Data Privacy Officer

(Responsable de Protección de Datos)

FUNCIONES

Misión:

Vigilar por el cumplimiento, dentro de la entidad, de las directrices de protección de datos.

En particular el papel será, garantizar la idoneidad de las políticas de protección de datos actuales de la entidad y actualización cuando sea necesario, para el correcto funcionamiento y cumplimiento dentro de la misma.

Mejores prácticas:

- El Data Privacy Officer implementará los procedimientos e instrucciones de trabajo en la seguridad en el tratamiento de datos.
  - Elaboración del *business plan de la seguridad del tratamiento.*
- En forma permanente el Data Privacy Officer, será el encargado de controlar todos los problemas internos de la organización, manteniendo un registro y control de las incidencias.
  - Informes de Impacto de Privacidad.
- El Data Privacy Officer debe ser consciente de cualquier problema e incidencia que presente un riesgo de reputación o material.
- El Data Privacy Officer se asegurará de una concienciación adecuada, en protección de datos, que debe llevar todo el personal de la entidad.
- El Data Privacy Officer trabajará constantemente y eficazmente, en la consecución e implantación dentro de la entidad, de directrices sobre mejores prácticas. Realización periódica y evaluación de riesgos de seguridad y llevar a cabo las actividades en curso de supervisión y funciones de auditoría
- El Data Privacy Officer debe garantizar el cumplimiento de las normas del grupo dentro de la entidad.
- El Data Privacy Officer se responsabilizará de la implantación y mantenimiento del futuro certificado basado en el Sello Europrise ("European Privacy Seal").
- El Data Privacy Officer perseverará en la Mejora Continua.

Responsabilidades claves:

- Garantizar cumplimiento de legislación de protección de datos y, en su caso, las regulaciones de comercio electrónico dentro de la entidad.
- Creación, actualización y difusión de las políticas de protección de datos.
- Elaboración de nuevas políticas si fuese necesario.
- Resolución de consultas *ad hoc* y las cuestiones relativas a la protección de datos.
- Determinación de datos información y protección de las cuestiones de seguridad que deben abordar, en particular en relación a los proveedores, clientes, empleados y sistemas informáticos, y asegurar la necesaria aprobación y recursos para abordar esas cuestiones.
- Gestión de la protección de datos y programa de seguimiento de la seguridad de información.
  a. Acciones organizativas.
  b. Técnicas.
  c. Acciones preventivas.
  d. Detectivas.
  e. Correctivas.
  f. Plan de auditorías.
- Gestión de solicitudes de acceso y control de las mismas, en materia de protección de datos.
- Mantener registro actualizado del Documento de Seguridad y tenerlo a disposición de la AEPD.
- Implementación de controles para el cumplimiento de la legislación de protección de datos vigente.

- Elaboración de normas de auditoría para el tratamiento de datos personales y actividades de seguridad de la información para asegurar el cumplimiento interno de la entidad.
    - *Privacidad por Diseño.*
    - *Privacidad por Defecto.*
- Enlace con los equipos pertinentes para poner a prueba la capacidad de la empresa para responder a una ruptura u otras contingencias graves en sus operaciones que afecta a la seguridad de la información y datos de carácter personal tanto de información automatizada como no automatizada.
- Mantener un registro de activos de información al día.
- Establecimiento y seguimiento de acuerdos de intercambio de información.
- Realizar evaluaciones de riesgo como parte del sistema de gestión de seguridad de información y su mantenimiento.
- Investigar y responder a violaciones de seguridad y reportando las brechas en el sistema de seguridad a la gerencia de la entidad.
- Garantizar que se cumplen los objetivos del proyecto.
- Colaborar con otros departamentos, tales como el cumplimiento corporativo, contabilidad, informática, medios electrónicos, registros médicos y de organización para mantener el cumplimiento con las leyes vigentes relacionadas con la privacidad, la seguridad, las transacciones electrónicas y la protección de los recursos de información.
- Informar periódicamente a la dirección sobre el estado de cumplimiento de la privacidad.
- Transferencia Internacional de Datos, comprobación con el país destinatario de un adecuado nivel de protección o existencia de una Autoridad de Control (para países de fuera de la Unión Europea).

Principal misión:

- Mantener la integridad de toda la entidad en materia de seguridad y de protección de datos.
- Desarrollo, supervisión posterior a la implementación por asegurar el cumplimiento con los códigos de regulación de la práctica, la legislación y las políticas internas de la entidad.
- Proteger a los intereses de la organización, en particular su acreditación en la reglamentación vigente.

El alcance del trabajo del equipo necesariamente cubre la totalidad de la organización, incluyendo:

- Proveedores
- Clientes
- Empleados

Desafíos clave:

- Implementar y/o incorporar nuevas políticas y métodos de trabajo.
- Trabajar y gestionar, conjuntamente con la ejecutiva de la entidad e implicación de la misma.
- Controlar que los empleados de la entidad tienen la formación y capacitación que necesiten para entender sus obligaciones en protección de datos.
- Establecer y crear un plan formativo.
- Iniciar y promover actividades para fomentar la concienciación sobre la seguridad, la privacidad y compliance dentro de la organización.

Normas de consulta:

Con la próxima aprobación del borrador de Protección de Datos de la Unión Europea, se determinará un sistema de normalización y certificación, queda por determinar si será a nivel nacional o internacional, en el cual se establecerán los diferentes mecanismos para dicha certificación.

Por lo que el sistema de trabajo del Data Privacy Officer se adaptará al modelo de procesos, en inglés PDCA, lo que es lo mismo en español PHVA (Planificar, Hacer, Verificar, Actuar). Siguiendo las directrices de la familia de normas ISO/IEC 27000*.

- **Planear-Planificar**
- Se fijará la política, objetivos, procesos y procedimientos relevantes, para manejar el riesgo y mejorar la seguridad del tratamiento de los datos de acuerdo con las políticas y objetivos generales de la organización..
- **Hacer**
- Se implementarán la política, los controles, los procesos y procedimientos.
- **Chequear-Verificar**
- Se evaluará y medirá el desempeño del proceso en comparación con la política, objetivos y experiencias establecidas.
- **Actuar**
- Se adoptarán las acciones correctivas y preventivas, basadas en los resultados de la auditoría, juntamente con la revisión gerencial y cualquier otra información relevante con el fin de lograr la Mejora Continua.

Marco legal, normativas de seguridad:

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal (LOPD).
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de comercio electrónico (LSSI-ce).
- Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.
- Real Decreto Legislativo 1/1996, de 12 abril, por el que se aprueba el texto refundido de la Ley de propiedad Intelectual.
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Reforma del Código Penal en materia de Delitos Informáticos.

*Familia de normas ISO/IEC 27000.

- ISO/IEC 27000:2009
- ISO/IEC 27001:2007
- ISO/IEC 27002:2009
- ISO/IEC 27003:2010 (información acerca del uso del modelo PDCA).