Análisis de Impacto en la Privacidad (PIA) - Secdata

Sección: 005D

Integrantes:

- Miguel Rubio Hoskins
- Martin Del Rio

Docente:

- Guillermo Pinto.

-

Contenido

1. Identificación de Procesos, Proyectos y/o Sistemas de Información Susceptibles de Riesgo

Secdata es un proyecto que se desarrollará con el manejo de datos personales es por esto que surge la necesidad de cubrir cualquier problemática al riesgo de la privacidad.

Datos Personales Críticos:

Nombre completo, RUT (Número de Identificación), Dirección, Teléfono, Correo electrónico u otros **datos sensibles** (como preferencias o información financieras según la ley).

Datos Sensibles :

Información Financiera, Diagnósticos Médicos, Creencias Creencias, Datos de Origen Étnico o Racial, Información sobre Vida Sexual,Datos Relacionados con Localización Geográfica y Datos sobre Hábitos de Consumo y Preferencias Personales.

Riesgos :

1) Intercepciòn de datos. Si los datos son enviados a través de conexiones no seguras, un hacker podría robar información.
2) Almacenamiento de datos sin autorización. Si los usuarios no están bien informados sobre qué datos recolectar y cual es el propósito de la acción, existe un riesgo de recolección de datos sin consentimiento.
3) Acceso no autorizado de los datos recolectados.
4) Los datos que se almacenan en servidores sin medidas de encriptación o con contraseñas débiles son vulnerables a ataques.
5) Inexistencia de políticas sobre la retención de datos a corto plazo.
6) Procesamiento de datos sin consentimiento.
7) Falta de trazabilidad, Si no se analiza ni se reporta el ciclo de vida del dato, hay una inexistencia de transparencia sobre el uso del dato.
8) Acceso indebido a datos anonimizados. Se podría identificar a las personas involucradas de los datos.
9) Exposición a los datos por falta de encriptación.
10) Eliminación incorrecta de los datos (Copias residuales).
11) Falta de cumplimiento con la Ley N° 19.628. No cumplir con los requisitos legales podría ocasionar sanciones.

2. Propósito, Objetivos y Alcance del PIA

El propósito del PIA es garantizar que Secdata cumpla con la Ley N° 19.628 y que los datos personales sean tratados de manera segura.

Objetivos :

Identificar los riesgos de privacidad, Evaluar las medidas de protección existentes y proponer nuevas medidas para mitigar los riesgos.

Alcance:

PIA incluye todas las etapas del ciclo de vida de los datos personales dentro del sistema.

3. Aprobación de la Autoridad

La aprobación del gerente de TI o del encargado de protección de datos de la organización es fundamental para llevar a cabo el análisis PIA. Se asegura que el análisis cuente con el apoyo necesario y los recursos adecuados para su desarrollo.

4. Establecimiento del Equipo de PIA

Equipo:

- Especialista en protección de datos.
- Desarrolladores de software.
- Experto en ciberseguridad o seguridad informática.
- Gerente ti

Este equipo trabajará en conjunto para recopilar datos, realizar el análisis y proponer soluciones para mitigar los riesgos.

5. Recopilación de Información Relevante para el Análisis

Se recopilaran datos personales que serán manejados por la solución Secdata, esto incluyen los datos personales sensibles y algunos críticos.

Mapeo flujo de datos dentro del sistema:

1) Recolección de datos :
    a) Entrada :
        i) Los usuarios proporcionan sus datos personales mediante un formulario en la solución web. También pueden incluir datos críticos.
    b) Sistema :
        i) Formularios web en django.
    c) Medidas de seguridad :

i) Uso de **HTTPS** para garantizar que la transmisión de datos esté encriptada.

2) Almacenamiento de datos :
    a) Entrada :
        i) Almacenamiento de datos en una base de datos protegida por técnicas de encriptación.
        ii) Esta base de datos es administrada por la solución web, la cual es la única con las claves para desencriptar los datos.
    b) Sistema :
        i) Base de datos encriptada (PostgreSQL o Sql Oracle).
    c) Medidas de seguridad:
        i) **Encriptación de datos en reposo** (AES-256 o similar).
        ii) **Control de acceso** mediante autenticación para administradores.
3) Procesamiento de datos y Consentimiento :
    a) Entrada :
        i) Cuando la empresa desee usar los datos personales, se envia solicitud de uso al individuo.
        ii) Usuario puede aceptar y rechazar el uso de sus datos a través de una notificación o correo electrónico.
    b) Sistema :
        i) **Gestión de consentimiento informado** a través de la aplicación de notificaciones de Django.
    c) Medidas de seguridad :
        i) **solicitudes de consentimiento** y generación de reportes del **ciclo de vida del dato** para auditar el uso de los datos.
4) Acceso a datos
    a) Entrada :
        i) La empresa puede acceder a datos personales anonimizados. Dependiendo del nivel de accesos y con el consentimiento obligatorio del usuario.
    b) Sistema :
        i) Anonimidad de los datos en la base de datos.
    c) Medidas :
        i) Control de acceso (Roles y permisos).
        ii) Técnicas de anonimidad y pseudonimización para garantizar que los datos puedan utilizarse de una forma segura.
5) Eliminación de datos :
    a) Entrada :
        i) Eliminación de datos cuando termine el tiempo establecido en el consentimiento del usuario.
    b) Sistema :
        i) Aplicación de eliminación en el proyecto de Django Framework.
    c) Medidas de seguridad :

i) Eliminación efectiva asegurando la nula recuperación de los datos.

6. Identificación de Amenazas, Vulnerabilidades y Controles de Privacidad

Las principales amenazas :

- Acceso no autorizado
- Fallos en la encriptación
- Uso indebido de los datos.

Vulnerabilidades :

- Configuraciones incorrectas de bases de datos.
- Fallas en los controles de acceso
- Falta de medidas de seguridad en la transmisión de datos.

Controles existentes :

- Encriptación y las auditorías de seguridad.

7. Herramientas de Evaluación

Para realizar el PIA, se utilizarán herramientas como plantillas de evaluación de riesgos y software especializado en protección de datos y ciberseguridad. Herramientas como OWASP ZAP o Burp Suite pueden ayudar a realizar pruebas de seguridad y detectar vulnerabilidades.

8. Evaluación y Aplicación de Buenas Prácticas

El análisis de impacto en la privacidad se llevará a cabo siguiendo buenas prácticas de seguridad, como el uso de encriptación avanzada, autenticación multifactor y auditorías periódicas. Se evaluará el cumplimiento de la Ley N° 19.628 en cada fase del manejo de datos.

9. Gestión de Riesgos de la Privacidad y Planes de Tratamiento

Una vez identificados los riesgos, se elaborarán planes de tratamiento que incluyan la implementación de nuevas medidas de seguridad, actualizaciones a las políticas de manejo de datos, y controles adicionales. Cada plan de tratamiento asignará responsabilidades específicas para su implementación.