OFICIAL DE PROTECCIÓN DE DATOS

Gustavo Landaeta Baeza

Universidad Mayor

Aspectos Legales y Regulatorios

Prof. Carlos Patricio Reusser

Junio 09, 2024

Índice

Introducción

En tiempos en donde la información esta al alcance de la gran parte de la población mundial existe

Rol y Atribuciones de un Oficial de Protección de Datos

¿Porque nace la figura del Oficial de Protección de datos?

La figura del Oficial de Protección de Datos (DPO, por sus siglas en inglés) o Delegado de Protección de Datos (DPD, siglas en español) surge como respuesta a diversas necesidades, circunstancias y hechos en el ámbito de la protección de datos considerados personales o sensibles. A medida que los estados y organizaciones van evolucionando en cuanto a la manipulación de información, es de vital importancia la aparición de una figura que sea capaz de conocer las aristas legales, procedimientos y normativas que la organización explote, guarde y resguarde. Entre los motivos principales de la necesidad de crear esta figura esta el Incremento de la regulación en cuanto a protección de datos, aumento de la conciencia pública sobre la privacidad, marcos legales referidos a los datos cada vez más complejos, fomento de la confianza que deben dar las organizaciones y sentido de responsabilidad y transparencia.

"Los datos sensibles o “especialmente protegidos” incluyen tipos de datos que se caracterizan por referir a aquellas esferas de la personalidad en que, si fueran mal utilizados por terceros, podrían prestarse para discriminaciones ilegales o arbitrarias, o conllevar graves riesgos para el interesado"(Lorena Donoso Abarca, 2021).

Por estos motivos a nivel internacional se destaca la figura del DPO en el Reglamento general de protección de datos (RGPD) Sección 4 artículos 37, 38 y 39 (Parlamento Europeo, 2016). Donde se evidencia la necesidad de las organizaciones a tener una figura encargada de velar por el cumplimiento de las reglas y garantizar la protección de los derechos de privacidad de los individuos.

Podemos destacar la ley de Sudáfrica "Protection of Personal Information Act (POPI Act)"(Law, 2024) que establece principios para el procesamiento de datos personales y requiere

que las organizaciones designen una figura a cargo de la proteccion de datos. En su articulo 55 define al Oficial de Información "Duties and responsibilities of Information Officer"(Law, 2021)

Por último podemos mencionar la ley PIPA (Ley de Protección Información Personal) de Corea del Sur(de Protección de Información Personal Corea del Sur, s.f.) , la cual es indicada como una de las leyes mas duras en cuanto a sanciones, aunque esta ley no obligue a adoptar la figura del DPO por el motivo de la rigurosidad de su ley las organizaciones optan por designar un encargado que cumple un rol muy similar al DPO (*PIPA de Corea del Sur | Entrust*, s.f.)

¿Cual es el rol y atribuciones de un Oficial de Protección de Datos?

El Oficial de Protección de Datos debe cumplir un rol fundamental en la organización. Ya que es la figura encargada de asegurar que exista una cultura de protección de datos dentro de la entidad a la cual desempeñe sus funciones. Debe garantizar que la privacidad de los datos sea un componente indispensable en el alcance de los objetivos relacionados con los datos bajo su responsabilidad. Es el asesor directo de la organización sobre cuestiones relacionadas con la protección de datos, esto incluye evaluaciones de impacto sobre la protección de datos, medidas adecuadas para mitigar los riesgos. Debe ser el supervisor principal de la organización velando por el cumplimiento de las leyes y regulaciones que vayan conformando los estados con respecto a protección de datos. Esto incluye en su rol el monitorizar constantemente las políticas de protección, revisión de practicas de procesamiento garantizando que se respeten los derechos de los interesados. Tiene un rol fundamental como punto de contacto, es decir que actúa como punto central de comunicación para los interesados(personas cuyos datos son procesados)y la autoridad que tenga las atribuciones del control de datos. Esto incluirá gestionar consultas y quejas de los interesados y colaborar con la autoridad de control para los casos de inspecciones o auditorias. Por ultimo debe ser la figura que organice y proporcione información al colaborador sobre sus obligaciones en

materia de protección de datos y fomento de la cultura de esta.

Las atribuciones serán las facultades o poderes que tendrá el DPO. Para el caso del Reglamento General de Datos(RGPD)(Parlamento Europeo, 2016, pg. L 119/56) Artículo 39, apartado 1 Indica una lista de funciones mínimas que tendrá el DPO:

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros.
- Supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35
- Cooperar con la autoridad de control
- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

Por estos ítems podemos concluir que el DPO debe tener acceso a toda la información de la organización que se estimen pertinentes como datos personales y tratamiento de estos. Debe ser independiente al desempeño de sus tareas. Ser participe de implementaciones nuevas referidas

a datos para salvaguardar el procesamiento y resguardo de estos. Poseer los recursos necesarios para poder llevar a cabo íntegramente su labor para poder reportar a las altas direcciones de la organización.

Perfil Profesional del Oficial de Protección de Datos

En el documento oficial del RGPD Articulo 37, apartado 5. Nos hace referencia del perfil que debe tener el DPO.“El delegado de protección de datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39“ (Parlamento Europeo, 2016, pg. L 119/55)

Conclusión

La ciberseguridad es un mundo amplio y dinámico, donde la detección y protección contra amenazas cibernéticas se ha transformado en prioridad en el último tiempo, convirtiéndose en una tarea vital para salvaguardar la integridad, confidencialidad y disponibilidad de sistemas, datos e información de las organizaciones. A lo largo del desarrollo este análisis exhaustivo, se exploraron múltiples herramientas y técnicas, las cuales son utilizadas en la identificación y guía de mitigación de riesgos en entornos digitales, desde el escaneo de red hasta la evaluación de vulnerabilidades y pruebas de malware. Uno de los principales hallazgos de este estudio es la importancia de comprender la estructura de la red y los puntos de entrada potenciales para amenazas. Las herramientas de escaneo de red proporcionan una visión detallada de la topología de la red, identificando dispositivos, puertos abiertos y servicios en ejecución, lo que permite a los profesionales de seguridad cibernética tomar medidas proactivas para fortalecer la seguridad de la red. Además, hemos explorado la evaluación de vulnerabilidades como un componente esencial en la estrategia de defensa cibernética. Estas herramientas avanzadas permiten detectar debilidades en la seguridad de los sistemas, proporcionando una evaluación detallada del riesgo y recomendaciones para su mitigación. Al abordar estas vulnerabilidades de manera proactiva, las organizaciones pueden fortalecer sus defensas cibernéticas y reducir la exposición a posibles amenazas. Por último, hemos examinado en las pruebas de malware como una medida crucial para simular escenarios de ataque y desarrollar estrategias de respuesta efectivas. A través de la simulación de infecciones y la exploración de técnicas de recuperación, los profesionales de seguridad pueden mejorar su capacidad para identificar, contener y eliminar amenazas, protegiendo así la integridad de los sistemas y la confidencialidad de los datos. En conclusión, este documento ofrece una visión integral y detallada de las prácticas y herramientas esenciales en la identificación y defensa contra amenazas cibernéticas. Al proporcionar una comprensión profunda de los conceptos y técnicas fundamentales en ciberseguridad, este

estudio ofrece una base sólida introductoria para la investigación y el desarrollo continuo en este campo crucial y en constante evolución.

Referencias

de Protección de Información Personal Corea del Sur, C. (s.f.). *Comisión de Protección de Información Personal.* https://www.privacy.go.kr/front/main/main.do.

Law, A. (2021, 6). *Section 55 Duties and responsibilities of Information Officer.* https://popia.co.za/section-55-duties-and-responsibilities-of-information-officer/.

Law, A. (2024, 1). *Protection of Personal Information Act (POPI Act) - POPIA.* https://popia.co.za/.

Lorena Donoso Abarca, C. R. M. (2021). *Derecho informático.* Santiago de Chile: Academia Judicial de Chile.

Parlamento Europeo. (2016). *Reglamento (ue) 2016/679 del parlamento europeo y del consejo de 27 de abril de 2016.* Diario Oficial de la Unión Europea. (L 119)

PIPA de Corea del Sur | Entrust. (s.f.). Descargado de `https://www.entrust.com/es/legal-compliance/hsm-solutions/apac/south-koreas-pipa`