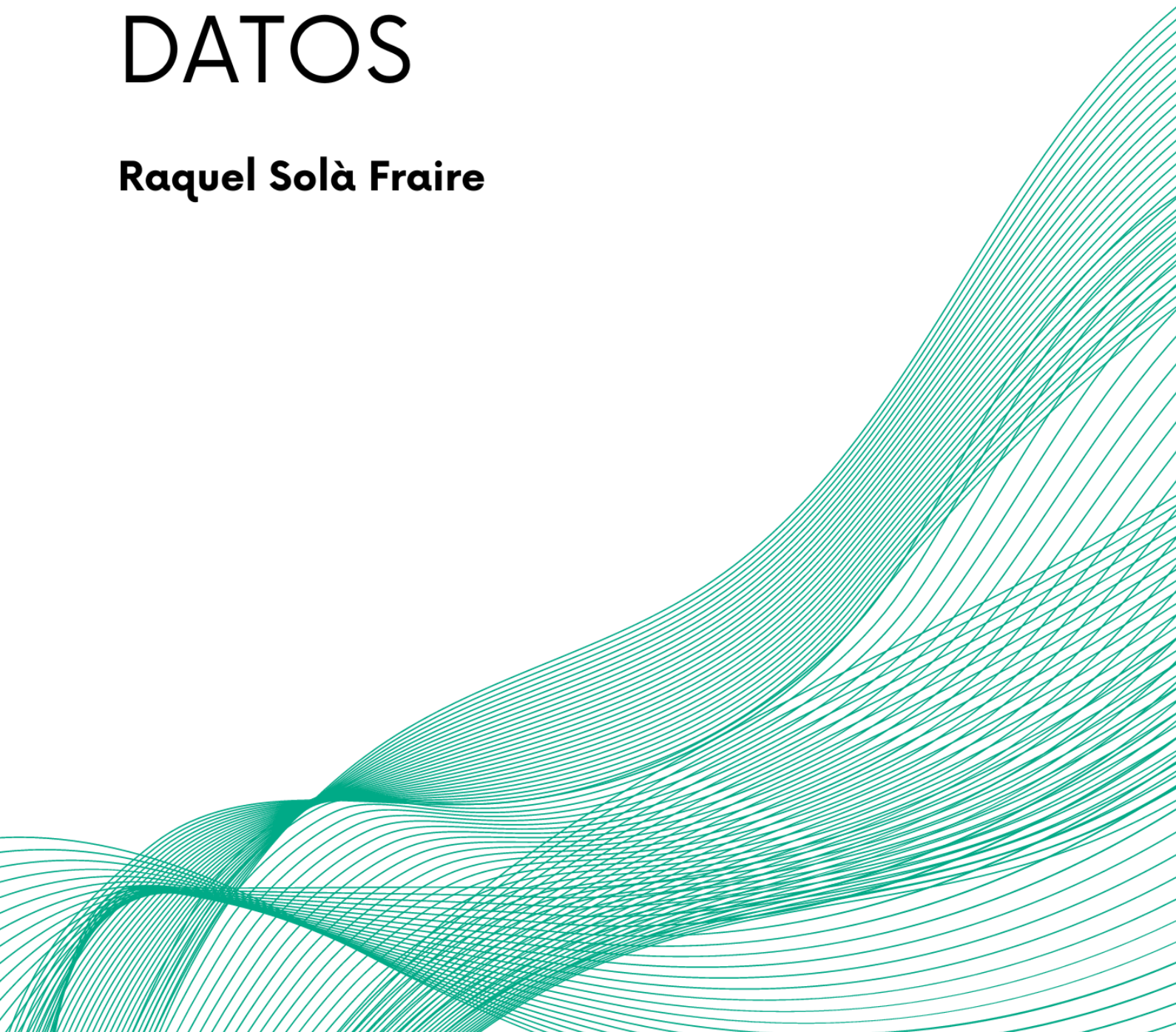
RETO 9 - DOCUMENTO 2

POLÍTICA DE PROTECCIÓN DE DATOS

Raquel Solà Fraire



ÍNDICE

INTRODUCCIÓN

En el entorno educativo, el uso y la gestión de datos se han convertido en aspectos fundamentales para el funcionamiento efectivo de las instituciones escolares. Con el avance de la tecnología y la digitalización de los procesos educativos, surge la necesidad de **establecer medidas claras y efectivas** para proteger la privacidad y la seguridad de los datos personales de estudiantes, personal educativo y otros miembros de la comunidad escolar.

Esta política de protección de datos tiene como objetivo principal **salvaguardar la confidencialidad, integridad y disponibilidad de la información sensible** que se recopila, procesa y almacena dentro de nuestra institución educativa. Reconocemos que los datos personales son recursos que deben ser tratados con responsabilidad y respeto.

Al establecer esta política, **nos comprometemos a cumplir con las leyes y regulaciones de protección de datos pertinentes**, así como a **adoptar las mejores prácticas y estándares internacionales en materia de privacidad y seguridad de la información.** Esta política proporciona una guía para el manejo adecuado de los datos personales en nuestra escuela, garantizando la confianza y tranquilidad de nuestra comunidad educativa.

Además, esta política no solo se limita a la conformidad legal, también refleja nuestro compromiso de proteger los derechos y la privacidad de todos los individuos involucrados en nuestros procesos educativos.

Esta introducción marca el inicio hacia la creación de un entorno seguro y confiable donde los datos personales sean tratados diligencia y respeto. Invitamos a todos los miembros de nuestra comunidad educativa a participar activamente en la implementación y el cumplimiento de esta política, reconociendo que la protección de datos es responsabilidad de todos y cada uno de nosotros. Juntos, trabajaremos para garantizar la integridad y la privacidad de los datos en nuestra escuela.

TÉRMINOS CLAVE

En el marco de una política de protección de datos para una escuela, es crucial establecer una comprensión clara y unificada de los términos clave que se utilizarán a lo largo de la política. Estos términos proporcionan el lenguaje común necesario para una comunicación efectiva y un cumplimiento consistente de las disposiciones de protección de datos.

DATOS PERSONALES

Se refiere a **cualquier información que identifique o pueda identificar a una persona física.**

- Nombres
- Direcciones
- Números de teléfono
- Correos electrónicos
- Números de identificación
- Fotografías
- Registros académicos

PROCESAMIENTO DE DATOS

Hace referencia a **cualquier operación o conjunto de operaciones realizadas sobre datos personales**, ya sea por medios automatizados o no automatizados.

TRATAMIENTOS CON LOS DATOS	
• Recopilación	• Almacenamiento
• Registro	• Adaptación o modificación
• Consulta	• Recuperación
• Uso	• Difusión

CONSENTIMIENTO

Es el **acto voluntario y explícito mediante el cual una persona otorga permiso para el procesamiento de sus datos personales para uno o varios fines específicos.**
El consentimiento debe ser informado, libremente dado, específico e inequívoco, y debe ser obtenido mediante una acción afirmativa clara, como una firma o una selección activa en una casilla.

INTERESADO

Se refiere a la **persona física a la que se refieren los datos personales.** En el contexto escolar, los interesados pueden incluir **estudiantes, padres o tutores legales, personal docente y administrativo,** así como cualquier otra persona cuyos datos personales sean procesados por la escuela.

ANONIMIZACIÓN

Es el **proceso mediante el cual se eliminan o modifican los datos personales de manera que ya no puedan asociarse con un individuo específico sin el uso de información adicional.** La anonimización se utiliza para proteger la privacidad de los interesados y reducir los riesgos asociados con el procesamiento de datos personales.

PRINCIPIOS RECTORES

Los principios rectores son directrices fundamentales que guían una política o actividad hacia un propósito específico.
En una política de protección de datos, son pilares que reflejan los valores de la organización sobre el manejo de información personal. Incluyen la transparencia, consentimiento informado, minimización de datos, seguridad, integridad, exactitud y retención limitada. Estos principios aseguran el respeto a los derechos y la privacidad de las personas, así como la protección adecuada de la información sensible.

TRANSPARENCIA	**CONSENTIMIENTO**	**MINIMIZACIÓN DE LOS DATOS**	**SEGURIDAD**
INTEGRIDAD DE Y EXACTITUD		**RETENCIÓN LIMITADA**	

TRANSPARENCIA

La escuela se compromete a **ser transparente sobre cómo se recopilan, utilizan, comparten y almacenan los datos personales.** Esto implica proporcionar información clara y accesible sobre las prácticas de protección de datos, incluidos los propósitos del procesamiento, los tipos de datos recopilados, los derechos de los interesados y cómo ejercerlos, así como cualquier otro aspecto relevante relacionado con la privacidad y seguridad de la información.

CONSENTIMIENTO

La escuela obtendrá el consentimiento explícito y libremente otorgado de los interesados antes de recopilar, procesar o compartir sus datos personales. Este consentimiento será específico para cada propósito de procesamiento y se obtendrá de manera clara y comprensible, asegurando que los interesados estén plenamente informados sobre cómo se utilizarán sus datos.

MINIMIZACIÓN DE DATOS

Nuestra escuela se compromete a **recopilar y procesar únicamente los datos personales que sean necesarios y proporcionales para cumplir con los fines específicos establecidos.** Se implementarán medidas para garantizar que no se recopilen más datos de los necesarios y que los datos se mantengan actualizados y precisos durante el tiempo que sea necesario para cumplir con dichos fines.

SEGURIDAD

La escuela adoptará **medidas técnicas y organizativas apropiadas para proteger los datos personales contra el acceso no autorizado, la divulgación, la alteración o la destrucción accidental o ilícita.** Se implementarán controles de seguridad adecuados, como cifrado, autenticación de usuarios, políticas de contraseñas, firewalls y protección contra malware, para garantizar la confidencialidad, integridad y disponibilidad de la información.

INTEGRIDAD Y EXACTITUD

La escuela se compromete a **garantizar que los datos personales sean precisos, completos y estén actualizados.** Se establecerán procedimientos para corregir o rectificar cualquier información inexacta o incompleta tan pronto como sea posible, y se tomarán medidas para garantizar que los datos no se conserven durante más tiempo del necesario para los fines para los que fueron recopilados.

RETENCIÓN LIMITADA

Nuestra escuela establece **períodos de retención claros y coherentes para los datos personales,** eliminando los datos cuando ya no sean necesarios para los fines para los que fueron recopilados.

	¿Qué incluye?	RETENCIÓN
Registros Estudiantiles	Registros académicos Registros de asistencia Registros médicos Registros disciplinarios	Durante el curso académico Periodo adicional de 2 años tras la graduación
Registros del Personal	Registros de empleo Contratos de trabajo Evaluaciones del desempeño Registros de salario y beneficios	Durante el periodo de empleo Periodo adicional de 2 años tras la desocupación
Registros Financieros	Registros contables Recibos de pagos Registros de subvenciones	Periodo de 6 años
Documentos Administrativos	Políticas escolares Procedimientos de la escuela Políticas de seguridad y privacidad	Retenidos 2 años después de obsolescencia o actualización
	Comunicaciones con los padres o tutores legales	Periodo de 1 años
	Decisiones administrativas: Cambios de personal Decisiones disciplinarias Cambios de política	Retenida durante un periodo de 2 años para mantener un historial completo de las acciones de la escuela.

RESPONSABILIDADES

Las responsabilidades relacionadas con la identificación de roles en una política de protección de datos son cruciales para asegurar una distribución clara de responsabilidades dentro de la organización.

OFICIAL DE PROTECCIÓN DE DATOS (DPO)

En el contexto de nuestra escuela este rol lo asume el subdirector de la escuela.

RESPONSABLE DE…

- Supervisar la conformidad con las leyes y regulaciones
- Asesorar a la organización sobre sus obligaciones de privacidad
- Cooperar con autoridad de protección de datos
- Servir como punto de contacto para consultas de protección de datos

RESPONSABLE DE LA POLÍTICA DE PROTECCIÓN DE DATOS

Consideramos que el equipo de coordinación tecnológica es el más adecuado para asumir este rol.

RESPONSABLE DE…

- Creación, implementación y mantenimiento continuo de la política de protección de datos
- Asegurar que la política esté actualizada

ADMINISTRADOR DE DATOS

Este rol lo asume el personal administrativo.

RESPONSABLE DE…

- Supervisar el procesamiento de datos personales
- Garantizar que se sigan los principios de protección de datos y que se implementen medidas de seguridad adecuadas.

USUARIOS AUTORIZADOS

Todo el **personal que tenga acceso a datos personales en el curso** de sus funciones tiene la responsabilidad de manejar esa información de manera segura y en cumplimiento de las políticas y procedimientos establecidos.

En el caso de nuestra escuela, los usuarios autorizados a tener acceso a los datos personales del alumnado son los siguientes:

- Personal administrativo: Esto incluye directores, secretarios, personal de recursos humanos y personal administrativo en general que necesiten acceder a los datos para llevar a cabo tareas administrativas y de gestión escolar.

- Docentes: **Los profesores y maestros** pueden requerir acceso a los datos personales de los estudiantes para llevar un registro preciso del progreso académico, planificar lecciones personalizadas, y mantener la comunicación con los padres o tutores.

- Personal de Servicios Educativos Especiales: Este grupo incluye a los **trabajadores sociales, psicólogos escolares, consejeros académicos** y otros profesionales que trabajan directamente con los estudiantes para brindar servicios de apoyo y atención personalizada.

- Personal de Apoyo Técnico: Los **administradores de sistemas de tecnología** de la información y personal de soporte técnico pueden requerir acceso a los datos personales para garantizar la seguridad y el funcionamiento adecuado de los sistemas informáticos y de tecnología de la escuela.

EQUIPO DE SEGURIDAD DE LA INFORMACIÓN

Este rol lo asume el equipo de administrador de sistemas, especialistas en seguridad cibernética, y otros profesionales de TI.

RESPONSABLES DE…

- Implementar y mantener medidas técnicas y organizativas para proteger los datos contra **accesos no autorizados, pérdidas o daños.**
- Garantizar que se sigan los principios de protección de datos y que se implementen medidas de seguridad adecuadas.

EQUIPO DE RESPUESTA A INCIDENTES

Este rol lo asume el equipo coordinador del centro

RESPONSABLES DE…

- Gestionar y responder a incidentes de seguridad de datos (brechas de seguridad, violaciones de datos…)
- Tomar medidas para mitigar el impacto y coordinar la notificación de incidentes.

PROCESAMIENTO DE LOS DATOS

PROPÓSITOS DE LA RECOPILACIÓN Y PROCESAMIENTO DE DATOS

Definir claramente los propósitos legítimos y específicos para los cuales se recopilan y procesan los datos personales en la organización.

ADMINISTRACIÓN ACADÉMICA

Recopilar y procesar **datos personales de estudiantes para gestionar** matrículas, registros académicos, asistencia, evaluaciones y otros aspectos relacionados con la educación y el aprendizaje.

GESTIÓN DEL PERSONAL

Recopilar y procesar **datos personales de empleados y personal docente** para gestionar la contratación, nóminas, evaluaciones de desempeño, capacitación y desarrollo profesional, así como otros aspectos relacionados con la gestión de recursos humanos.

COMUNICACIÓN CON PADRES Y TUTORES

Recopilar y procesar **datos personales de padres, tutores y otros contactos de emergencia** para facilitar la comunicación con la comunidad escolar, enviar información relevante sobre actividades escolares, eventos y noticias, así como para notificar sobre emergencias y situaciones importantes.

SERVICIOS DE APOYO ESTUDIANTIL

Recopilar y procesar **datos personales de estudiantes para proporcionar servicios de apoyo educativo,** como orientación académica, servicios de salud estudiantil, asesoramiento psicológico, y adaptaciones o ajustes razonables para estudiantes con necesidades especiales.

SEGURIDAD Y GESTIÓN DE INSTALACIONES

Recopilar y procesar datos personales para garantizar la s**eguridad de los estudiantes, el personal y las instalaciones escolares,** incluyendo la gestión de acceso a las instalaciones, el monitoreo de video, y la identificación de visitantes.

CUMPLIMIENTO LEGAL Y REGULATORIO

Recopilar y procesar datos personales para **cumplir con las obligaciones legales y regulatorias aplicables,** como informes gubernamentales, presentación de impuestos, cumplimiento de normativas educativas, y respuesta a solicitudes de información de autoridades competentes.

INVESTIGACIÓN Y DESARROLLO EDUCATIVO

Recopilar y procesar datos personales para **fines de investigación y desarrollo educativo,** como la mejora de programas académicos, la evaluación del rendimiento estudiantil, el análisis de resultados educativos, y la planificación estratégica institucional.

Es importante que estos propósitos estén claramente definidos y nos comprometemos a que se recopilen únicamente los datos necesarios para cumplir con dichos fines, garantizando siempre el respeto a la privacidad y los derechos de los interesados.

PROCEDIMIENTOS PARA LA RECOPILACIÓN DE DATOS, INCLUIDA LA OBTENCIÓN DE CONSENTIMIENTO CUANDO SEA NECESARIO

Establecer procedimientos **claros y transparentes** para la recopilación de datos personales, asegurando que se recolecten **únicamente los datos necesarios** para cumplir con los propósitos establecidos.
Cuando sea necesario obtener consentimiento para el procesamiento de datos, garantizar que se obtenga de manera **voluntaria, específica, informada y explícita** por parte de los interesados, utilizando medios **claros y comprensibles** para solicitar y registrar el consentimiento.

SEGURIDAD DE DATOS DURANTE LA TRANSMISIÓN Y ALMACENAMIENTO

- Implementar **medidas técnicas y organizativas adecuadas** para proteger los datos personales durante la transmisión y el almacenamiento.
- Utilizar **métodos de cifrado y protocolos seguros** para garantizar la **confidencialidad** y la integridad de los datos durante la transmisión a través de redes internas o externas.
- Asegurar que los sistemas de almacenamiento de datos estén **protegidos contra accesos no autorizados,** mediante el uso de controles de acceso, autenticación de usuarios, firewalls, y otras medidas de seguridad apropiadas.
- Establecer **políticas de retención de datos** para determinar el período de tiempo durante el cual se retendrán los datos, y asegurar su eliminación segura cuando ya no sean necesarios para los fines establecidos.

DERECHOS DE LOS INTERESADOS

La política de protección de datos debe incluir una **descripción clara de los derechos de privacidad de los interesados**, así como los procedimientos para ejercer estos derechos. Aquí tienes una descripción general:

	DERECHO	Los interesados tienen derecho a…
1	**ACCESO**	Solicitar y recibir información sobre qué datos personales están siendo procesados, para qué fines y quiénes son los destinatarios de dichos datos.
2	**RECTIFICACIÓN**	Solicitar la corrección de datos personales inexactos o incompletos que estén siendo procesados.
3	**SUPRESIÓN**	Solicitar la eliminación de sus datos personales cuando ya no sean necesarios para lo que fueron recopilados, cuando se retire el consentimiento, o cuando los datos estén siendo procesados de forma ilegal.
4	**LIMITACIÓN DEL TRATAMIENTO**	Solicitar la limitación del procesamiento de sus datos personales en ciertas circunstancias.
5	**PORTABILIDAD DE DATOS**	Recibir sus datos personales en un formato estructurado y transmitir esos datos a otro controlador sin impedimentos, cuando el procesamiento se realice por medios automatizados y esté basado en el consentimiento o un contrato.
6	**OPOSICIÓN**	Oponerse en cualquier momento, por motivos relacionados con su situación particular, al procesamiento de sus datos personales, cuando dicho procesamiento se base en el interés legítimo del responsable o en el ejercicio de una tarea realizada en interés público.

PROCEDIMIENTOS PARA EJERCER ESTOS DERECHOS

SOLICITUD POR ESCRITO O ELECTRÓNICA

Los interesados pueden ejercer sus derechos **presentando una solicitud por escrito o electrónica al responsable del tratamiento de datos.** Esta solicitud debe incluir la identificación del solicitante y la especificación del derecho que se desea ejercer.

VERIFICACIÓN DE IDENTIDAD

El responsable del tratamiento puede solicitar al interesado que **verifique su identidad antes de procesar la solicitud**, para evitar el acceso no autorizado a los datos personales.

TIEMPO DE RESPUESTA

El responsable del tratamiento está **obligado a responder a las solicitudes de los interesados en un plazo determinado,** generalmente dentro de los 30 días siguientes a la recepción de la solicitud.

ACCIONES A TOMAR

Dependiendo de la naturaleza de la solicitud, el responsable del tratamiento puede tomar medidas como **proporcionar acceso a los datos solicitados, corregir información inexacta, eliminar datos o limitar su procesamiento**, según corresponda.

Nos comprometemos a ofrecer una política de protección de datos clara y transparente respecto a los derechos de los interesados y los procedimientos para ejercerlos, cumpliendo así con las regulaciones de privacidad aplicables, como el Reglamento General de Protección de Datos (GDPR) en la Unión Europea.

TRANSFERENCIAS INTERNACIONALES

Nuestra política de protección de datos incluye directrices claras para el manejo de datos personales transferidos fuera del área geográfica del país y la Unión Europea (UE), si aplica.

EVALUACIÓN DE LA ADECUACIÓN

Antes de transferir datos personales a un país fuera del área geográfica del país y la UE, se debe **realizar una evaluación para determinar si ese país proporciona un nivel adecuado de protección de datos.** Esto puede implicar considerar si el país en cuestión tiene leyes de protección de datos sólidas o si existen mecanismos alternativos para garantizar un nivel adecuado de protección.

MECANISMOS DE TRANSFERENCIA ADECUADOS

En ausencia de una decisión de adecuación, se deben utilizar **mecanismos adecuados para garantizar la protección de los datos personales transferidos.** Estos mecanismos pueden incluir cláusulas contractuales estándar aprobadas por la Comisión Europea, normas corporativas vinculantes, códigos de conducta o certificaciones aprobadas.

CONSENTIMIENTO INFORMADO

Cuando sea necesario transferir datos personales fuera del área geográfica del país y la UE, se debe **obtener el consentimiento informado de los interesados.** Este consentimiento debe ser **claro, específico y libremente otorgado,** y los interesados deben ser informados sobre los riesgos asociados con la transferencia de datos a países que puedan no proporcionar un nivel adecuado de protección.

SEGURIDAD DE LA TRANSFERENCIA

Se deben implementar medidas adecuadas para **garantizar la seguridad de la transferencia de datos personales** fuera del área geográfica del país y la UE. Esto puede incluir el uso de cifrado, el anonimato o seudonimato de datos, y el establecimiento de políticas y procedimientos de seguridad robustos.

TRANSPARENCIA Y DIVULGACIÓN

Los interesados deben ser **informados de manera clara y transparente sobre cualquier transferencia de sus datos personales** fuera del área geográfica del país y la UE, así como sobre los mecanismos utilizados para garantizar la protección de sus datos.

REGISTRO Y DOCUMENTACIÓN

Es importante mantener **registros y documentación adecuados de todas las transferencias de datos personales** fuera del área geográfica del país y la UE, así como de los mecanismos utilizados para garantizar la protección de esos datos. Esto puede ser útil en caso de auditorías o investigaciones regulatorias.

INCIDENTES DE SEGURIDAD Y BRECHAS DE DATOS

Los protocolos para la detección, gestión y notificación de incidentes de seguridad y brechas de datos son fundamentales para garantizar la protección de la información y el cumplimiento de las leyes de privacidad de datos. Aquí hay algunos elementos clave que podrías considerar incluir en tu política de protección de datos:

DETECCIÓN DE INCIDENTES DE SEGURIDAD Y BRECHAS DE DATOS

Para garantizar la seguridad de los datos, es crucial implementar **sistemas de monitoreo continuo de la red y los sistemas,** detectando así cualquier actividad inusual o sospechosa. Esto se logra mediante el uso de herramientas como las de detección de intrusiones (IDS) y prevención de intrusiones (IPS), las cuales identifican posibles amenazas.

Además, se deben establecer alertas automáticas que notifiquen al equipo de seguridad sobre posibles incidentes, permitiendo una respuesta rápida y efectiva ante cualquier situación de riesgo.

GESTIÓN DE INCIDENTES

Para asegurar una respuesta eficaz ante cualquier violación de seguridad o brecha de datos, es fundamental **designar un equipo de respuesta a incidentes.** Este equipo debe estar capacitado y preparado para actuar rápidamente. Se debe elaborar un plan detallado de respuesta a incidentes que incluya los pasos a seguir, como la evaluación de la situación, la contención de la brecha y la recuperación de los datos afectados.

Asimismo, es esencial asignar roles y responsabilidades claras dentro del equipo para garantizar una coordinación efectiva durante la gestión del incidente.

NOTIFICACIÓN DE INCIDENTES Y BRECHAS DE DATOS

Es imperativo **cumplir con los requisitos legales y regulatorios** relacionados con la notificación de incidentes de seguridad y brechas de datos. Para ello, es necesario establecer procedimientos claros que permitan notificar de manera adecuada a las autoridades de protección de datos y a los individuos afectados en caso de una violación de seguridad o una brecha de datos.

Esto incluye **determinar los plazos de notificación y los contenidos mínimos que deben incluirse en las notificaciones,** tales como la descripción del incidente, el tipo de datos comprometidos y las medidas tomadas para mitigar el impacto.

ANÁLISIS POST-INCIDENTE

Tras cada incidente, es crucial llevar a cabo un **análisis exhaustivo para identificar las causas subyacentes y extraer lecciones importantes.** Este análisis post-incidente proporciona información valiosa que se utiliza para mejorar los controles de seguridad y prevenir futuros incidentes. Así, se aprovechan las experiencias pasadas para fortalecer la protección de los datos y evitar posibles vulnerabilidades en el futuro.

FORMACIÓN Y CONCIENCIACIÓN

Para reducir el riesgo de incidentes causados por errores humanos, es esencial proporcionar **formación regular sobre seguridad de la información y buenas prácticas de seguridad** a todos los empleados. Esta formación les permite estar al tanto de los riesgos de seguridad y cómo mitigarlos.

Además, es crucial fomentar una cultura de seguridad en toda la organización, donde los empleados se sientan responsables de proteger los datos de la empresa y estén comprometidos con la seguridad en todos los niveles.

REVISIÓN Y ACTUALIZACIÓN PERIÓDICA

Revisar y actualizar periódicamente los protocolos de detección, gestión y notificación de incidentes para mantenerse al día con las amenazas emergentes y los cambios en las leyes y regulaciones de protección de datos.

Consideramos que con la implementación de estos protocolos y procedimientos, nos convertimos en una organización mejor preparada para detectar, gestionar y notificar de manera efectiva cualquier incidente de seguridad o brecha de datos que pueda ocurrir.

FORMACIÓN Y CONCIENCIACIÓN

Nuestra política de protección de datos incluye programas de formación y concienciación para el personal sobre prácticas de protección de datos y privacidad. Consideramos estos programas fundamentales para garantizar que todos los empleados comprendan la importancia de proteger la información confidencial y cumplan con las leyes y regulaciones de protección de datos pertinentes.

SENSIBILIZACIÓN SOBRE LA IMPORTANCIA DE LA PROTECCIÓN DE DATOS

Un documento de sensibilización sobre la importancia de la protección de datos es un recurso que tiene como objetivo educar a las personas sobre la relevancia de salvaguardar la información personal y confidencial contra accesos no autorizados, pérdidas o uso indebido.

Hacer un documento de sensibilización sobre la importancia de la protección de datos para una escuela es fundamental por varias razones:

1. **Proteger la privacidad de los estudiantes:** Los datos personales de los estudiantes, como sus nombres, direcciones, registros académicos y de salud, deben ser manejados con cuidado y protegidos contra accesos no autorizados. Un documento de sensibilización ayuda a concienciar al personal sobre la importancia de salvaguardar esta información confidencial.

2. **Cumplir con las regulaciones:** Las escuelas están sujetas a regulaciones de protección de datos, como FERPA en los Estados Unidos o el GDPR en la Unión Europea. Es esencial que el personal escolar esté al tanto de estas regulaciones y entienda sus responsabilidades para cumplir con ellas.

3. **Prevenir incidentes de seguridad de datos:** La concienciación sobre la importancia de la protección de datos ayuda a prevenir incidentes de seguridad, como brechas en sistemas informáticos, pérdida de dispositivos electrónicos o divulgación no autorizada de información confidencial. Al educar al personal sobre las mejores prácticas de seguridad, se reduce el riesgo de que ocurran estos incidentes.

4. **Fomentar una cultura de privacidad:** Al hacer hincapié en la importancia de la protección de datos, las escuelas pueden fomentar una cultura de privacidad en toda la comunidad educativa. Esto incluye no solo al personal, sino también a los estudiantes y a los padres, quienes deben entender la importancia de proteger su información personal y respetar la privacidad de los demás.

5. **Mantener la confianza de los padres y tutores:** Los padres y tutores confían en que la escuela protegerá adecuadamente la información personal de sus hijos. Al demostrar un compromiso con la protección de datos a través de la sensibilización y la capacitación, la escuela puede mantener la confianza de los miembros de la comunidad escolar.

A continuación, incluimos el documento de sensibilización sobre importancia de la protección de datos que hemos generado para nuestra escuela:

SENSIBILIZACIÓN SOBRE LA IMPORTANCIA DE LA PROTECCIÓN DE DATOS

POLÍTICAS Y PROCEDIMIENTOS INTERNOS

Los empleados deben estar familiarizados con las políticas y procedimientos internos de la organización relacionados con la protección de datos. Esto puede incluir cómo manejar los datos de manera segura, cómo responder a solicitudes de acceso a datos por parte de los individuos y cómo informar sobre posibles brechas de seguridad.

MANEJO SEGURO DE DATOS

Se deben proporcionar pautas claras sobre cómo manejar los datos de manera segura en todas las etapas de su ciclo de vida, desde la recopilación hasta la eliminación. Esto puede incluir el uso de contraseñas seguras, el cifrado de datos sensibles, la restricción de acceso a la información confidencial y la eliminación segura de datos obsoletos.

CAPACITACIÓN ESPECÍFICA PARA FUNCIONES

Dependiendo de las responsabilidades de cada empleado, puede ser necesario proporcionar capacitación específica sobre cómo cumplir con las regulaciones de protección de datos en su función particular. Por ejemplo, los empleados de recursos humanos pueden necesitar capacitación adicional sobre cómo manejar datos de empleados de manera segura.

PRUEBAS Y EVALUACIÓN

Los programas de formación deben incluir **pruebas o evaluaciones para garantizar que los empleados comprendan los conceptos clave** y estén cumpliendo con las políticas y procedimientos de protección de datos de la organización.

Algunas pruebas o evaluaciones que podrían garantizar que los empleados comprendan los conceptos clave en una escuela son las siguientes:

- **Estudios de caso:** Presentar situaciones hipotéticas o reales que el personal podría enfrentarse en su trabajo diario y pedirles que apliquen los conceptos clave para resolver problemas o tomar decisiones.

- **Simulaciones:** Organizar ejercicios prácticos donde el personal interactúe con escenarios de la vida real, como simulaciones de aula, reuniones de padres y maestros, situaciones de disciplina estudiantil, etc.

- **Observaciones en el aula:** Observar a los empleados mientras enseñan o interactúan con los estudiantes y proporcionar retroalimentación específica sobre su aplicación de los conceptos clave en un entorno práctico.

- **Entrevistas:** Realizar entrevistas individuales o grupales donde se les hagan preguntas relacionadas con los conceptos clave y se les pida que expliquen cómo aplicarían esos conceptos en situaciones específicas.

- **Evaluaciones en línea:** Utilizar plataformas en línea para administrar cuestionarios o pruebas que cubran los conceptos clave y proporcionen retroalimentación inmediata sobre el desempeño de los empleados.

ACTUALIZACIÓN CONTINUA

Dado que las leyes y regulaciones de protección de datos pueden cambiar con el tiempo, es importante proporcionar capacitación continua y **mantener a los empleados informados sobre cualquier cambio relevante en las políticas** y procedimientos de protección de datos.

Implementando programas de formación y concienciación efectivos sobre protección de datos, garantizamos que todos los empleados estén comprometidos en proteger la información confidencial y cumplir con las regulaciones de protección de datos aplicables.

REVISIONES Y ACTUALIZACIONES

Nuestra política de protección contempla procedimientos claros para revisar y actualizar la misma en respuesta a cambios legislativos, tecnológicos o institucionales.

MONITOREO DE CAMBIOS LEGISLATIVOS

Designar a un equipo o persona responsable de monitorear de manera regular los cambios en las leyes y regulaciones relacionadas con la protección de datos en la jurisdicción relevante. Esto puede incluir leyes de privacidad, regulaciones específicas de la industria y cualquier otra normativa pertinente.

EVALUACIÓN DE IMPACTO

Realizar evaluaciones de impacto de manera periódica para determinar si los cambios legislativos tienen algún impacto en las políticas y prácticas de protección de datos de la organización.

ANÁLISIS DE RIESGOS TECNOLÓGICOS

Mantener un proceso continuo de análisis de riesgos relacionados con la tecnología utilizada para el manejo y procesamiento de datos. Esto puede implicar revisar regularmente las medidas de seguridad tecnológica y evaluar si son adecuadas para proteger los datos de acuerdo con los estándares actuales.

REVISIÓN POR PARTE DEL EQUIPO DE CUMPLIMIENTO

Establecer un equipo de cumplimiento o función similar dentro de la organización que sea responsable de revisar periódicamente la política de protección de datos y asegurarse de que cumpla con las normativas aplicables y las mejores prácticas de la industria.

CONSULTAR CON EXPERTOS LEGALES

Mantener un contacto regular con abogados especializados en protección de datos para obtener asesoramiento sobre cambios legislativos y cómo afectan a la política de protección de datos de la organización.

CAPACITACIÓN Y CONCIENTIZACIÓN

Proporcionar capacitación regular a todos los empleados sobre los cambios en las políticas y procedimientos de protección de datos, así como sobre las implicaciones legales y éticas de estos cambios.

DIVULGACIÓN DE ACTUALIZACIONES

Comunicar claramente cualquier cambio en la política de protección de datos a todas las partes interesadas relevantes, incluidos empleados, clientes, proveedores y otras partes externas que puedan verse afectadas.

AUDITORÍAS INTERNAS

Realizar auditorías internas de manera regular para asegurarse de que la política de protección de datos se esté implementando de manera efectiva y que se estén siguiendo los procedimientos establecidos.

REVISIONES PERIÓDICAS

Establecer un calendario para revisar la política de protección de datos en intervalos regulares (por ejemplo, anualmente o cada dos años) para garantizar que siga siendo relevante y efectiva en la protección de la privacidad de los datos de la organización y de las personas involucradas.

CUMPLIMIENTO Y SANCIONES

El incumplimiento de la política de protección de datos puede tener diversas consecuencias, que pueden variar dependiendo de las leyes y regulaciones específicas en cada jurisdicción. Sin embargo, algunas de las posibles consecuencias incluyen:

MULTAS ECONÓMICAS: Las autoridades de protección de datos pueden imponer multas significativas por incumplimiento de las leyes de protección de datos. Estas multas pueden ser proporcionales a la gravedad de la violación y al tamaño de la organización.

ACCIONES LEGALES POR PARTE DE LOS AFECTADOS: Las personas cuyos datos se ven comprometidos debido al incumplimiento de la política de protección de datos pueden emprender acciones legales contra la organización responsable. Esto podría resultar en costos adicionales para la organización en términos de compensación y honorarios legales.

DAÑO A LA REPUTACIÓN: El incumplimiento de las leyes de protección de datos puede dañar la reputación de una organización, lo que a su vez puede afectar la confianza del público, la percepción de la marca y las relaciones con los clientes y socios comerciales.

PROHIBICIÓN DE PROCESAMIENTO DE DATOS: Las autoridades pueden imponer prohibiciones al procesamiento de datos como medida correctiva por incumplimiento grave de la política de protección de datos. Esto podría afectar significativamente las operaciones comerciales de una organización.

AUDITORÍAS Y SUPERVISIÓN ADICIONALES: Las autoridades pueden imponer auditorías y supervisión adicionales a una organización como parte de las medidas para garantizar el cumplimiento futuro de las leyes de protección de datos.

El incumplimiento de la política de protección de datos comporta serias consecuencias legales, financieras y de reputación para una organización. Por lo tanto, es fundamental que las organizaciones tomen las medidas necesarias para cumplir con las leyes y regulaciones de protección de datos aplicables. Esto incluye implementar políticas y procedimientos adecuados, capacitar al personal, realizar evaluaciones de riesgos de manera regular y mantenerse al tanto de los cambios en las leyes y regulaciones de protección de datos.

ANEXOS

A continuación, incluimos un conjunto de documentos de ejemplo que podrían formar parte de una política de protección de datos para una escuela.

Autoritat Catalana de Protecció de Dades	Pautas de protección de datos para los centros educativos
Agencia española de protección de datos	Guía para Centros Educativos de la AEPD
Formulario derecho de acceso AEDP	formulario-derecho-de-acceso.pdf