UNIVERSIDAD BERNARDO O'HIGGINS

FACULTAD DE INGENIERÍA, CIENCIAS Y TECNOLOGÍA

Carrera de Ingeniería en Informática

Curso Diseño y Auditoría en Ciberseguridad

Prueba Unidad 3

Marco legal chileno

Profesor:

Miguel Castillo.

Estudiante:

Aldo Fernando Hernández Tamez

Examen de Desarrollo: Protección de Datos Personales

Instrucciones: Responda cada pregunta de manera concisa y clara, desarrollando los conceptos solicitados y citando las bases legales (Ley N°19.628 o referencias a los principios) que sustentan su respuesta.

Preguntas de Desarrollo (6 Preguntas)

1. Conceptos Fundamentales y Alcance (Definiciones)

Explique la diferencia esencial entre un **Dato Personal** y un **Dato Sensible**. Además, describa brevemente las dos condiciones que deben cumplirse para que una información sea calificada como Dato Personal según la Ley N°19.628.

R. Un **dato de carácter personal** se refiere a cualquier información concerniente a personas naturales, identificadas o identificables, mientras que un **dato sensible** son aquellos datos personales que se refieren a las características físicas o morales o a hechos o circunstancias de su vida privada o intimidad. Es decir, un dato personal es información relacionada a personas que puedan ser identificadas por dicho dato y los datos sensibles son datos personales que se refieren a características de las personas o circunstancias de su vida privada.

Las dos condiciones que deben cumplirse para que un dato sea calificado como **personal** son las siguientes:

1. Sea relevante para una persona, y
2. Permita identificar a dicha persona.

2. Principios de Licitud y Finalidad en Órganos Públicos

Defina qué es una **Brecha de Seguridad** (*Data Breach*) en el contexto de la protección de datos personales. Explique dos (2) de las obligaciones fundamentales que la **nueva Ley de Protección de Datos Personales** chilena impone a los Responsables del tratamiento de datos ante la ocurrencia de una Brecha de Seguridad, detallando a quién se debe notificar y la finalidad de esta notificación.

R. Según *IBM*, un *data breach* es cualquier incidente de seguridad en el que terceros sin autorización acceden a información sensible o confidencial, incluyendo datos personales y datos corporativos.

La **nueva Ley Chilena de Protección de Datos Personales** impone las siguientes obligaciones a los responsables del tratamiento de datos ante una brecha de seguridad:

1. Reportar a la Agencia (ANCI) las vulneraciones a las medidas de seguridad que ocasionaron la destrucción, filtración, pérdida o alteración accidental o ilícita de los datos personales que trate o la comunicación o acceso no autorizados a dichos datos, y

2. Registrar dichas comunicaciones describiendo la naturaleza de las vulneraciones, sus efectos, las categorías de datos y el número aproximado de titulares afectados y las medidas adoptadas para gestionarlas y precaver incidentes futuros.

Además, si dichas vulneraciones son datos personales sensibles, datos relativos a niños y niñas menores de catorce años o datos relativos a obligaciones de carácter económico, financiero, bancario o comercial, debe haccerse la comunicación a los titulares de los datos a través de sus representantes.

3. Derechos del Titular (Derechos ARCO y Novedades)

Describa el concepto y el objetivo de tres (3) de los derechos que el titular de los datos personales puede ejercer ante un organismo público (Responsable del tratamiento), según lo establecido en la Ley N°19.628 (ej. Acceso, Rectificación, Cancelación, Bloqueo). Adicionalmente, mencione y explique brevemente uno de los nuevos derechos considerados en la actualización de la Ley (ej. Portabilidad, Derecho al olvido).

R.

1) Acceso (Artículo 12)
    a) Toda persona tiene derecho a exigir a quien sea responsable de un banco que se dedique al tratamiento de datos personales, información sobre los datos relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente.
2) Rectificación (Artículo 12)
    a) En caso de que los datos personales sean erróneos, inexactos, equívocos o incompletos (y se acredite), toda persona tendrá derecho a que se modifiquen.
3) Cancelación (Artículo 12)
    a) Las personas pueden exigir que se eliminen sus datos en caso de que su almacenamiento carezca de fundamento legal o cuando estuvieren caducos.
4) Bloqueo (Artículo 12)
    a) Se podrá hacer cuando la persona haya proporcionado voluntariamente sus datos personales o ellos se usen para comunicaciones comerciales y no desee continuar figurando en el registro respectivo.
5) Portabilidad (Artículo 9)
    a) El titular de datos tiene derecho a solicitar y recibir una copia de los datos personales que le conciernen, que haya facilitado al responsable, en un formato electrónico estructurado, genérico y de uso común, que permita ser operado por distintos sistemas.

4. Modernización Regulatoria y Responsabilidad Proactiva

La nueva Ley de Protección de Datos Personales de Chile busca alinearse con estándares internacionales como el GDPR. Explique qué implica el **Principio de Responsabilidad Proactiva** (o *Accountability*) y cómo este principio transforma la obligación de las instituciones, pasando de una postura reactiva a una activa en el manejo y la gestión de riesgos asociados a los datos personales.

R. Es la obligación de que el responsable de los datos aplique medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento de los datos es conforme con el Reglamento, esto implica prácticamente que las organizaciones analicen qué datos tratan, con qué finalidad y qué tipo de operaciones llevan a cabo con ellos (básicamente que tengan más cuidado y sean más selectivos con la información personal que manejan).

Este principio exige una actitud consciente de las organizaciones acerca del tratado de datos, por lo que existe una postura activa (con protocolo y seguridad de la información) en caso de algún riesgo o brecha en lugar de una reactiva (que ocurra el ataque y después ver cómo solucionarlo).

Preguntas de Desarrollo sobre la Ley Marco de Ciberseguridad (Ley N° 21.663)

5. Principios Fundamentales y Seguridad como Bien Público

El Título I de la Ley establece los principios que rigen la ciberseguridad en Chile.

Mencione y desarrolle dos (2) de los principios rectores que establece la ley, explicando su significado en el contexto de la ciberseguridad. Finalmente, relacione estos principios con el objeto de la ley (Artículo 1°) y la concepción de la ciberseguridad como una función esencial y un bien que afecta directamente el interés público.

R.

1) Principio de control de daños
    a) Frente a un ciberataque o incidente, siempre se deberá actuar de manera coordinada y adoptar las medidas necesarias para evitar que el ciberataque escale y se propague a otros sistemas informáticos.
2) Principio de cooperación con la autoridad
    a) A fin de resolver incidentes de ciberseguridad, se deberá cooperar con la autoridad competente e incluso entre diferentes sectores si es necesario.

Estos principios permiten estructurar y coordinar las acciones de ciberseguridad de los organismos del Estado y entre éstos y los particulares, además de establecer los requisitos mínimos para la contención y respuesta a incidentes de ciberseguridad. Por otro lado, conciben a la ciberseguridad como una función esencial que afecta al interés público debido a que reiteran implícitamente la necesidad y urgencia de contener y resolver los incidentes relacionados a la ciberseguridad y manejo de datos personales de la población.

6. De las responsabilidades de la ANCI, defina las siguientes:

A. Estratégica y de Coordinación
B. Operativa y de Respuesta a Incidentes
C. Regulatoria y Fiscalizadora

R.

A. Coordinar y supervisar al CSIRT Nacional y a los demás pertenecientes a la Administración del Estado, establecer una coordinacion con el CSIRT de la Defensa Nacional, cooperar con organismos públicos e instituciones privadas, colaborar con los organismos integrantes del Sistema de Inteligencia del Estado en la identificación de amenazas y la gestión de incidentes o ciberataques que puedan representar un riesgo para la seguridad nacional, requerir a los organismos de la Administración del Estado y a las instituciones privadas señaladas en el artículo 4º acceso a la información estrictamente necesaria para prevenir la ocurrencia de incidentes de ciberseguridad o para gestionar uno que ya hubiera ocurrido. Para lo anterior, podrá requerir la entrega del registro de actividades de las redes y sistemas informáticos que permitan comprender detalladamente los incidentes de ciberseguridad que puedan haber ocurrido.
B. Aplicar e interpretar administrativamente las disposiciones legales y reglamentarias en materia de ciberseguridad, requerir a las entidades obligadas por la presente ley que hayan visto afectados sus servicios por un incidente de ciberseguridad o ciberataque, que entreguen a los potenciales afectados información veraz, suficiente y oportuna sobre su ocurrencia, conforme lo dispuesto en el literal g) del artículo 8º.
C. Dictar los protocolos y estándares que señala el artículo 7°; las instrucciones generales y particulares, de carácter obligatorio, para las instituciones, tanto públicas como privadas obligadas por la presente ley, y las demás disposiciones necesarias para la aplicación y el cumplimiento de esta ley y sus reglamentos, fiscalizar el cumplimiento de las disposiciones de esta ley y sus reglamentos, y de los protocolos, estándares técnicos e instrucciones generales y particulares que emita la Agencia en ejercicio de las atribuciones conferidas en la ley, instruir el inicio de procedimientos sancionatorios y sancionar las infracciones e incumplimientos en que incurran las instituciones obligadas por la presente ley respecto de sus disposiciones y reglamentos y de las instrucciones generales y particulares que emita la Agencia.

Bibliografía

Gobierno de Chile. (1999). *Ley N.º 19.628 sobre protección de la vida privada*. Biblioteca del Congreso Nacional de Chile. https://www.bcn.cl/leychile/navegar?idNorma=141599

Gobierno de Chile. (2024). *Ley N.º 21.719 que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales*. Biblioteca del Congreso Nacional de Chile. https://www.bcn.cl/leychile/navegar?idNorma=1209272

Gobierno de Chile. (2024). *Ley N.º 21.663, Ley Marco de Ciberseguridad*. Biblioteca del Congreso Nacional de Chile. https://www.bcn.cl/leychile/navegar?idNorma=1202434

Kosinski, M. (2024). *What is a data breach?* IBM. https://www.ibm.com/think/topics/data-breach

Agencia Española de Protección de Datos. (s. f.). ¿Qué es el principio de responsabilidad proactiva? https://www.aepd.es/preguntas-frecuentes/2-tus-obligaciones-como-responsable-del-tratamiento/4-los-principios-del-tratamiento/FAQ-0208-que-es-el-principio-de-responsabilidad-proactiva