MODULE 18

Sistemas de organización y gestión de documentos

Para trabajar en casos de tortura, es necesario que las personas litigantes utilicen sistemas efectivos de gestión de documentos. Es importante que los sistemas implementados usen criterios de organización uniformes en todos los niveles de la organización para facilitar la localización de archivos por parte de personas litigates actuales y futuras. Podría ser beneficioso para algunas organizaciones utilizar herramientas en línea o almacenamiento de datos en nube para facilitar la administración y conservación de archivos.

1. Gestión de documentos

Sistemas de almacenamiento: de ser posible, se deben conservar copias electrónicas de todo documento, dado que los archivos digitales son menos susceptibles a ser confiscados. En caso de utilizar herramientas en línea para gestionar documentos, será necesario cumplir con los requisitos de seguridad necesarios.

Creación de carpetas y subcarpetas para cada caso: en caso de almacenar los archivos relativos a los casos en formato digital, podría ser útil organizar las carpetas agrupando los tipos de documentos, de la siguiente forma: (i) Asuntos Administrativos; (ii) Pruebas y otros documentos probatorios; (iii) Correspondencia; (iv) Escritos; (v) Decisiones; e, (vi) Implementación. Otra forma de organizar los documentos en subcarpetas podría ser siguiendo la vida procesal del caso, diferenciando el litigio nacional y las diversas fases del litigio regional o internacional. Lo importante es seguir una metodología uniforme en todos los casos que permita la fácil ubicación de documentos.

Determinar criterios para nombrar documentos: resulta particularmente útil acordar cómo nombrar los documentos. Por ejemplo: *fecha (año/mes/día) – Nombre del caso – Título corto del documento – Iniciales del autor – versión del documento.doc – Multiples borradores.com*

Revisión periódica de documentos: es importante revisar los documentos de los casos de forma regular para cerciorar que estén correctamente guardados y no se hayan eliminado o extraviado documentos.

2. Organización de correspondencia

Todas las comunicaciones relacionadas con un caso, tanto escritas como orales, deben ser realizadas de forma segura. Las organizaciones deben buscar maneras de mantener el contacto periódico con las víctimas de tortura representadas, incluso en periodos en que sus casos estén inactivos. Como buena práctica, las organizaciones deberían mantener registro de sus comunicaciones con las víctimas de tortura, especialmente si en dichas reuniones se acuerda la estrategia con las personas representadas o se discuten estrategias con personas expertas, colaboradores u otras organizaciones.

Comunicaciones en persona o por teléfono: es buena práctica mantener un registro escrito de las conversaciones. Sea en persona o por teléfono, se aconseja tomar notas breves en forma de minutas que resuman lo discutido y cualquier decisión tomada.

Correspondencia vía correo electrónico: los sistemas de almacenamiento de datos en nube que permiten organizar archivos de forma automática son útiles para tener un registro de la correspondencia por email en cada caso. Aún cuando el servicio utilizado no cuente con esta herramienta, se aconseja mantener copia de todos los correos enviados para llevar un registro fehaciente del caso.

Correspondencia por correo postal: se aconseja que toda correspondencia física sea escaneada y guardada en formato electrónico. La copia escaneada es registro suficiente, por lo cual sería posible desechar los documentos originales, salvo que el documento no pueda reemplazarse en el futuro (por ejemplo, declaraciones juradas ante notario o documentos judiciales apostillados).

Correspondencia de tribunales y cortes: la correspondencia oficial debe ser enviada mediante carta formal, que puede ser enviada mediante correo electrónico, de acuerdo a las reglas de procedimiento relevantes de la corte, tribunal u órgano pertinente. Por ejemplo, la Comisión Interamericana de Derechos Humanos sólo acepta documentos enviados electrónicamente mediante el portal de casos. Las guías prácticas de cada órgano deben ser revisadas para corroborar los requerimientos formales de escritos y documentos. Por ejemplo, ciertos documentos pueden requerir rellenar formularios determinados.

3. Organización y recolección de pruebas

La recolección de prueba usualmente involucra a varias personas. Algunas organizaciones que trabajan a nivel internacional pueden precisar recolectar prueba en otras jurisdicciones. Por ello, es fundamental tener en consideración los desafíos logísticos involucrados en la recolección de base probatoria desde el comienzo del litigio.

Al realizar entrevistas con testigos, es necesario considerar lo siguiente:

- **Preparación:** ¿qué información se está intentando obtener?
- **Logística:** las personas entrevistadas deben sentirse seguras y cómodas
- **Idioma:** puede ser necesario contratar a un intérprete para llevar a cabo una entrevista, si la persona entrevistada no habla nuestro idioma. Será necesario entonces considerar presupuesto para ello con anticipación.
- **Confidencialidad:** es necesario explicar claramente a la persona entrevistada cómo las declaraciones vertidas por ella serán usadas durante el litigio, bajo qué parámetros de confidencialidad y cómo se les protegerá si es que se requieren medidas de protección.
- **Lugar:** escoger un lugar en que la persona entrevistada se sienta segura y cómoda
- **Grabación y almacenamiento:** obtener consentimiento y almacenar los registros de forma segura.
- **Requerimientos especiales:** las personas entrevistadoras deben tener el conocimiento, capacitación y habilidades suficientes para realizar las entrevistas.
- **Otras consideraciones:** tales como, entre otras, considerar cómo el trauma sufrido puede impactar a la persona entrevistada; evaluar la necesidad de tener a personal

médico o psicológico presente; considerar la posibilidad de consecuencias negativas para la persona entrevistada; asegurar su seguridad, etc.

Asimismo, toda prueba debe ser grabada con un nombre que facilite su identificación y ser archivada en la carpeta del caso. Si la prueba está en una lengua diferente a la del escrito, los documentos y declaraciones obtenidas deberán ser traducidas al idioma en que los escritos sean presentados al tribunal u órgano. La recolección y almacenamiento de prueba puede presentar riesgos de seguridad para las víctimas y organizaciones. Por ello los riesgos deben ser evaluados, manejados y mitigados correctamente.

4. Bitácora de casos y calendarios de litigación

Además de la gestión de documentos y comunicaciones, resulta útil llevar seguimiento de los movimientos de causas mediante bitácoras. Las bitácoras deben ser actualizadas periódicamente, y pueden incluir información como: (i) el personal asignado al caso; (ii) la información de contacto de la víctima; (iii) la información de contexto relevante; (iv) los delitos y violaciones involucrados; (v) los escritos presentados ante el tribunal u órgano; (vi) los siguientes pasos a seguir en la causa.

Llevar registro de plazos y fechas límite es fundamental. Un plazo perdido puede significar la pérdida de la única oportunidad procesal que las víctimas tienen para obtener reparaciones, verdad y justicia. Por ello es aconsejable registrar los plazos de las causas en calendarios compartidos para que la organización tenga conciencia de la carga de trabajo y pueda planificar de manera acorde.

5. Cerrar una causa

Al final de un litigio, la carpeta de una causa puede ser cerrada de forma tal que todos los datos vinculados al caso sean gestionados de acuerdo con los estándares legales, éticos y en cumplimiento de las reglas proveídas por el tribunal u órgano competente.

Cuándo cerrar un caso: los criterios para cerrar una causa deben ser los mismos utilizados para considerar su apertura. Es decir, **considerar el mandato y experticia de la organización, las consideraciones y preferencias de las víctimas y si el litigio ha respondido a sus expectativas, las características del caso y estado de implementación de la decisión, la estrategia, impacto y consideraciones relativas a la organización, incluidos sus recursos.**

Cerrar una causa: una vez tomada la decisión de cierre de un caso, se aconseja informar mediante carta formal a la víctima, además de las conversaciones más informales, explicando las medidas para el almacenamiento o destrucción de la carpeta relativa al caso. Los archivos electrónicos no deben ser eliminados inmediatamente luego de cerrar la causa, debido al riesgo de acciones legales que se puedan tomar en contra de la organización por el asesoramiento prestado. La decisión sobre qué documentos se pueden desechar puede atender a las políticas de datos privados que existan en la jurisdicción determinada.

Consentimiento: los archivos nunca deben ser destruidos sin el consentimiento de las víctimas. En caso de no tener consentimiento, será necesario ponderar los riesgos de destruir los datos (por ejemplo, si la víctima quiere recuperar archivos o hay posibilidad de que interponga una demanda o reclamo contra la organización) y los costos de conservarlos.

Seguridad digital el manejo efectivo de casos

1. Principios generals de la seguridad digital

- **Prevenir:** diseñar e implementar un **plan de prevención de vulneración de datos**. Este plan debe incluir la capacitación del personal respecto a los pasos y procesos para resolver potenciales amenazas y mitigar su impacto sobre la seguridad y privacidad de las víctimas.
- **Proteger:** las herramientas en línea de gestión de datos o almacenamiento de datos en la nube deben cumplir con los requisitos y requerimientos de seguridad según el trabajo que se lleve a cabo en ellas. Deben ser gestionadas por proveedores confiables y certificados, cuyos productos estén configurados para reducir riesgos/vulnerabilidades; y en caso de que éstas existan, sean capaces de identificarlas y corregirlas a tiempo.
- **Responder:** de identificarse un riesgo o vulneración de datos, será necesario evaluar qué datos fueron comprometidos, los grupos afectados, el daño potencial y la implementación de planes de recuperación y compensación por los daños causados.

2. Identificar y entender el riesgo

Al evaluar riesgos de seguridad, las organizaciones deben considerar:

- ¿Cuáles son los recursos informáticos más relevantes?
- ¿Qué clase de vulneración de datos presentaría el mayor impacto al trabajo realizado?
- ¿Cuáles son las fuentes de las amenazas y el potencial impacto de cada una de ellas?
- ¿Cuál es el nivel de riesgo que la organización está dispuesta a tomar al lidiar con información reservada y confidencial entregada por las víctimas y qué afecta la seguridad de las víctimas, la organización, y otras personas vinculadas con el litigio?

3. Compartir información y realizar comunicaciones de manera segura

Práctica general: Al compartirse información sensible, las siguientes acciones deben ser consideradas:

- Usar advertencias o declaraciones de confidencialidad al compartir información mediante correo electrónico.
- Tomar precaución al abrir correos, enlaces o archivos adjuntos de remitentes desconocidos.
- Usar plataformas encriptadas, tales como Tresorit, Proton Mail, o sistemas de acceso digital, tales como Office 365 o Dropbox para compartir documentos.

Medidas de seguridad avanzadas: Para incrementar la protección de las comunicaciones e información, las organizaciones pueden:

- Usar nombres en clave para referirse a casos al discutir información del proyecto con terceras partes.
- Usar sistemas de correo electrónico, acceso de información, mensajería y voz encriptados.
- Usar contraseñas para reuniones confidenciales.
- Usar sistemas de mensajería seguros tales como Signal y considerar activar la desaparición automática de mensajes.
- Realizar reuniones en persona y apagar celulares o dejarlos fuera de las salas de reunión.

- Eliminar datos del escritorio y bandeja de reciclaje de celulares y computadores al viajar.
- Proteger documentos confidenciales mediante contraseñas.
- Entregar versiones impresas de documentos cuando sea necesario por motivos de seguridad.
- Usar Microsoft Document Inspector para remover metadata de archivos cuando hayan riesgos de seguridad.
- Usar cuentas anónimas en redes sociales para investigar a personas de interés.
- Usar modo incógnito o privado en internet para ocultar búsquedas previas y protegerse de cookies al realizar investigaciones.

Prepararse para enfrentarse a vulneraciones: determinar una estrategia para mitigar el daño causado, reportar ataques (en algunas jurisdicciones esto es obligatorio), asignar responsabilidades y proveer compensaciones por daños de ser el caso.

Cumplimiento de normas: el personal de la organización debe conocer las obligaciones legales de protección de datos dispuestas por el ordenamiento jurídico doméstico y regional. Por ejemplo, organizaciones europeas deben recolectar y procesar datos personales de acuerdo con las responsabilidades dispuestas en la RGDP.