consejo para la Transparencia

OFICIO N° 001809

MAT.: Remite recomendaciones en materia de protección de datos carácter personal y seguridad de la información, en relación con la filtración de información contenida en archivos administrados por Carabineros de Chile.

ANT.: No hay

ADJ.: Informe filtración de base de datos de Carabineros de Chile, de fecha 21 de noviembre de 2019.

Santiago, 22 NOV 2019

A: GENERAL MARIO ROZAS CÓRDOVA
GENERAL DIRECTOR
CARABINEROS DE CHILE

DE: ANDREA RUIZ ROSAS
DIRECTORA GENERAL
CONSEJO PARA LA TRANSPARENCIA

1. Que, conforme a las facultades de formular recomendaciones y de velar por el adecuado cumplimiento de la Ley N°19.628, sobre Protección de la Vida Privada, por parte de los órganos de la Administración del Estado, establecidas en las letras e) y m) del artículo 33 de la Ley de Transparencia de la Función Pública y de Acceso a la Información de la Administración del Estado, aprobada por el artículo primero de la ley N°20.285, el Consejo Directivo del Consejo para la Transparencia, en sesión ordinaria N°1.048, de fecha 21 de noviembre de 2019, acordó remitir a usted un conjunto de recomendaciones en materia de protección de datos carácter personal y seguridad de la información.

2. Que, las presentes recomendaciones son formuladas como consecuencia de información difundida a través de diversos medios de comunicación, dando cuenta que, entre los días 25 de octubre y 01 de noviembre de 2019, se habría verificado una masiva filtración y/o acceso no autorizado a ciertos bancos de datos tratados por su institución, los que contendrían una amplia gama de información -desde el punto de vista cuantitativo y cualitativo- concerniente tanto a funcionarios policiales como a terceras personas.

   La Dirección de Desarrollo de este Consejo, en cumplimiento de la función de velar por la protección de los datos personales por parte de los órganos de la Administración del Estado, y con el objeto de determinar los alcances y riesgos derivados de esta brecha de seguridad, llevó a cabo un proceso de análisis técnico de los factores que pudieron influir

en esta filtración, así como de las características de las bases de datos afectadas. A partir de dicha revisión, se pudo establecer que la vulneración de seguridad en cuestión habría expuesto múltiples datos de carácter personal, tanto estructurados como no estructurados, entre ellos, datos sensibles de los funcionarios de su Institución, así como de terceras personas.

3. Que, teniendo presente el marco normativo general contenido en la Ley N°19.628, que exige a los responsables del tratamiento de información de carácter personal dar estricto cumplimiento a los principios de finalidad, calidad de los datos, protección especial de los datos sensibles, seguridad de la información y el deber de confidencialidad, se debe garantizar, en todo momento, el adecuado resguardo de los derechos de los titulares de datos personales. Es menester señalar de la misma forma que, conforme lo establecido en el artículo 11 de la Ley N°19.628, el responsable del tratamiento de datos debe cuidar de ellos con la debida diligencia, haciéndose responsable de posibles daños.

4. Que así, y con miras a asegurar la debida protección de la información contenida en las bases de datos administradas por su institución, resulta indispensable considerar, a lo menos, los siguientes elementos:

   a) **Identificación y gestión de riesgos**. En el tratamiento de bases de datos personales, resulta recomendable la aplicación de herramientas que permitan identificar y jerarquizar los riesgos asociados a operaciones de procesamiento de dichos datos, llevando a cabo, además, evaluaciones de impacto de privacidad, permanentes y aleatorias. Las actividades de evaluación de impacto deben estar presente desde el inicio de las operaciones de tratamiento, en orden a precaver la eventual divulgación no autorizada de datos personales. Con dicha evaluación, se podrán determinar de mejor manera las medidas necesarias para proteger la integridad y confidencialidad de los datos objeto de tratamiento.

   b) **Medidas de seguridad**. Conforme a las Recomendaciones del Consejo para la Transparencia sobre Protección de Datos Personales por parte de los Órganos de la Administración del Estado, se deben adoptar *"todas las medidas, tanto organizativas como técnicas, para resguardar la integridad, confidencialidad y disponibilidad de los datos contenidos en sus registros con la finalidad de evitar la alteración, pérdida, transmisión y acceso no autorizado de los mismos. Para ello, los organismos públicos aplicarán diversos niveles de seguridad atendiendo al tipo de dato almacenado, a título ejemplar, respecto de los datos sensibles deberán adoptarse niveles de seguridad más altos que en relación a aquellos que no poseen dicha calidad."*. Por consiguiente, y considerando la naturaleza o calidad de los datos personales que, en un caso concreto, sean objeto de tratamiento, resulta imprescindible:

      i) Adoptar medidas de seguridad adecuadas, mediante el uso de sistemas informáticos actualizados y robustos.

ii) Incorporar procedimientos, tecnologías y recursos humanos capacitados para la prevención de filtraciones de datos personales y accesos no autorizados a redes o sistemas informáticos de la institución.

iii) Definir roles y perfiles de acceso diferenciados según los distintos tipos de información contenida en las bases de datos institucionales, con la correspondiente capacitación del personal que opera las plataformas o sistemas. En caso de que la información deba ser comunicada a otros organismos públicos, resulta necesario utilizar sistemas seguros de transmisión basados en tecnologías de encriptación para asegurar su integridad y confidencialidad.

iv) Establecer deberes de confidencialidad estrictos, garantizando su cumplimiento a través de los mecanismos disciplinarios que la institución contemple, respecto de todas aquellos funcionarios o personal civil que participe en el tratamiento de los datos recolectados, incluyendo a las entidades privadas contratadas para proveer servicios informáticos. Esta clase de medidas permite consolidar los mecanismos de resguardo.

En esta misma línea, en el evento de sufrir ataques o intrusiones al banco de datos, se aconseja adoptar las medidas especiales de resguardo de la información que el caso amerite, con el objeto de preservar su integridad, e informar a los titulares de los datos de eventuales brechas de seguridad, las posibles consecuencias de estas vulneraciones y las medidas de solución o resguardo adoptadas.

Para garantizar la incorporación de estándares adecuados de seguridad de la información, resulta necesario adoptar un enfoque integral, a través de políticas efectivas de gestión de la información (que se identifican con el concepto de Sistema de Gestión de Seguridad de la información - SGSI). En este orden de cosas, se deben considerar medidas de seguridad que garanticen apropiadamente tanto la seguridad de la información como la protección de los datos personales.

Conforme lo anterior, se recomienda a Carabineros de Chile: (i) la implementación de un sistema comprehensivo de seguridad de la información, que permita la preservación de confidencialidad, integridad y disponibilidad de la información, haciendo uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo organizacional; e (ii) incorporar, planificar y estructurar controles de protección de datos personales como un componente crucial del SGSI.

c) Desde el punto de vista de operatividad tecnológica, debiese considerarse el desarrollo de un programa de acciones tendientes a la implementación de medidas de ciberseguridad, sobre la base de los siguientes elementos:

i) Incorporación de políticas de contraseñas, respaldo de la información, control de acceso a sistemas y sectores restringidos, procedimientos de

gestión de ambientes, procedimientos de operaciones, y procedimientos de gestión de incidentes.

ii) Adecuado desarrollo de infraestructura física y lógica, lo que incluye planes de actualización de servidores, estaciones de trabajo y dispositivos conectados, tanto para sistemas operativos como aplicaciones instaladas; uso de firewalls de nueva generación, con protección de amenazas avanzadas, análisis de tráfico y monitoreo; uso de dispositivos HSM (Hardware Security Module o Módulo de Seguridad Hardware); uso de antivirus y antimalware, con actualización permanente; y actividades de inventario de la infraestructura tecnológica, con programación de auditorías internas y externas.

iii) Incorporación de herramientas de cifrado de las comunicaciones y segmentación de redes, que permitan separar accesos entre grupos de usuarios y/o servidores, acompañado de la adecuada gestión en el acceso a la red privada interna de la institución.

iv) Constante monitoreo de servicios, servidores y potenciales actividades sospechosas, mediante un programa de evaluaciones periódicas.

v) Respecto a los funcionarios, llevar a cabo programas de concientización para usuarios (por ejemplo, indicaciones sobre navegación segura, actitud defensiva ante la llegada de correos, uso correcto y seguro de dispositivos, entre otras).

vi) Adoptar resguardos que permitan el desarrollo seguro de sistemas (construcción de software, aplicaciones, bases de datos). Los sistemas que manejen datos sensibles deben restringir el acceso a la misma, enmascarando o seudo-anonimizando la información, y estableciendo permisos de acceso estrictos.

d) **Conservación y eliminación**. El artículo 6° de la Ley N°19.628 dispone que los datos personales deben ser eliminados cuando su almacenamiento carezca de fundamento legal o cuando hayan caducado. Por extensión, los datos personales deben conservarse sólo durante el tiempo necesario para cumplir con la finalidad para la cual fueron recabados. Una vez cumplida la finalidad que motivó su recolección, el responsable del tratamiento debe proceder con la eliminación segura y certificada de todos los datos recolectados, por cuanto el almacenamiento de éstos carecería de fundamento legal.

En este proceso de eliminación de los datos, se sugiere adoptar las medidas técnicas necesarias para impedir que se pueda reversar la operación y recuperar posteriormente los datos eliminados.

5. Que, con miras a promover el mejor cumplimiento de los principios, derechos y deberes contenidos en la ley N°19.628, y a las buenas prácticas en la materia y, en virtud de la atribución contenida en el literal k) del artículo 33 de la Ley de Transparencia, que confiere a esta Corporación la atribución de colaborar con los órganos públicos en el ámbito de su competencia, este Consejo pone a disposición de Carabineros de Chile su experticia técnica, para realizar actividades que potencien las capacidades institucionales en materia de protección de datos de carácter personal. Esta propuesta de colaboración comprende el desarrollo de instancias de capacitación dirigidas a funcionarios directivos, jefaturas, profesionales, técnicos y administrativos que participen en cualquier proceso vinculado al tratamiento de bases de datos personales, para fortalecer el adecuado cumplimiento de las obligaciones que exige la ley N°19.628 y su normativa complementaria.

6. Que, finalmente y teniendo presente las consideraciones precedentemente expuestas, el Consejo Directivo del Consejo para la Transparencia, acordó remitir a la Contraloría General de la República, tanto el presente oficio, como los antecedentes que forman parte del presente pronunciamiento, para los fines que estime pertinentes

Sin otro particular, le saluda atentamente a usted,

REPÚBLICA DE CHILE ★ CONSEJO PARA LA TRANSPARENCIA ★ Directora General

ANDREA RUIZ ROSAS
DIRECTORA GENERAL
Consejo para la Transparencia

DIM/GAS/AMM
DISTRIBUCIÓN:
- Sr. Mario Rozas Córdova, General Director de Carabineros.
- Sr. Jorge Bermúdez Soto, Contralor General de la República.
- Sr. Gonzalo Blumel Mac - Iver, Ministro del Interior y Seguridad Pública (copia informativa).
- Archivo.

INFORME

FILTRACIÓN DE BASE DE DATOS DE CARABINEROS DE CHILE

21.11.19

RESUMEN EJECUTIVO.

1. De acuerdo con la información de la cual dan cuenta diversos medios de prensa, se puede observar que la información contenida en las filtraciones de las que fue víctima Carabineros de Chile se refiere a:
   a) Antecedentes de las actividades de inteligencia policial;
   b) Documentos que contienen un número importante de datos personales no sólo del personal de Carabineros de Chile, sino que también de terceras personas, como detenidos y autoridades.
2. El tratamiento de ciertas bases de datos por parte de Carabineros que se vincula a procesos de recolección, evaluación y análisis de información **con fines de inteligencia se encuentra sujeto al estatuto especial contenido en la Ley N°19.974, y en tanto tal, no le serían aplicables las disposiciones contenidas en la Ley N°19.628.**
3. Sin embargo, se advierte que en algunos casos resulta complejo determinar a priori con certeza cuáles documentos caben dentro del marco del desempeño de las labores de inteligencia policial y cuáles no.
4. Por otra parte, es posible establecer que, en vista a las funciones y competencias legales de Carabineros, que dicen relación con labores de orden y seguridad pública que conllevan la gestión de grandes cantidades de recursos humanos, materiales y financieros, **este organismo policial es responsable del tratamiento de una amplia gama de información, la que comprendería tanto datos de carácter personal como datos no personales.**
5. Al respecto, el marco normativo general aplicable al **tratamiento de estos datos personales se encuentra contenido en la Ley N°19.628**, siendo necesario dar cumplimiento a los principios de licitud, finalidad, confidencialidad, exactitud y seguridad.
6. Adicionalmente, para la debida protección y resguardo de dichos datos, es fundamental llevar a cabo **evaluaciones de riesgos a la privacidad y establecer medidas idóneas de seguridad digital, junto con la adopción de enfoques que tiendan a la minimización en la recolección de datos personales.**
7. Respecto al **potencial tratamiento de datos personales**, expuestos en la filtración, cabe indicar, que los formatos filtrados son información estructurada y no estructurada. El primer grupo, que facilita el tratamiento, son de aquellas bases de datos relacionales y planillas Excel, mientras el segundo compuesto por archivos de texto, documentos Word y PDF, y audios, si bien requieren un esfuerzo para su utilización, no impide que, a través de

métodos de extracción de datos, puedan ser tratados. De esta manera, **las posibilidades de tratamiento cruzado de bases de datos personales entre la información filtrada o con otras fuentes son múltiples**, ya que contienen identificadores únicos de los funcionarios. Por ejemplo, en días posteriores a la filtración, se publicó el sitio web https://pacolog.com/, que cruza parte de la información filtrada con direcciones de las personas y su georreferenciación, de esta forma, se puede buscar a funcionarios de carabineros por Nombre, Rut, Código Funcionario, Comisaria y Prefectura, obteniendo el listado de datos personales que se filtraron para cada uno de ellos, además, vía georreferenciación utilizando mapas de Google se pueden ver visualmente las direcciones de los Carabineros.

8. **Respecto a la vulneración de seguridad que originó la filtración de información, se recomienda lo siguiente:**

   a) **Implementar un Sistema de Gestión de Seguridad de la Información (SGSI),** basado en la norma 27.001:2013, que permita la preservación de confidencialidad, integridad y disponibilidad de la información, haciendo uso de un proceso sistemático, documentado y conocido por toda la institución, desde un enfoque de riesgo organizacional.

   b) **Integrar controles entre Seguridad de la Información (27.001:2013) y Protección de Datos Personales**, creándose un nuevo dominio en el Sistema de Gestión de Seguridad de la Información (SGSI). Este nuevo dominio debe tener controles de PDP, y puede considerar los estándares y buenas prácticas asociadas al Proyecto de Ley de PDP que actualmente se tramita en el Congreso y al Reglamento General de Protección de Datos (RGPD) de Europa, además de otras fuentes y estándares internacionales.

   c) Atendiendo el tipo de vulneración de seguridad ocurrida y sin ser taxativos en las propuestas, se propone **implementar recomendaciones y actividades que pueden ser parte del plan integral de aplicación de medidas de Ciberseguridad** que adopte Carabineros de Chile. Estas recomendaciones van en los ámbitos de Políticas y Procedimientos, Infraestructura Tecnológica, Comunicaciones y Redes, Monitoreo, equipos de trabajo, evaluaciones de Ethical Hacking y Desarrollo Seguro de Sistemas.

9. Se hace presente que con fecha 29 de octubre del presente, **la Contraloría General de la República ofició a la Subsecretaría del Interior**, para que, en el plazo de 10 días hábiles, informe sobre las medidas adoptadas por Carabineros a raíz del hackeo de sus sistemas informáticos. De la misma forma, se **ofició a Carabineros de Chile** para que informe sobre la filtración de antecedentes e información sobre las funcionarias y funcionarios de la policía.

10. Finalmente, en relación con el **ejercicio del derecho de acceso a la información** respecto a la diversa información que ha sido filtrada, se debe tener presente que se trata de información que obra en poder de Carabineros de Chile, por lo que, en principio, podría tratarse de información pública. Sin embargo, dado el tipo de información y antecedentes de que se trata, se deben realizar varias precisiones al respecto.

I. ANTECEDENTES: FILTRACIÓN DE INFORMACIÓN DE CARABINEROS DE CHILE.

Entre los días 25 de octubre y 01 de noviembre de 2019 se efectuó una masiva filtración de información de Carabineros de Chile. Según informó CIPER[1], se habrían producido tres filtraciones sucesivas de documentos como resultado de un ataque informático a sus redes o sistemas informáticos.

De acuerdo con la nota de prensa, en la primera de estas filtraciones, se dio a conocer una base de datos con nombres, Rut, sexo, zona y comisarías, de funcionarios de Carabineros de Chile. En la segunda filtración se habría accedido una base de datos que registra la situación procesal de múltiples personas. Asimismo, se distribuyó un conjunto de códigos de la plataforma de documentación electrónica, que permitiría a un usuario con conocimientos técnicos suficientes acceder a los archivos internos de Carabineros.

En la tercera filtración, ocurrida el lunes 28 de octubre, se expusieron comunicaciones internas de Carabineros, que daban cuenta de información de inteligencia, algunas de ellas amparadas por secreto legal, y otros antecedentes sensibles, como, por ejemplo, registros de movimientos internos de Carabineros; planes de resguardo de residencias de altas autoridades y traslado de material para dispersar manifestaciones; reportes sobre eventuales ataques a comisarías; etc. También, los documentos filtrados incluyen información personal de detenidos, como su nombre, cédula de identidad, direcciones, teléfonos, delitos o faltas por las que se encontrarían privadas de libertad.

En síntesis, de acuerdo con la información que dan cuenta diversos medios de prensa, se puede observar que la información contenida en las filtraciones de las que fue víctima Carabineros de Chile, se refiere, por una parte, a:

(i) Diversos antecedentes de las actividades de inteligencia policial y, por otra,

(ii) Múltiples documentos que contienen un número importante de datos personales no sólo del personal de Carabineros de Chile, sino que también de terceras personas, como detenidos y autoridades.

Sobre el particular, a la información relativa a actividades de inteligencia policial le es aplicable el estatuto contenido en la Ley N°19.974, sobre el Sistema de Inteligencia del Estado (SIE) y que crea la Agencia Nacional de Inteligencia, por lo tanto, aquellos los procesos de recolección, evaluación y análisis de información con fines de inteligencia quedan sujetos a dicho estatuto.

Por su parte, en vista a las funciones y competencias legales de Carabineros, que dicen relación con labores de orden y seguridad pública que conllevan la gestión de grandes cantidades de

[1] https://ciperchile.cl/2019/10/29/hackeo-a-carabineros-en-medio-de-la-crisis-expone-10-515-archivos-entre-ellos-hay-datos-de-inteligencia/

recursos humanos, materiales y financieros, este organismo policial es responsable del tratamiento de una amplia gama de información, la que comprendería tanto datos de carácter personal como datos no personales. Al respecto, el marco normativo general aplicable al tratamiento de estos datos personales se encuentra contenido en la Ley N°19.628, siendo necesario dar cumplimiento a los principios de licitud, finalidad, confidencialidad, exactitud y seguridad.

II. ESTATUTO APLICABLE A LA INFORMACIÓN DE INTELIGENCIA: LEY N°19.974, SOBRE EL SISTEMA DE INTELIGENCIA DEL ESTADO Y CREA LA AGENCIA NACIONAL DE INTELIGENCIA.

1. Concepto de inteligencia.

En conformidad a esta ley, la **inteligencia**, definida en su artículo 2°, se entiende como el *"proceso sistemático de recolección, evaluación y análisis de información, cuya finalidad es producir conocimiento útil para la toma de decisiones."*.

2. Características del sistema de inteligencia.

El modelo SIE se caracteriza por ser multifuncional, aunque con una autonomía inorgánica. El SIE es multifuncional dado que es posible identificar **dos subsistemas de inteligencia con objetivos diferenciados**:

a) Los organismos de las Fuerzas Armadas, cuyo objetivo es velar por la Defensa Nacional y, los de Orden y Seguridad, responsables del orden público y la seguridad interior.

b) Un subsistema de coordinación, compuesto por: la Dirección de Inteligencia de Defensa, radicada en el Estado Mayor Conjunto, en lo que respecta a los militares; y la Agencia Nacional de Inteligencia (ANI), en lo que respecta a los organismos policiales y de seguridad interior.

Derivado de este **rasgo de polifuncionalidad**, otra característica es que los organismos de inteligencia civil y militar tienen un alto grado de independencia, de forma tal que el artículo 4° establece que el SEI *"es el conjunto de organismos de inteligencia, independientes entre sí (y) funcionalmente coordinados."*.

3. Atribuciones de la ANI.

El artículo 8° de la ley señala que a la ANI le corresponden, entre otras, las siguientes funciones:

a) Recolectar y procesar información de todos los ámbitos del nivel nacional e internacional, con el fin de producir inteligencia y de efectuar apreciaciones

globales y sectoriales, de acuerdo con los requerimientos efectuados por el Presidente de la República.

b) Elaborar informes periódicos de inteligencia, de carácter secreto, que se remitirán al Presidente de la República y a los ministerios u organismos que determine.

c) Proponer normas y procedimientos de protección de los sistemas de información crítica del Estado.

d) Requerir de los servicios de la Administración del Estado los antecedentes e informes que estime necesarios para el cumplimiento de sus objetivos, como asimismo, de las empresas o instituciones en que el Estado tenga aportes, participación o representación mayoritarios.

4. Obtención de información.

El Título V de la ley regula los procedimientos especiales de obtención de la información que sea estrictamente indispensable para el cumplimiento de los objetivos del SIE (resguardar la seguridad nacional y proteger a Chile y su pueblo de las amenazas del terrorismo, el crimen organizado y el narcotráfico) y que no pueda ser obtenida de fuentes abiertas. Tales procedimientos son los siguientes:

a) La intervención de las comunicaciones telefónicas, informáticas, radiales y de la correspondencia en cualquiera de sus formas;

b) La intervención de sistemas y redes informáticos;

c) La escucha y grabación electrónica incluyendo la audiovisual; y

d) La intervención de otros sistemas tecnológicos destinados a la transmisión, almacenamiento o procesamiento de comunicaciones o información.

Los directores o jefes de los organismos de inteligencia deben solicitar la autorización judicial para emplear los procedimientos antes señalados (un Ministro de la Corte de Apelaciones en cuyo territorio jurisdiccional se realizará la diligencia o donde se inicie la misma). Es importante notar que en este proceso no intervienen ni los superiores jerárquicos de los Directores de los organismos de inteligencia, esto es, los comandantes en jefe de las instituciones de las Fuerzas Armadas o el director general de las respectivas policías, ni las autoridades políticas responsables de ambos grupos de organizaciones, esto es, los ministros del Interior y Seguridad Pública y de Defensa Nacional[2].

5. Carácter secreto de los antecedentes y obligación de guardar secreto.

[2] Esto daría cuenta de una falta de control civil adecuado respecto de la acción de los órganos del SIE.

a) Los antecedentes, informaciones y registros que obren en poder de los organismos que conforman el Sistema o de su personal, cualquiera que sea su cargo o la naturaleza de su vinculación jurídica con éstos, se consideran secretos y de circulación restringida, para todos los efectos legales. Asimismo, tendrán dicho carácter aquellos otros antecedentes de que el personal de tales organismos tome conocimiento en el desempeño de sus funciones o con ocasión de éstas.

b) Respecto a los estudios e informes que elaboren los organismos de inteligencia, éstos sólo podrán eximirse de dicho carácter con la autorización del Director o Jefe respectivo, en las condiciones que éste indique.

c) Los funcionarios de los organismos de inteligencia que hubieren tomado conocimiento de estos antecedentes, estarán obligados a mantener el carácter secreto de su existencia y contenido aun después del término de sus funciones en los respectivos servicios.

d) La obligación de guardar secreto rige, además, para aquellos que, sin ser funcionarios de los organismos de inteligencia, tomaren conocimiento de las solicitudes para la ejecución de procedimientos especiales de obtención de información, de los antecedentes que las justifiquen y de las resoluciones judiciales que se dicten al efecto.

e) Los funcionarios de los organismos de inteligencia, cualquiera que sea su rango o nivel jerárquico, tendrán derecho a mantener en secreto la identidad de las personas que han sido sus fuentes de información, las que no estarán obligados a revelar ni aun a requerimiento judicial.

6. Responsabilidad de los funcionarios del SIE.

a) El personal de los organismos de inteligencia que infrinja sus deberes u obligaciones incurrirá en **responsabilidad administrativa**, conforme lo determinen las normas reglamentarias de las respectivas instituciones, sin perjuicio de la responsabilidad civil o penal que pueda afectarle.

b) A este último respecto, la ley establece una serie de sanciones penales (e inhabilidades para ejercer cargos públicos) en caso de **abuso o exceso en el ejercicio de las atribuciones o facultades que ella confiere y en caso que los procedimientos empleados no se adecúen al respeto de las garantías constitucionales y a las normas legales y reglamentarias.**

c) Adicionalmente, si los directores o jefes de los organismos de inteligencia del Sistema estimaren que existen antecedentes suficientes de que algún funcionario ha incurrido en una **falta grave de sus deberes funcionarios**, podrán disponer, por resolución someramente fundada, la suspensión inmediata en el ejercicio de su cargo por un plazo no superior a sesenta días, con goce de sus remuneraciones.

d) Además, somete a los miembros y funcionarios de los organismos de inteligencia de las Fuerzas Armadas y de Carabineros de Chile que incurran en las conductas tipificadas en el Título VIII, a las normas y sanciones que al respecto establece el **Código de Justicia Militar**.

7. Control de los organismos de inteligencia.

El Título VI de la ley dispone que el control externo de los organismos de inteligencia corresponderá a la Contraloría General de la República, a los Tribunales de Justicia y a la Cámara de Diputados, en el ámbito de sus respectivas competencias. La Contraloría General de la República procederá a la toma de razón, en forma reservada, de los decretos y resoluciones de la Agencia o expedidos por ella.

III. DEBER DE SEGURIDAD EN EL MARCO DE LA LEY N°19.628.

1. Medidas de seguridad y deber de confidencialidad.

Conforme a las Recomendaciones del Consejo para la Transparencia sobre Protección de Datos Personales por parte de los Órganos de la Administración del Estado, se deben adoptar "todas las medidas, tanto organizativas como técnicas, para resguardar la integridad, confidencialidad y disponibilidad de los datos contenidos en sus registros con la finalidad de evitar la alteración, pérdida, transmisión y acceso no autorizado de los mismos. Para ello, los organismos públicos aplicarán diversos niveles de seguridad atendiendo al tipo de dato almacenado, a título ejemplar, respecto de los datos sensibles deberán adoptarse niveles de seguridad más altos que en relación a aquellos que no poseen dicha calidad.".

a) Así, teniendo especialmente **en vista la naturaleza o calidad de los datos personales** que son objeto de tratamiento, resulta imprescindible garantizar en todo momento:

   i) Medidas de seguridad adecuadas, mediante el uso de sistemas informáticos actualizados y protegidos;
   ii) La incorporación de procedimientos para la prevención de filtraciones y accesos indebidos;
   iii) La definición de perfiles de acceso, con la correspondiente capacitación del personal que opera las plataformas o sistemas. En caso de que la información deba ser comunicada a otros organismos públicos, resulta necesario utilizar sistemas seguros de trasmisión, junto con emplear mecanismos de encriptación para asegurar su integridad y confidencialidad; y
   iv) Establecer deberes de confidencialidad estrictos, garantizando su cumplimiento respecto de todas aquellas personas que participen en el

tratamiento de los datos recolectados, incluyendo a las entidades privadas contratadas para proveer servicios de tratamiento de datos. Esta clase de medidas permite consolidar los mecanismos de resguardo.

b) En esta misma línea, en el evento de sufrir ataques o intrusiones al banco de datos, resulta necesario:

i) Adoptar las medidas especiales de resguardo de la información que el caso amerite, con el objeto de preservar su integridad.
ii) Informar a los titulares de los datos de eventuales brechas de seguridad, las posibles consecuencias de estas vulneraciones y las medidas de solución o resguardo adoptadas.

2. Conservación y eliminación.

a) El artículo 6° de la LPVP dispone que los datos personales deben ser eliminados cuando su almacenamiento carezca de fundamento legal o cuando hayan caducado.

b) Por extensión, los datos personales deben conservarse sólo durante el tiempo necesario para cumplir con la finalidad para la cual fueron recabados.

c) Una vez cumplida la finalidad que motivó su recolección, el responsable del tratamiento debe proceder con la eliminación de todos los datos recolectados, por cuanto el almacenamiento de éstos carecería de fundamento legal.

d) En este proceso de eliminación de los datos, se sugiere adoptar las medidas técnicas necesarias para impedir que se pueda reversar la operación y recuperar posteriormente los datos eliminados.

3. Identificación de los riesgos.

a) En el tratamiento de bases de datos personales, resulta recomendable la aplicación de soluciones técnicas que permitan identificar previamente los riesgos de privacidad asociados a operaciones de procesamiento de datos específicas, llevando a cabo **evaluaciones de impacto de privacidad, permanentes y aleatorias**.

b) En este sentido, cobra relevancia el **principio de *privacidad por diseño***, que dice relación con la adopción proactiva de medidas necesarias y en forma preventiva, frente a la eventualidad de usos indebidos que se puedan efectuar respecto de datos personales.

c) **Entre otras medidas, se debe asegurar la confidencialidad de los datos personales, la minimización de los datos, y otorgar todos los mecanismos que sean necesarios para asegurar el pleno ejercicio de los derechos que la ley**

consagra. Aquí, cobra relevancia también el empleo de taxonomías depuradas para la categorización y la organización de los datos que son gestionados por el responsable del tratamiento[3].

d) En este sentido, resulta importante llevar a cabo evaluaciones de impacto en la privacidad, con anterioridad a iniciar actividades de procesamiento de datos, en orden a precaver la eventual divulgación no autorizada de datos de carácter personal. Con dicha evaluación, se podrán determinar de mejor manera las medidas necesarias para resguardar la privacidad de los datos personales contenidos en las bases de datos objeto de tratamiento.

IV. VULNERACIÓN DE SEGURIDAD Y RECOMENDACIONES.

1. Antecedentes de la vulneración de seguridad.

De acuerdo con información publicada en redes sociales y sitios web por un grupo de Hackers, el pasado 22 de octubre de 2019, Carabineros de Chile, fue hackeado en sus servidores, de los cuales se extrajeron información de bases de datos y archivos de sistemas y distintos documentos. Configurándose de esta manera, una vulneración de seguridad.

Los hackers han filtrado los siguientes archivos por día de publicación:

- Archivos publicados el 25 de octubre 2019:
  - "funcionarios.zip". Bases de datos con datos personales de funcionarios de la institución.
  - "instructivos.zip". Instructivos de uso de plataforma de Documentación electrónica (DOE).
- Archivos publicados el 26 de octubre 2019:
  - "codigofuente.tar.gz". Código fuente plataforma de Documentación Electrónica (DOE) de Carabineros.
  - "dump_intranet.txt". Datos de cuentas de acceso al DOE.
  - "grabaciones-walkie-talkie.zip". Algunas grabaciones de comunicaciones radiales de Carabineros.
- Archivos publicados el 27 de octubre 2019:

[3] La taxonomía de datos consiste en la clasificación de diversos tipos de información en diversas categorías y subcategorías. Proporciona una vista unificada de los datos en una organización e introduce terminologías y semánticas comunes, aplicables a distintos sistemas de procesamiento de datos. La taxonomía permite establecer jerarquías dentro de un conjunto de datos, los que son segregados en múltiples grupos, dependiendo de los niveles de cuidado o seguridad que requieren y los riesgos asociados a su tratamiento.

- "msg.zip". Algunos mensajes desencriptados intercambiados en la plataforma DOE.
- "adjuntos-10-2019-10k.tar.gz". Archivos adjuntados a los mensajes.

- Archivos publicados el 01 de noviembre 2019:
  - "Adjunt09.zip". Archivos adjuntados a mensajes.

De acuerdo con lo indicado por los hackers, vía informativos, referido a la forma en la cual obtuvieron la información, se extrae lo siguiente:

- *"Por cierto, en el archivo "instructivos.zip", incluimos el archivo de configuración de las bases de datos del DOE. La cual, por cierto, es inútil, ya que, al ser parte de la red interna, es imposible conectarse desde fuera. El objetivo de aquello es que los mismos administradores, el gobierno y los carabineros, se den cuenta de que SÍ hubo un hackeo y que esto es real"*[4].
- *"No hubo ningún "ayudante interno" ni un proveedor de servicios que haya facilitado el acceso. Todo fue hecho desde 0"*[5].
- *"SÍ fue un hackeo"*[6].
- *No fue un "un ataque phishing" ni "Ingeniería social"*[7].
- *"Los estándares de seguridad de Carabineros no eran malos, ni básicos. Simplemente les toco pelear contra alguien más fuerte"*[8].

2. Potencial Tratamiento de Datos Personales.

La vulneración de seguridad de Carabineros de Chile expuso múltiples datos personales, entre ellos, datos sensibles de los funcionarios de la Institución.

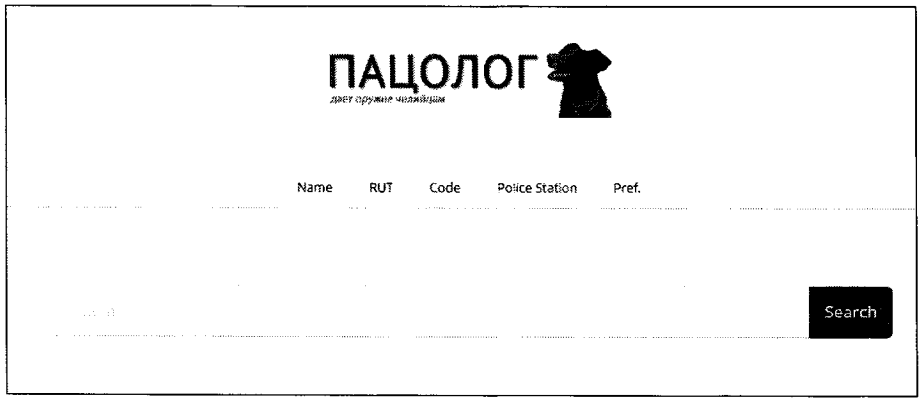
Los formatos de publicación de la filtración consisten en información estructurada y no estructurada. El primer grupo, que facilita el tratamiento, está constituido por bases de datos relacionales y planillas Excel, mientras el segundo compuesto por archivos de texto, documentos Word y PDF, y audios, si bien requieren un esfuerzo para su utilización, no impide que, a través de métodos de extracción de datos, puedan ser tratados.

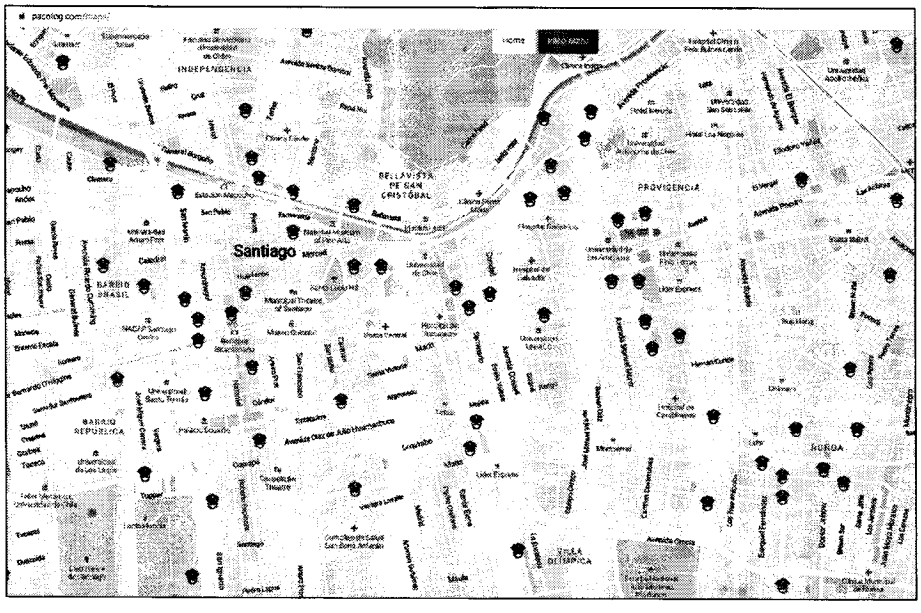
En los datos estructurados se cuenta con identificadores como el RUT o código del funcionario. Esto permite no solo hacer tratamiento de estos datos, sino que también se habilita el cruce con fuentes de datos que son parte de la misma filtración u otras externas que se pueden obtener

[4] Texto literal extraído de informativo N#1 del grupo de hackers.
[5] Texto literal extraído de informativo N#1 del grupo de hackers.
[6] Texto literal extraído de informativo N#2 del grupo de hackers.
[7] Texto literal extraído de informativo N#2 del grupo de hackers.
[8] Texto literal extraído de informativo N#1 del grupo de hackers.

desde Internet. Por ejemplo, quién pueda acceder a la base de datos del registro electoral, mediante cruce con el RUT, puede obtener la dirección electoral de la respectiva persona.

Por ejemplo, en días posteriores a la filtración, se publicó el sitio web https://pacolog.com/, que cruza parte de la información filtrada con direcciones de las personas y su georreferenciación. Conforme lo anterior, se puede buscar a funcionarios de carabineros por Nombre, Rut, Código Funcionario, Comisaria y Prefectura, obteniendo el listado de datos personales que se filtraron para cada uno de ellos, además, vía georreferenciación utilizando mapas de Google se pueden ver visualmente las direcciones de los Carabineros. A continuación, se muestran un par de imágenes del tratamiento de datos personales:





Respecto a los tipos de tratamientos de datos personales, que potencialmente se pueden realizar con los datos observados de la filtración de la vulneración de seguridad, y haciendo referencia a lo definido por el Reglamento General de Protección de Datos de Europa (RGPD),

y la Agencia Española de Protección de Datos (AEPD) en su documento "Listas de tipos de tratamiento de Datos que requieren Evaluación de Impacto relativa a Protección de Datos[9]", y siendo una lista no exhaustiva, se identifican al menos, los siguientes potenciales tratamientos:

- Tratamientos que impliquen perfilado o valoración de sujetos (punto 1 del documento de la AEPD).
- Tratamientos que impliquen la toma de decisiones automatizadas o que contribuyan en gran medida a la toma de tales decisiones (punto 2 del documento de la AEPD).
- Tratamientos que impliquen la observación, monitorización, supervisión, geolocalización o control del interesado de forma sistemática y exhaustiva (punto 3 del documento de la AEPD).

3. Recomendaciones de Seguridad de la Información y Protección de Datos Personales.

La seguridad de la información, según la norma ISO 27.001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Estos tres términos constituyen la base sobre la que se cimienta la Seguridad de la información:

- **Confidencialidad:** la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Integridad:** mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Disponibilidad:** acceso y utilización de la información y los sistemas de tratamiento de esta por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Para garantizar que la Seguridad de la Información sea gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo organizacional. Este proceso es el que constituye un Sistema de Gestión de Seguridad de la información (SGSI), basado en la norma ISO 27.001.

Se deben considerar las medidas de seguridad que garanticen apropiadamente tanto la Seguridad de la Información como la Protección de los Datos Personales, desde un punto de vista integrado, gestionando en la Institución, ya sea datos de los propios funcionarios, o de ciudadanos o bien datos externos que puedan ser tratados.

Respecto a la mirada integrada de la Protección de Datos Personales (PDP) con el Sistema de Gestión de Seguridad de la Información (SGSI), se propone lo siguiente:

a) Integrar controles entre Seguridad de la Información (27.001:2013) y Protección de Datos Personales, creándose un nuevo dominio en el Sistema de Gestión de Seguridad de la Información. Este nuevo dominio debe tener controles de PDP, y

[9] https://www.aepd.es/media/criterios/listas-dpia-es-35-4.pdf. Publicado el 6 de mayo de 2019.

puede considerar los estándares y buenas prácticas asociadas al Proyecto de Ley de PDP que actualmente se tramita en el Congreso y el Reglamento General de Protección de Datos (RGPD) de Europa, el además de otras fuentes y estándares internacionales.

b) Para integrar PDP, se deben considerar las siguientes dimensiones:
   i) Caracterización del Organismo.
   ii) Elementos Claves de PDP.
      - Análisis de Riesgos.
      - Evaluación de Impacto (EIPD).
      - Registro de Actividades de Tratamiento.
      - Documento de Seguridad.
      - Contratos con Terceros.
      - Política Privacidad Empleados.
      - Textos Legales en las Páginas Web.
      - Derechos ARCOP.
      - Videovigilancia.
      - Consentimiento para el Tratamiento de Datos Personales.
   iii) Modelo Integrado a la 27001:2013.
   iv) Controles y Recomendaciones del Modelo PDP.
   v) Adaptación de Modelos de Trabajo.

De esta forma, desde el punto de vista de la Seguridad de la Información y la Protección de Datos Personales, se propone a Carabineros de Chile:

c) Implementación de Sistema de Seguridad de la Información, basado en la norma 27.001:2013, que permita la preservación de confidencialidad, integridad y disponibilidad de la información, haciendo uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo organizacional.
d) Incorporar, planificar e implementar controles de Protección de Datos Personales como un nuevo dominio dentro del SGSI.

4. Recomendaciones Tecnológicas, de Operación y Ciberseguridad.

Con respecto a la seguridad asociada a los ambientes tecnológicos, existen múltiples recomendaciones de Ciberseguridad, que deben ser consideradas o analizadas, dependiendo del caso, por Carabineros de Chile. Entre otras se puede citar:

- Instructivo Presidencial de Ciberseguridad.
- Decretos de Ciberseguridad.
- CSIRT (Equipo de Respuesta ante Incidentes de Seguridad Informática), dependiente del Ministerio del Interior y Seguridad Pública.
- Cybersecurity Framework del NIST (National Institute of Standards and Technology), dependiente del Departamento de Comercio de los Estados Unidos de América.
- Normas ISO de Ciberseguridad.

- INCIBE. Instituto Nacional de Ciberseguridad de España.

En forma más específica, atendiendo el tipo de vulneración de seguridad ocurrido y sin ser taxativo en las propuestas, se propone el siguiente listado de recomendaciones y actividades que pueden ser parte del plan de implementación de medidas de Ciberseguridad, Sistema de Seguridad de la Información o modelo de Seguridad que adopte Carabineros de Chile:

a) Respecto a Políticas y Procedimientos:
   i) Política de contraseñas (complejas y expiración), idealmente tener autenticación multi factor para las cuentas de administración.
   ii) Políticas de respaldos, que defina donde se almacenan los respaldos, y se establezca como y con qué periodicidad se prueban.
   iii) Política de control de acceso a sistemas y sectores restringidos.
   iv) Política y procedimiento de gestión de ambientes, para desarrollo de aplicaciones. Al menos considerar ambientes de Desarrollo, Testing y Productivo, con accesos diferenciados para cada uno.
   v) Procedimientos de operaciones. Por ejemplo, creación de usuarios, asignación de permisos, eliminación de cuentas etc.
   vi) Procedimiento de Gestión de Incidentes.
   vii) Planes de recuperación de desastres.

b) Respecto a Infraestructura Tecnológica:
   i) Plan de actualización de servidores, estaciones de trabajo y dispositivos conectados, tanto para sistemas operativos como aplicaciones instaladas.
   ii) Uso de Firewall de nueva generación, con alta disponibilidad (al menos un Firewall de backup), con protección de amenazas avanzadas, análisis de tráfico y monitoreo.
   iii) Uso de dispositivo HSM (Hardware Security Module o Módulo de Seguridad Hardware), que asegure el almacenamiento de firmas electrónicas, certificados digitales, llaves criptográficas, entre otras.
   iv) Uso de antivirus y antimalware, con actualización permanente.
   v) Inventario de la infraestructura Tecnológica, con programación de auditorías.

c) Respecto a las Comunicaciones y Redes:
   i) Cifrado de las comunicaciones de acuerdo a estándares de la industria.
   ii) Segmentación de Redes, para separar accesos entre grupos de usuarios y/o servidores.
   iii) Gestión en el acceso de VPN a la red interna de la institución.
   iv) Aislar redes WiFi de uso de externos a la institución.

d) Respecto a Monitoreo:
   i) Monitoreo de servicios.

ii) Revisión de log de servidores.
iii) Revisión de las actualizaciones de los servidores.
iv) Monitoreo ante escaneos externos, denegación de servicios (DDoS) u otra actividad sospechosa.

e) Respecto a los funcionarios: Programa de concientización para usuarios. Por ejemplo, indicaciones sobre navegación segura, actitud defensiva ante la llegada de correos, uso de dispositivos, entre otras.

f) Respecto a evaluaciones periódicas: Considerar servicios de Hacking Ético, en distintas dimensiones, con detección de brechas y generación de planes de mejora.

g) Respecto al Desarrollo Seguro de Sistemas (construcción de software, aplicaciones, bases de datos).
   i) Usar arquitectura en capas, separando la capa de Front-End con el Back-End a través de servicios, tales como API/REST o Web Services. Estos servicios deben tener mecanismos de seguridad, como OpenID, uso de token, encriptación de los canales de comunicación basados en TLS.
   ii) En caso de utilizar IIS como Server Application, se debe deshabilitar la opción de "Listado de Directorios".
   iii) Tener definido los accesos a las API a nivel de Cors, restringiendo a través de la IP los accesos. Las APIs deben tener la configuración de que dominios la pueden acceder.
   iv) En caso de utilizar el motor de base de datos SQL Server, se debe deshabilitar el usuario "sa" y crear un usuario especifico por base de datos sin privilegios de Owner.
   v) En el caso de utilizar el motor de base de datos MySQL, se debe deshabilitar el usuario "root" y crear un usuario especifico por base de datos sin privilegios de Owner.
   vi) Utilizar una capa para orquestar las transacciones y estas sean atómicas, evitando que alguna intrusión maliciosa intervenga la transacción.
   vii) Para la base de datos se recomienda utilizar un ORM (Object-Relational mapping), tales como Entity Framework o Hibernate, en caso de no tener acceso a estas tecnologías y usar base de datos como SQL, Oracle u otra y se utilicen procedimientos almacenados directamente en el motor, éstos deben ser securitizados de forma correcta, por ejemplo, utilizando bind variables.
   viii) En el diseño de los sistemas, las contraseñas que se encuentran almacenadas deben utilizar algoritmos criptográficos muy fuertes, tales como bcript, PBKDF2 y Argon2.
   ix) En caso de que el sistema contenga certificados digitales, credenciales, base de datos, servicios, llaves criptográficas, deben quedar debidamente parametrizables en un archivo de variables de entorno y éste debe ser excluido de la herramienta de control de versiones.

x) Los sistemas que manejen datos sensibles deben restringir el acceso a la información sensible, enmascarando o seudo anonimizando la información. Solo deben tener acceso solo aquellos usuarios donde exista un fundamento con base jurídica y/o que sea el responsable de la gestión y/o tratamiento de los datos personales.

xi) Pruebas (Testing). La planificación de pruebas y su ejecución debe considerar revisiones de seguridad.

xii) Planificar sesiones de revisión de código fuente, para detección de errores, brechas de seguridad y oportunidades de mejora.

xiii) Gestionar el acceso y control de los códigos fuente, mediante softwares administración de código fuente.

V. EJERCICIO DEL DERECHO DE ACCESO A LA INFORMACIÓN.

En relación con el ejercicio del derecho de acceso a la información respecto a la diversa información que ha sido filtrada en las últimas semanas, se debe señalar, en primer lugar, que se trata de información que obra en poder de Carabineros de Chile, por lo que, en principio, se trataría de información pública. Sin embargo, dado el tipo de información y antecedentes de que se trata, se deben realizar algunas precisiones:

i) En efecto, se observa que parte importante de la información divulgada dice relación con datos personales, e incluso sensibles, tanto de funcionarios de Carabineros como de terceras personas. Respecto de eventuales solicitudes de información que se refieran a dichos datos, se deben tener presente las disposiciones de la Ley N°19.628 para proceder a su tratamiento.

ii) Asimismo, se observa que parte de los antecedentes divulgados están relacionados con los sistemas de inteligencia de la institución. Sobre el particular, el artículo 21 N°3 y N°4 de la Ley de Transparencia, contemplan como causales de secreto o reserva la afectación de la seguridad de la nación o el interés nacional.

Por lo tanto, al momento de requerirse la entrega de dichos antecedentes, se deberá tener en consideración las citadas causales de reserva, las que en todo caso deberán ser analizadas y ponderadas caso a caso.