLICY)

9. Uso de equipos y cuentas

- Los equipos informáticos (computadoras, tablets, teléfonos institucionales) son propiedad de la Fundación y deben ser utilizados **exclusivamente para fines laborales**.
- **Prohibido:** Compartir contraseñas, dejar sesiones abiertas en equipos compartidos, instalar software no autorizado, conectar dispositivos de almacenamiento personal sin escaneo previo.
- **Política de contraseñas:**
    - Mínimo **12 caracteres**, con combinación de mayúsculas, minúsculas, números y símbolos.
    - Cambio obligatorio cada **90 días**.

- No reutilizar contraseñas de servicios personales.
- No escribir contraseñas en papeles visibles.
- Uso de **gestor de contraseñas institucional** (ej: Bitwarden, LastPass) recomendado y provisto por la Fundación.

- **Bloqueo de sesión:** Toda computadora debe bloquearse al ausentarse del puesto de trabajo (Windows + L o equivalente).

---

10. Correo electrónico y comunicaciones

- Uso exclusivo de correos institucionales (@fundacioncip.org.ar) para toda comunicación laboral.
- **Prohibido:** Reenviar cadenas, contenido político partidario, material ofensivo o discriminatorio, spam.
- **Phishing y correos sospechosos:** Ante cualquier correo sospechoso (adjuntos extraños, urgencias, remitente desconocido, errores ortográficos):
  - No abrir adjuntos.
  - No hacer clic en enlaces.
  - Reportar inmediatamente al responsable de IT.
- Para comunicaciones con datos sensibles (denuncias, información de víctimas, datos personales de beneficiarios), utilizar exclusivamente:
  - **ProtonMail** (para correo electrónico cifrado).
  - **Signal** (para mensajería instantánea cifrada).
  - El **Canal Ético Digital (CED)** para denuncias.

---

11. Clasificación y protección de datos

Nivel	Definición	Ejemplos	Almacenamiento / Transferencia

Nivel	Definición	Ejemplos	Almacenamiento / Transferencia
Público	Información que puede ser divulgada sin restricción	Material de difusión, informes públicos, folletos	Sin restricciones; puede publicarse en web y redes sociales.
Interno	Uso dentro de la Fundación, no para público general	Actas de reunión, borradores de informes, comunicaciones internas	Carpeta compartida en la nube institucional con acceso restringido al equipo (autenticación requerida).
Confidencial	Datos personales de beneficiarios, información financiera detallada, evaluaciones de personal	Fichas de admisión, rendiciones con datos personales, contratos, evaluaciones de desempeño	Carpeta encriptada en la nube (cifrado en reposo), acceso por roles (solo personal autorizado), doble autenticación obligatoria. Transferencia solo por canales cifrados (ProtonMail, CED).
Restringido	Altamente sensible: denuncias, datos de salud, información de comunidades en riesgo, claves de sistemas, informes de investigación de incidentes	Denuncias de abuso, datos biométricos, secretos de comunidades, claves maestras	Almacenamiento fuera de línea en disco duro encriptado, guardado en caja de seguridad. Acceso solo para casos puntuales y con autorización expresa de Coordinación General y Comité de Ética. Copia de respaldo en servidores fuera de la jurisdicción provincial (ver sección 12.3).

---

12. Copias de seguridad (backups) y almacenamiento estratégico

- **Frecuencia:**

    - Automática diaria para archivos críticos (carpetas Financiero, Proyectos, RRHH, Proteccion_Datos).
    - Semanal para el resto de las carpetas.

- **Responsable:** Administración (o persona designada) verifica semanalmente que los backups se estén realizando correctamente.
- **Almacenamiento:** Mínimo **dos copias**:
    - **Copia 1 (en caliente):** En la nube institucional (cifrada), con proveedor que garantice soberanía de datos y cumplimiento de la Ley 25.326.
    - **Copia 2 (en frío):** En disco externo encriptado, almacenado en la oficina en lugar seguro, actualizado semanalmente.
- **Prueba de restauración:** Cada **6 meses** se realizará una prueba de restauración de un archivo aleatorio para verificar la integridad de los backups. Se documentará el resultado.

12.3. Requisito de almacenamiento externo estratégico

Los datos de nivel **Restringido** que involucren:

- Denuncias de corrupción o abuso de autoridad,
- Información sobre comunidades originarias en situación de riesgo,
- Datos de salud de personas en contextos de vulnerabilidad,
- Cualquier información que pueda exponer a denunciantes o víctimas a represalias,

deberán tener al menos una copia de respaldo en servidores ubicados fuera de la jurisdicción provincial (preferentemente en países con legislación de protección de datos equivalente al GDPR, como los miembros de la Unión Europea). El proveedor de este servicio debe acreditar certificaciones de seguridad (ISO 27001, certificación GDPR) y garantizar que los datos no serán accesibles a autoridades locales sin el consentimiento de la Fundación, salvo orden judicial internacionalmente reconocida.

Esta medida busca garantizar la continuidad operativa y la protección de los derechos de las personas frente a posibles situaciones de coerción política, allanamientos ilegítimos o desastres que afecten la infraestructura local.

---

13. Uso de dispositivos personales (BYOD)

- Permitido solo con autorización expresa de Coordinación General y para tareas específicas (ej: trabajo de campo, teletrabajo).
- El dispositivo debe cumplir con:
    - Contraseña de bloqueo de pantalla (PIN, patrón o biometría).
    - Cifrado de disco completo (si el sistema operativo lo permite).
    - Antivirus actualizado.
    - No tener jailbreak o root.
- La Fundación se reserva el derecho de **borrado remoto** de datos institucionales en caso de pérdida, robo o fin de la relación laboral.
- El usuario acepta que la Fundación pueda auditar el cumplimiento de estas normas en caso de sospecha fundada de incumplimiento.

---

14. Incidentes de seguridad y Protocolo de violación de datos

Este procedimiento desarrolla el **Protocolo de violación de datos (Data Breach)** mencionado en el Código de Ética y en la Política de Protección de Datos.

14.1. Definición de incidente de seguridad

Se considera incidente de seguridad cualquier evento que comprometa la **confidencialidad, integridad o disponibilidad** de la información de la Fundación, incluyendo:

- Pérdida o robo de equipos (computadoras, teléfonos, discos duros).
- Acceso no autorizado a sistemas, cuentas o bases de datos.
- Filtración o divulgación no autorizada de información confidencial o restringida.
- Ataque de ransomware, virus o malware.
- Borrado accidental de información.
- Intento de phishing exitoso que haya comprometido credenciales.

14.2. Clasificación de incidentes

Nivel	Descripción	Ejemplos
Bajo	Impacto limitado, información interna no sensible, rápida contención.	Correo no deseado, intento de phishing fallido, pérdida de un documento público.
Medio	Impacto moderado, información confidencial comprometida, pero con medidas de mitigación posibles.	Pérdida de un teléfono con acceso a correo institucional, acceso no autorizado a una cuenta de usuario, filtración de datos internos no sensibles.
Alto	Impacto significativo, información confidencial o restringida comprometida, posible daño a personas.	Robo de computadora con datos de beneficiarios, filtración de denuncias, acceso no autorizado a la base de datos de proyectos, ataque de ransomware.
Crítico	Impacto grave y extenso, riesgo para la integridad física o psicológica de personas, daño reputacional severo, posible responsabilidad legal.	Filtración masiva de datos de salud de comunidades, publicación de identidad de denunciantes, ataque que paraliza todos los sistemas.

14.3. Equipo de respuesta a incidentes

Rol	Responsabilidad
Coordinador del incidente	Designado por Coordinación General. Lidera la respuesta, coordina al equipo, toma decisiones.
Responsable de IT	Evalúa el alcance técnico, contiene el incidente, recupera sistemas, preserva evidencias.
Responsable de comunicación	Prepara comunicaciones internas y externas (si aplica), informa a afectados.

Rol	Responsabilidad
Responsable legal (abogado de la Fundación)	Evalúa implicaciones legales, contacta a autoridades si corresponde, asesora sobre notificaciones.
Oficial de Protección de Datos (si designado)	Coordina la notificación a la autoridad de control (Dirección Nacional de Protección de Datos Personales) y a los afectados.

14.4. Procedimiento paso a paso

Fase 1: Detección y reporte inicial

1. Cualquier persona que detecte un posible incidente debe reportarlo **inmediatamente** a:
    - Responsable de IT (por teléfono o mensaje urgente).
    - Coordinación General.
    - Correo: incidentes@fundacioncip.org.ar (si está disponible).
2. El reporte debe incluir: qué ocurrió, cuándo, dónde (qué sistema/equipo), quién lo detectó, acciones tomadas hasta el momento.

Fase 2: Evaluación y contención inmediata (primeras 24-48 horas)

1. El equipo de respuesta se reúne (virtual o presencialmente) para evaluar la gravedad y clasificar el incidente.
2. **Contención:** Se toman medidas para detener el daño y evitar que se extienda:
    - Desconectar equipos afectados de la red.
    - Cambiar contraseñas comprometidas.
    - Bloquear accesos remotos.
    - Aislar sistemas infectados.
3. **Preservación de evidencias:** Se realiza una imagen forense de los sistemas afectados (si es posible) o se documenta el estado. No se apagan los sistemas sin antes preservar la evidencia (a menos que sea necesario para contener).

Fase 3: Investigación y evaluación de alcance (48-72 horas)

1. Se determina:

- Qué información se ha visto comprometida (tipo de datos, cantidad de registros, personas afectadas).
- Cómo ocurrió el incidente (vector de ataque, vulnerabilidad explotada).
- Quién es el responsable (si se puede determinar).
- Posibles consecuencias para las personas afectadas (riesgo de daño).

2. Se documenta todo en un **Informe de Incidente** (ver Anexo 3).

Fase 4: Notificación a afectados y autoridades (72 horas máximo)

- **Si el incidente es de nivel Medio, Alto o Crítico**, y afecta datos personales, se debe notificar a la **Dirección Nacional de Protección de Datos Personales** en un plazo máximo de **72 horas** desde que se tuvo conocimiento del incidente (estándar GDPR, adoptado como buena práctica).
- **Notificación a afectados:** Se informará a las personas cuyos datos se hayan visto comprometidos, explicando:
  - Naturaleza del incidente.
  - Datos afectados.
  - Riesgos potenciales.
  - Medidas adoptadas.
  - Recomendaciones para protegerse (ej: cambiar contraseñas, estar alerta a phishing).
  - Datos de contacto para más información.
- La notificación debe ser clara, en lenguaje accesible y, si corresponde, en la lengua de la comunidad afectada.

Fase 5: Remediación y medidas correctivas

1. Se implementan medidas para evitar que el incidente se repita:
   - Parches de seguridad.
   - Refuerzo de políticas de contraseñas.
   - Capacitación adicional al personal.
   - Mejora de controles de acceso.

2. Se actualizan las políticas y procedimientos si es necesario.

Fase 6: Cierre y documentación

1. Se completa el Informe de Incidente con todas las acciones tomadas, lecciones aprendidas y medidas correctivas implementadas.
2. El informe se archiva en la carpeta 07_Proteccion_Datos/03_Incidentes.
3. Se realiza una reunión de lecciones aprendidas con el equipo.

14.5. Modelos de comunicación (Anexo 3)

- Plantilla de informe de incidente interno.
- Plantilla de notificación a la autoridad de control.
- Plantilla de comunicación a afectados.

Para la realización de **Evaluaciones de Impacto de Protección de Datos (DPIA)** y la activación del **Protocolo de fuga digital**, deberán consultarse los Anexos 5 y 6 respectivamente.

---

15. Software y licencias

- Solo se permite software con licencia válida o de código abierto autorizado por la Fundación.
- **Prohibido** instalar software pirateado, sin licencia o de dudosa procedencia.
- El responsable de IT mantendrá un **inventario de software** instalado en cada equipo, con sus respectivas licencias y fechas de vencimiento.
- Las actualizaciones de seguridad deben aplicarse de manera automática o lo antes posible.

---

16. Redes Wi-Fi y conectividad

- La red de oficina (Wi-Fi) tendrá:
    - Contraseña segura (WPA2 o WPA3).
    - Cambio de contraseña cada 6 meses.
    - Acceso solo para personal de la Fundación y visitas autorizadas (con invitado).

- **Red de invitados:** Separada de la red interna, para visitas, eventos y reuniones. No tiene acceso a los recursos internos (carpetas compartidas, impresoras, servidores).
- Para trabajo remoto con datos sensibles, se deberá usar **VPN (Red Privada Virtual)** proporcionada por la Fundación.

---

17. Capacitación en seguridad

- Todo nuevo integrante recibirá una **inducción obligatoria** en esta IT Policy, con especial énfasis en:
    - Clasificación de datos.
    - Uso de contraseñas seguras.
    - Detección de phishing.
    - Procedimiento de reporte de incidentes.
- Anualmente, se realizará una **cápsula de actualización** (presencial o virtual) sobre riesgos comunes (phishing, ingeniería social, nuevas amenazas).
- Se enviarán periódicamente **recordatorios por correo** con buenas prácticas.

---

18. Monitoreo de la política (KPIs y mejora continua)

Para garantizar la efectividad de este manual y su alineación con los estándares internacionales, la Fundación realizará un seguimiento periódico de los siguientes indicadores:

KPI	Meta	Frecuencia de medición	Responsable
% de personal capacitado en seguridad informática y protección de datos (inducción + actualización anual)	100%	Anual	Coordinación + IT
Tiempo promedio de respuesta a incidentes de nivel Alto o Crítico (desde detección hasta	< 24 horas	Por incidente	Responsable de IT

KPI	Meta	Frecuencia de medición	Responsable
contención inicial)			
% de pruebas de restauración de backups exitosas	100%	Semestral	Administración / IT
N° de DPIAs realizados en proyectos de alto riesgo (denunciantes, comunidades originarias)	100% de los proyectos que lo requieran	Por proyecto	Oficial de Protección de Datos
Cumplimiento de plazos de notificación a autoridad de control (72 horas)	100%	Por incidente	Oficial de Protección de Datos
Resultados de auditorías externas (si aplica)	Sin observaciones críticas	Anual	Coordinación

Estos KPIs se revisarán anualmente y se ajustarán en función de la experiencia y los cambios normativos. Los resultados se reportarán en el **Informe Anual de Ética y Transparencia** de la Fundación. El seguimiento se registrará en la tabla del Anexo 7.

---

19. Disposiciones finales

- El incumplimiento de las normas de este manual podrá dar lugar a sanciones disciplinarias, según lo establecido en el Código de Ética y la Política de Anticorrupción.
- Este manual será revisado anualmente o antes si se producen cambios significativos en la tecnología, la legislación o las necesidades de la Fundación.
- Cualquier duda sobre su aplicación debe ser consultada con el responsable de IT o con Coordinación General.

ANEXOS

Anexo 1: Formulario de solicitud de viáticos

(Modelo a implementar en formato digital - Google Forms o similar)

Solicitud de Viáticos - Fundación CIP

- Fecha de solicitud:
- Nombre del solicitante:
- Proyecto / Área:
- Motivo del viaje:
- Destino:
- Fecha de salida:
- Fecha de regreso:
- Cantidad de días:
- Presupuesto estimado:
    - Alojamiento: $
    - Comidas: $
    - Transporte (detallar): $
    - Otros: $
- Total estimado: $
- Adjuntar cotizaciones si corresponde (alojamiento, pasajes).
- Firma del solicitante:
- Autorizado por (Coordinación General):
- Fecha de autorización:

Anexo 2: Formulario de recepción de activos

Recepción de Activo Fijo - Fundación CIP

- Fecha:
- Nombre del receptor:
- Cargo / Área:
- Descripción del activo:
- Número de serie (si aplica):
- Número de etiqueta de inventario:
- Estado del activo al recibirlo (nuevo, usado, observaciones):
- Firma del receptor:
- Firma del responsable de inventario:
- Fecha de devolución prevista (si es préstamo temporal):
- Fecha de devolución real (al momento de la devolución):

Anexo 3: Plantilla de informe de incidente de seguridad

Informe de Incidente de Seguridad - Fundación CIP

Campo	Detalle
N° de incidente	[Año]-[Número correlativo]
Fecha de detección	
Fecha de reporte inicial	
Reportado por	
Tipo de incidente	(Robo de equipo / Acceso no autorizado / Filtración / Ransomware / Otro)

Campo	Detalle
Nivel de gravedad	(Bajo / Medio / Alto / Crítico)
Sistemas afectados	
Datos afectados	(Tipo, cantidad de registros)
Personas afectadas	(Número, colectivo)
Descripción del incidente	(Qué ocurrió, cómo se detectó)
Acciones de contención	
Investigación realizada	(Hallazgos, causa raíz)
Notificaciones realizadas	(Afectados, autoridades, otros)
Medidas correctivas	
Lecciones aprendidas	
Fecha de cierre	
Responsable del informe	

Anexo 4: Glosario de términos

Término	Definición
BYOD	Bring Your Own Device. Política que permite a empleados usar sus dispositivos personales para fines laborales.
Cifrado en reposo	Protección de datos almacenados en discos o bases de datos mediante algoritmos de cifrado.
Cifrado de extremo a extremo	Método de comunicación donde solo los usuarios que se comunican pueden leer los mensajes.
Data breach	Violación de seguridad que provoca la destrucción, pérdida, alteración, divulgación o acceso no autorizado a datos.
Derechos ARCO	Derechos de Acceso, Rectificación, Cancelación y Oposición sobre los datos personales.
DPO	Data Protección Officer (Oficial de Protección de Datos).
GDPR	Reglamento General de Protección de Datos de la Unión Europea.
IT	Information Technology (Tecnologías de la Información).
Ley 25.326	Ley de Protección de Datos Personales de Argentina.
Malware	Software malicioso diseñado para dañar o infiltrarse en un sistema.
Phishing	Técnica de ingeniería social para obtener información confidencial mediante engaño.

Término	Definición
Ransomware	Tipo de malware que cifra los archivos de la víctima y exige un rescate.
VPN	Virtual Private Network. Red privada virtual que extiende una red segura a través de internet.

Anexo 5: Protocolo DPIA (Data Protection Impact Assessment)

5.1. Objetivo

El DPIA (Evaluación de Impacto de Protección de Datos) es un proceso sistemático para identificar y minimizar los riesgos para los derechos y libertades de las personas derivados del tratamiento de datos personales, especialmente cuando dicho tratamiento puede presentar un alto riesgo.

5.2. Triggers obligatorios (¿cuándo hacer un DPIA?)

Se realizará un DPIA de forma obligatoria en los siguientes casos:

- Proyectos que impliquen tratamiento de datos de nivel **Restringido** (salud, denuncias, información de comunidades originarias).
- Proyectos que involucren a **denunciantes de corrupción o abuso**.
- Proyectos que utilicen **nuevas tecnologías** para el tratamiento de datos (ej: aplicaciones móviles, bases de datos complejas, inteligencia artificial).
- Proyectos que impliquen **transferencias internacionales** de datos.
- Proyectos que puedan generar **alto riesgo para los derechos y libertades** de las personas (ej: evaluaciones, perfiles, decisiones automatizadas).
- Cuando el **Oficial de Protección de Datos** lo considere necesario, aunque no se den los supuestos anteriores.

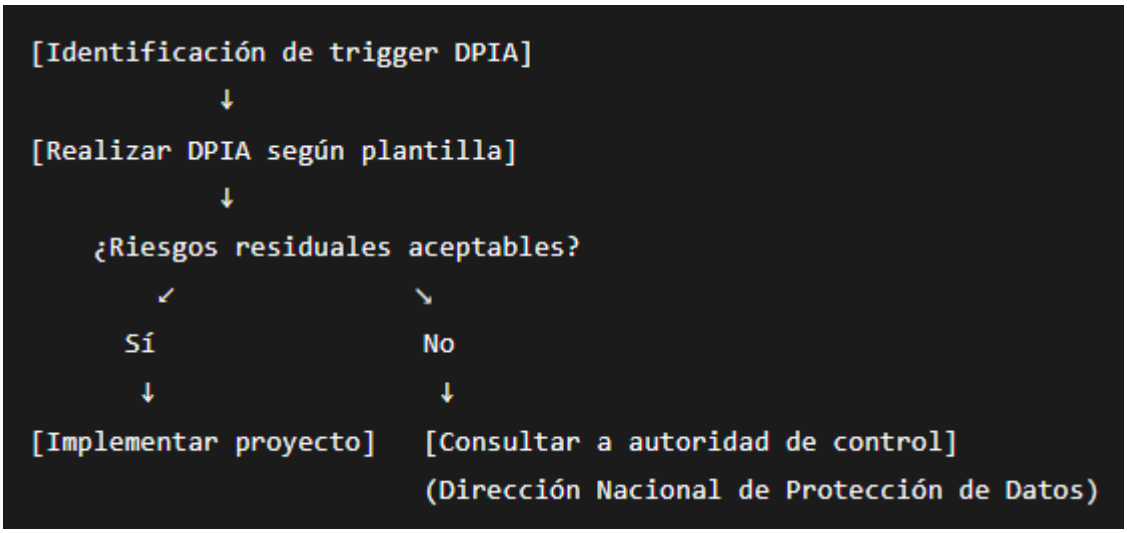
5.3. Procedimiento DPIA

El DPIA se realizará siguiendo la siguiente plantilla:

Sección	Contenido

Sección	Contenido
1. Identificación del proyecto	Nombre del proyecto, responsable, fecha de inicio prevista.
2. Descripción del tratamiento	¿Qué datos se tratarán? ¿De quién es? ¿Con qué finalidad? ¿Qué tecnologías se utilizarán? ¿Habrá transferencias?
3. Evaluación de necesidad y proporcionalidad	¿El tratamiento es necesario para la finalidad? ¿Hay formas menos invasivas de lograr el mismo objetivo?
4. Identificación de riesgos	Listar riesgos potenciales para los derechos y libertades de los titulares (ej: discriminación, robo de identidad, pérdida de confidencialidad, revictimización). Evaluar probabilidad (baja, media, alta) y gravedad (baja, media, alta).
5. Medidas de mitigación	Para cada riesgo identificado, describir las medidas técnicas, organizativas y legales que se implementarán para eliminarlo o reducirlo.
6. Riesgo residual	Una vez aplicadas las medidas, evaluar si el riesgo residual es aceptable.
7. Consulta a interesados	Si corresponde, describir si se ha consultado a los potenciales afectados o a sus representantes.
8. Conclusión y recomendación	El DPIA concluye que el proyecto puede implementarse (con las medidas descritas) / no puede implementarse / debe consultarse a la autoridad de control.
9. Firmas de aprobación	Oficial de Protección de Datos, Comité de Ética (si corresponde), Coordinación General.

5.4. Flujo de decisión DPIA



5.5. Archivo

Los DPIAs completados se archivarán en la carpeta 07_Proteccion_Datos/04_DPIA y estarán disponibles para auditorías internas y externas.

Anexo 6: Protocolo de fuga digital

6.1. Objetivo

Establecer un procedimiento para, en caso de amenaza inminente (coerción política, riesgo de incautación, desastre natural, conflicto armado, orden judicial cuestionable), resguardar o transferir de manera segura la totalidad de la información sensible bajo custodia de la Fundación, garantizando su confidencialidad e integridad.

6.2. Criterios de activación

El protocolo será activado por:

- **Coordinación General.**
- **Comité de Ética Externo** (en caso de que la Coordinación esté inhabilitada).
- Por decisión conjunta de al menos dos de los siguientes: Oficial de Protección de Datos, responsable de IT, un miembro del Consejo Directivo.

La activación procederá ante situaciones como:

- Allanamiento ilegítimo o judicialmente cuestionable de la sede.
- Amenaza de violencia física contra el personal o las instalaciones.
- Orden de entrega de datos que pueda poner en riesgo a denunciantes o comunidades.
- Desastre natural o conflicto que inhabilite la sede.
- Detección de un ataque informático de gran escala que comprometa los sistemas.

6.3. Contactos autorizados

Rol	Contacto	Canal de comunicación de emergencia
Coordinación General	[Nombre, teléfono, Signal]	Signal / ProtonMail
Oficial de Protección de Datos	[Nombre, teléfono, Signal]	Signal / ProtonMail
Responsable de IT	[Nombre, teléfono, Signal]	Signal / ProtonMail
Miembro Comité Ética Externo	[Nombre, teléfono, Signal]	Signal / ProtonMail
Contacto internacional (alianza)	[Organización, persona, contacto]	Signal / ProtonMail

(Este listado se mantendrá actualizado en un documento separado, accesible solo para el equipo de respuesta, y se revisará trimestralmente.)

6.4. Procedimiento paso a paso

1. **Evaluación de la amenaza:** El equipo de respuesta evalúa el tipo de riesgo y el nivel de urgencia.
2. **Identificación de datos críticos:** Se prioriza la transferencia de:
    - Denuncias de SEAH y corrupción.
    - Datos de salud y relatos de violencia.

- Información de comunidades originarias.
- Consentimientos informados y documentación legal sensible.
- Claves y accesos a sistemas institucionales.

3. **Cifrado adicional:** Todos los datos a transferir serán cifrados con una clave adicional (diferente a la de uso cotidiano) utilizando herramientas de código abierto verificadas (ej: VeraCrypt, 7-Zip con AES-256). La clave se comunicará por un canal diferente al de la transferencia (ej: la transferencia se hace por un medio, la clave por Signal).
4. **Transferencia segura:**
   - **Opción A (Nube externa):** Subir los datos a un servidor en la nube con jurisdicción fuera de Argentina (ej: UE, con proveedor certificado GDPR), utilizando una cuenta de emergencia creada previamente. Verificar la integridad de la subida (hash).
   - **Opción B (Dispositivo físico):** Copiar los datos a un disco duro encriptado (cifrado completo) y entregarlo a una persona de confianza (miembro del Comité de Ética Externo, embajada amiga, organización aliada internacional) con instrucciones claras y un acta de recepción.
   - **Opción C (Transferencia a aliado internacional):** Utilizar canales seguros (Signal, ProtonMail) para transferir claves y ubicación a un contacto predefinido en una organización internacional aliada, que actuará como depositario temporal.
5. **Comunicación post-emergencia:** Una vez que el riesgo haya pasado (o si la situación lo permite durante la emergencia), se informará a las personas afectadas (si es posible y seguro) ya la autoridad de control sobre la activación del protocolo, explicando las razones y las medidas adoptadas.
6. **Registro:** Se documentarán todas las acciones en un informe confidencial, archivado en 07_Proteccion_Datos/05_Fuga_Digital. Este informe incluirá: fecha y hora de activación, descripción de la amenaza, datos transferidos y método utilizado, personas involucradas, resultado y estado actual de los datos.

6.5. Verificación post-transferencia

Una vez restablecida la normalidad, se procederá a:

- Verificar la integridad de los datos transferidos.
- Restaurar la copia de seguridad en los sistemas habituales (si corresponde).
- Actualizar las políticas y procedimientos en función de las lecciones aprendidas.

Anexo 7: Tabla de seguimiento de KPIs

KPI	Meta	Q1	Q2	Q3	Q4	Observaciones
% de personal capacitado	100%					
Tiempo promedio respuesta incidentes Alto/Crítico	< 24 h					
% pruebas restauración backups exitosas	100%					
% DPIAs realizados en proyectos de alto riesgo	100%					
% notificaciones a autoridad en plazo (72 h)	100%					
Auditorías externas (resultado)	Sin observaciones críticas					

Este anexo será completado trimestralmente por el responsable de cada indicador y revisado en las reuniones de Coordinación.

Aprobación y vigencia

Elaborado por	Santiago R. Tristany

Fecha	01/02/2016
Revisado por	Coordinación General / Responsable de IT Juan Pablo Britez Svoboda Director
Fecha	01/03/2026
Aprobado por	Consejo Directivo de la Fundación Centro de Investigaciones Psicológicas Waldemar Krieger Longo fundador Bogado Ana María Bogado secretaria
Fecha de aprobación	[13/03/2026
Firma	
Vigencia	A partir de su aprobación, hasta nueva versión.
Próxima revisión	01/03/2027 + 1 año]

Nota final (para el equipo)

Este manual es una **herramienta de trabajo diario**. Su objetivo no es burocratizar, sino facilitar una gestión ordenada, transparente y segura, en coherencia con los valores y principios de nuestra Fundación. Las nuevas incorporaciones (DPIA, fuga digital, almacenamiento externo estratégico y KPIs) nos preparan para los escenarios más exigentes y nos posicionan como una organización de vanguardia en la protección de datos y la seguridad de la información.

Ante cualquier duda, consulten con la Coordinación General, el Oficial de Protección de Datos o el responsable de IT. La seguridad y la transparencia son responsabilidad de todos.

Este documento ha sido actualizado para alinearse con el Código de Ética v3.1, la Política de Protección de Datos Sensibles (v1.1), la Política Anticorrupción (v1.1) y los estándares internacionales de transparencia y seguridad de la información, incluyendo GDPR, ISO 27001 y las

recomendaciones del documento estratégico "*Estructura y organización de vanguardia internacional*".