Medidas de protección de datos desde el Diseño

Minimizar:

- Diseño de un formulario adaptado a los datos necesarios para el tratamiento de los datos, evitando la recogida de datos innecesarios.
- Pseudoanonimización de los datos almacenados en la base de datos y en alguno de los subprocesos del tratamiento.

Ocultación:

- Pseudoanonimización de los datos almacenados en la base de datos y en alguno de los subprocesos del tratamiento.
- Control de la privacidad de los metadatos en las comunicaciones electrónicas
- Cifrado de la información almacenada o en tránsito

Separación:

- Particionamiento por atributos de las bases de datos.
- Compartimentación del acceso a los datos en el tiempo.

Agregación:

- Agregación de registros
- Aplicación de diferenciales de privacidad en la difusión/acceso a los resultados del tratamiento

Información:

- Transparencia de la extensión del tratamiento para el sujeto de los datos
- Transparencia sobre el momento en el que se está realizando una recogida de datos

Control:

- Cifrado de la información extremo-extremo

Cumplimiento:

- Fijar requisitos de privacidad en los productos/servicios adquiridos o encargados para su desarrollo.
- Implementar procedimientos para garantizar la autenticidad o calidad de datos.
- Configuraciones de privacidad máximas por defecto.

Medidas de Seguridad y de gestión de brechas de datos personales

1. Almacenar los datos por periodos superiores a los necesarios para la finalidad del tratamiento y a la legislación vigente:

a) Creación y actualización del registro de actividades del tratamiento.

b) Identificación de la finalidad del tratamiento

2. Error en la configuración de un sistema, aplicación, estación de trabajo, impresora o componente de red:

a) Mantenimiento de los equipos

b) Gestión de cambios

c) Gestión de las vulnerabilidades técnicas

3. Fallas de seguridad en desarrollos de una nueva aplicación o de nuevas funcionalidades y/o parches de una aplicación ya existente:

a) Separación de entornos de desarrollo, prueba y producción

b) Política de desarrollo seguro de software

c) Seguridad en entornos de desarrollo

d) Pruebas de aceptación

e) Notificación de los eventos de seguridad de la información

f) Respuesta a los incidentes de seguridad

g) Notificación de los eventos de seguridad a la Autoridad competente e interesados

h) Recopilación de evidencias

4. Errores humanos en tareas de mantenimiento

a) Concienciación, educación y capacitación en seguridad de la información

b) Uso aceptable de los activos

c) Mantenimiento de los equipos

5. Robo o extravío de equipos, soportes o dispositivos con datos personales

a) Formación y capacitación en materia de protección de datos

b) Concienciación, educación y capacitación en seguridad de la información

c) Gestión de altas / bajas en el registro de usuarios

d) Gestión de los derechos de acceso con privilegios especiales

e) Revisión de los derechos de acceso de los usuarios

f) Retirada o adaptación de los derechos de acceso

g) Uso de información confidencial para la autenticación

h) Restricción del acceso a la información

i) Procedimientos seguros de inicio de sesión

j) Recopilación de evidencias

k) Notificación de los eventos de seguridad a la Autoridad competente e interesados

l) Respuesta a los incidentes de seguridad

m) Notificación de los eventos de seguridad de la información

n) Seguridad de oficinas, despachos y recursos

o) Controles físicos de entrada

6. Información no actualizada o incorrecta (pe. registros duplicados con informaciones contradictorias o con campos de datos incorrectos)

a) Gestión de altas / bajas en el registro de usuarios

b) Gestión de los derechos de acceso con privilegios especiales

c) Revisión de los derechos de acceso de los usuarios

d) Retirada o adaptación de los derechos de acceso

e) Copias de seguridad de la información

f) Integridad de la información en la entrada, almacenamiento y procesamiento de los datos de los datos

7. Acceso a una información, servicios, aplicaciones o dispositivos de forma no consentida, por personas no autorizadas, traspasando de barreras (Hacking)

a) Política de control de accesos

b) Gestión de altas / bajas en el registro de usuarios

c) Gestión de los derechos de acceso con privilegios especiales

d) Revisión de los derechos de acceso de los usuarios

e) Retirada o adaptación de los derechos de acceso

f) Recopilación de evidencias

g) Notificación de los eventos de seguridad a la Autoridad competente e interesados

h) Respuesta a los incidentes de seguridad

i) Notificación de los eventos de seguridad de la información

8. Manipulación o modificación no autorizada de la información

a) Segregación de tareas

b) Política de control de accesos

c) Gestión de altas / bajas en el registro de usuarios

d) Gestión de los derechos de acceso con privilegios especiales

f) Retirada o adaptación de los derechos de acceso

g) Revisión de los derechos de acceso de los usuarios

9. Existencia de errores técnicos o fallos que ocasionen una indisponibilidad de los sistemas de información

a) Recopilación de evidencias

b) Notificación de los eventos de seguridad a la Autoridad competente e interesados

c) Notificación de los eventos de seguridad de la información

d) Disponibilidad de instalaciones para el procesamiento de la información

e) Planificación de la continuidad de la seguridad de la información

f) Implantación de la continuidad de la seguridad de la información

10. Catástrofes naturales que afectan a las infraestructuras (inundaciones, huracanes, terremotos, etc.)

a) Protección contra las amenazas externas y ambientales

11. Deficiencias en los protocolos de almacenamiento de los datos personales en formato físico

a) Seguridad de oficinas, despachos y recursos

b) Controles físicos de entrada

Reevaluación del riesgo

En la siguiente tabla se adjuntan algunos ejemplos de factores que podrían ser utilizados para determinar cuándo es necesario realizar la revisión del nivel de riesgo:

Naturaleza:

- Cambios en la identidad del responsable.
- Cambios en la implementación del tratamiento.
- Cambios o actualización de elementos tecnológicos.
- Sustitución de elementos humanos por elementos técnicos.
- Cambios sustanciales en los elementos organizativos.
- Cambios sustanciales en los encargos de tratamiento.
- Detección de falta de eficacia en las medidas y garantías incluidas en el tratamiento.

Ámbito:

- Cambio en la extensión del tratamiento.
- Modificación en las categorías de los datos recogidos.
- Cambio en el volumen de los datos recogidos.
- Cambio en la frecuencia de la recogida de datos.
- Modificación del alcance (temporal o espacial).

Contexto:

- Cambios importantes en los objetivos de la organización, sus modelos de gobernanza o su cultura.
- Cambio en las situaciones que justificaron el tratamiento.
- Ocurrencia de incidencias y brechas que se han producido en el tratamiento o tratamientos similares.
- Evolución del modelo de amenazas, las incidencias, las brechas o las tecnologías aplicables.
- Cambios en el volumen o tipología de solicitudes en el ejercicio de los derechos de los interesados.
- Cambios en los marcos o garantías jurídicas.
- Cambios en el marco normativo de aplicación.
- Cambios sociales, políticos, económicos o estratégicos.

Fines:

- Cambio o ampliación de los fines

Plan de acción de la gestión de riesgos

AMENAZA/RIESGO	REFERENCIA MEDIDA DE CONTROL	DESCRIPCIÓN DE LA MEDIDA DE CONTROL	RESPONSABLE DE LA IMPLANTACIÓN	FECHA PREVISTA
Error en la configuración de un sistema **Errores humanos**	2.a, 4.c	Mantenimiento de los equipos	Miguel Caurin Perpiñá	01/01/2023
Fallas de seguridad	3.a	Separación de entornos de desarrollo, prueba y producción	Pere Caimari Fuster	01/02/2023
Fallas de seguridad	3.b	Política de desarrollo seguro de software	Mireia Risueño Guillot	01/12/2022
Errores técnicos	9.f	Implantación de la continuidad de la seguridad de la información	Pablo Gómez Martínez	01/12/2022
Errores humanos **Robo o extravío de equipos**	4.a,5.b	Concienciación, educación y capacitación en seguridad de la información	Amparo Gálvez Vilar	01/12/2022

Robo o extravío de equipos con datos personales **Información no actualizada o incorrecta** **Hacking** **Manipulación o modificación no autorizada de la información**	5.e,6.c,7.d,8.g	Revisión de los derechos de acceso de los usuarios	Pablo Gómez Martínez	01/02/2023
Robo o extravío de equipos con datos personales **Información no actualizada o incorrecta** **Hacking** **Manipulación o modificación no autorizada de la información**	5.c,6.a,7.b,8.c	Gestión de altas / bajas en el registro de usuarios	Pere Caimari Fuster	01/12/2022
Robo o extravío de equipos con datos personales	5.a	Formación y capacitación en materia de protección de datos	Mireia Risueño Guillot	01/12/2022
Robo o extravío de equipos con datos personales **Información no actualizada o incorrecta** **Hacking** **Manipulación o modificación no autorizada de la información**	5.d,6.b,7.c,8.d	Gestión de los derechos de acceso con privilegios especiales	Pere Caimari Fuster	01/12/2022

Robo o extravío de equipos con datos personales **Información no actualizada o incorrecta** **Hacking** **Manipulación o modificación no autorizada de la información**	5.f,6.d,7.e,8.f	Retirada o adaptación de los derechos de acceso	Miguel Caurin Perpiñá	01/01/2023
Errores técnicos	9.e	Planificación de la continuidad de la seguridad de la información	Amparo Gálvez Vilar	01/12/2022
Información no actualizada o incorrecta	6.e	Copias de seguridad de la información	Pere Caimari Fuster	15/12/2022
Fallas de seguridad **Robo o extravío de equipos con datos personales** **Hacking** **Errores técnicos**	3.e, 5.m, 7.i, 9.c	Notificación de los eventos de seguridad de la información	Amparo Gálvez Vilar	01/12/2022
Fallas de seguridad **Robo o extravío de equipos con datos personales** **Hacking** **Errores técnicos**	3.g, 5.k, 7.g, 9.b	Notificación de los eventos de seguridad a la Autoridad competente e interesados	Mireia Risueño Guillot	01/12/2022
Fallas de seguridad **Robo o extravío de equipos con datos personales** **Hacking**	3.f,5.l,7.h	Respuesta a los incidentes de seguridad	Pablo Gómez Martínez	01/12/2022
Catástrofes naturales que afectan a las infraestructuras	10.a	Protección contra las amenazas externas y ambientales	Miguel Caurin Perpiñá	01/12/2022