consejo para la Transparencia

APRUEBA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DEL CONSEJO PARA LA TRANSPARENCIA Y DEJA SIN EFECTO RESOLUCIÓN EXENTA N°803, DE 27 DE DICIEMBRE DE 2016.

RESOLUCIÓN EXENTA N° 99

SANTIAGO, 27 FEB 2023

VISTO:

Lo dispuesto en la Constitución Política de la República; en 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, en adelante, la "Ley de Transparencia"; en la Ley N°19.628 sobre Protección de la Vida Privada; en el decreto con fuerza de ley N°1/19.653, de 2000, del Ministerio Secretaría General de la Presidencia, que fija el texto refundido, coordinado y sistematizado de la Ley N°18.575, orgánica constitucional de bases generales de la Administración del Estado; en la Ley N°19.880, que establece Bases de los Procedimientos Administrativos que rigen los Actos de los Órganos de la Administración del Estado; en la Ley N°21.180 de Transformación Digital del Estado; en el Decreto Supremo N°83, de 2004, del Ministerio Secretaría General de la Presidencia, que Aprueba Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos; en el decreto supremo N°533, de 27 de abril de 2015, del Ministerio del Interior y Seguridad Pública, que crea Comité Interministerial sobre Ciberseguridad; en el decreto supremo N°20, de 3 de marzo de 2009, del Ministerio Secretaría General de la Presidencia, que aprueba los Estatutos de funcionamiento del Consejo para la Transparencia; en la resolución exenta N°304, de 30 de noviembre de 2020, del Consejo para la Transparencia, que aprueba el texto actualizado y refundido de las recomendaciones del Consejo para la Transparencia sobre protección de datos personales por parte de los órganos de la Administración del Estado y sustituye texto que indica; y, en la resolución exenta N°139, de 17 de junio de 2021, del Consejo, que Aprueba Anexo de contrato de trabajo suscrito con don David Ibaceta Medina, nombrándolo Director General de esta Corporación.

CONSIDERANDO:

consejo para la Transparencia

1. Que, el Consejo para la Transparencia -en adelante el Consejo- ha sido creado por la Ley de Transparencia, como una corporación autónoma de derecho público con personalidad jurídica y patrimonio propio, que tiene por objeto promover la transparencia de la función pública, fiscalizar el cumplimiento de las normas sobre transparencia y publicidad de la información de los órganos de la Administración del Estado, y garantizar el derecho de acceso a la información.

2. Que el inciso cuarto del artículo 1° de la Constitución establece que el Estado está al servicio de la persona humana y su finalidad es promover el bien común, para lo cual debe contribuir a crear las condiciones sociales que permitan a todos y a cada uno de los integrantes de la comunidad nacional su mayor realización espiritual y material posible, con pleno respeto a los derechos y garantías que la Constitución establece. Por su parte, el inciso segundo de su artículo 5° dispone que el ejercicio de la soberanía reconoce como limitación el respeto a los derechos esenciales que emanan de la naturaleza humana, siendo deber de los órganos del Estado respetar y promover tales derechos, garantizados por la Constitución, así como por los tratados internacionales ratificados por Chile y que se encuentren vigentes.

3. Que, mediante resolución exenta N°803, de 27 de diciembre de 2016, esta Corporación, en cumplimiento del acuerdo del Consejo Directivo del Consejo para la Transparencia adoptado en sesión ordinaria N°761, de 16 de diciembre de 2016, dictó la Política General de Seguridad de la Información del Consejo para la Transparencia, con el propósito de resguardar sus activos de información de aquellas amenazas internas y externas que pudieran poner en riesgo su confidencialidad, integridad y disponibilidad.

4. Que, esta Política declaraba que el Consejo protegerá sus activos de información de amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar la confidencialidad, integridad y disponibilidad en base a la implementación de un "Sistema de Gestión de la Seguridad de la Información" y su respectivo ciclo de mejora continua, basado en la norma ISO 27001.

5. Por su parte, esta Política establecía que ella será revisada cada tres años, y además, cada vez que el Director General lo requiera, ya sea debido a cambios en el Consejo para la Transparencia que afecten el enfoque de la seguridad de la información, la disponibilidad de recursos y el ambiente técnico, o bien, a modificaciones en las condiciones legales aplicables. También se disponía que se revisará el estado del Sistema de Gestión de Seguridad de la Información a lo menos cada tres años mediante auditorías internas o externas.

6. Que, conforme las determinaciones de revisión y mejora continua señaladas anteriormente y constatando los nuevos desafíos y amenazas para la seguridad de la información que se han generado en el último tiempo, así como la relevancia que su protección tiene para los derechos fundamentales de las personas y el adecuado funcionamiento de los organismos del Estado, es que esta Corporación ha estimado necesario actualizar, ajustar y robustecer la referida Política y de orientar su planteamiento hacía el "activo de información" del Consejo para la Transparencia, cuestión por la cual esta Corporación ha estimado procedente la elaboración y consecuente dictación de una nueva y

segunda versión (2.0) de la Política General de Seguridad de la Información, derogándose al mismo tiempo la resolución exenta N°803, de 27 de diciembre de 2016, con el propósito de mantener un texto único y consolidado de esta Política.

7. Que, entre otras cosas, esta nueva Política establece una reestructuración importante de su contenido, incorporando nuevos capítulos y párrafos, así como actualizando ciertos elementos de seguridad y procedimientos. Por último, se establecen disposiciones que buscan habilitar una coexistencia armónica entre esta normativa y las demás políticas internas del Consejo en materias asociadas, como de protección de datos personales.

8. Que, a la luz de lo expuesto precedentemente,

RESUELVO:

ARTÍCULO PRIMERO: APRUÉBESE Y FÍJESE, la Política General de Seguridad de la Información del Consejo para la Transparencia, cuyo texto es el siguiente:

"POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DEL CONSEJO PARA LA TRANSPARENCIA"

TÍTULO I

ASPECTOS GENERALES

Párrafo 1°

Introducción

Artículo 1°.- Introducción. El Consejo para la Transparencia (en adelante, el "Consejo"), es una corporación autónoma de derecho público, con personalidad jurídica y patrimonio propio, creada por la Ley de Transparencia de la Función Pública y de Acceso a la Información de la Administración del Estado. La misión del Consejo es contribuir a fortalecer la democracia en Chile a través de la rendición de cuentas y el control social, al garantizar el derecho de acceso a la información pública, la transparencia y la protección de datos personales.

Como tal, el Consejo reconoce la importancia y el valor de la información con respecto al funcionamiento eficiente y efectivo de la organización. La información no es sólo crítica para el éxito de la organización, sino estratégica para su supervivencia a largo plazo.

El Consejo procesa información (crea, recibe, difunde, modifica, almacena, conserva y elimina) con la finalidad de ejecutar las actividades necesarias para el cumplimiento de sus funciones. Adicionalmente, entre sus bases de datos y documentación cuenta con datos personales de sus funcionarias y funcionarios, y de terceros (proveedores, clientes, enlaces de órganos públicos y reclamantes, entre otros). Conforme a lo anterior, el Consejo hace una clasificación de la información, considerando los siguientes elementos: la información estratégica y relevante para sus procesos de negocio y soporte; la continuidad de la operación de sus servicios; el cumplimiento de las leyes y la conservación de información histórica, relevante para la institución y el país.

Es por ello que el Consejo para la Transparencia asume la responsabilidad de implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI) que permita lograr niveles adecuados de seguridad para todos los activos de información institucional considerados relevantes, de manera de garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma sistemática, estructurada, eficiente y que se adapte a los cambios que se produzcan por el entorno y las tecnologías.

En este contexto, el Consejo define una Política General de la Seguridad de la Información ("Política"), además de un conjunto de normas y procedimientos, desarrollados a partir de los estándares y buenas prácticas más idóneos, para gestionar sus activos de información.

Artículo 2°.- Contenido de la Política. La Política se compone de los siguientes títulos:

a) Título I: Aspectos generales.

b) Título II: Roles y responsabilidades.

c) Título III: De la información del Consejo para la Transparencia.

d) Título IV: Aspectos finales.

Artículo 3°.- Declaración institucional. El Consejo para la Transparencia protegerá sus activos de información de amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar la confidencialidad, integridad y disponibilidad en base a la implementación de un "Sistema de Gestión de la Seguridad de la Información" y su respectivo ciclo de mejora continua, basado en la norma ISO 27001.

Párrafo 2°

Términos y definiciones

Artículo 4°.- Términos y definiciones de la Política. Para los efectos de esta Política, se entenderá por:

1. Activo de Información: Todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución. Podemos distinguir tres tipos de activos:

a) La información propiamente tal, en sus múltiples formatos (papel o digital, texto, imagen, audio, video, entre otros).

b) Los equipos/sistemas que la soportan.

c) Las personas que la utilizan.

Los activos poseen valor para la organización, y necesitan por tanto ser protegidos adecuadamente para que el organismo no se vea perjudicado (implica detectar vulnerabilidades y establecer controles).

2. Alta Dirección: persona o grupo de personas que dirige y controla una organización al más alto nivel. [ISO/IEC 27000:2014, 2.84]; en el Consejo se define que la Alta Dirección es el Consejo Directivo o el director o directora general.

3. Aplicación: solución TI, incluyendo los softwares de aplicación, procedimientos y datos de aplicación, diseñada para ayudar a los usuarios de una organización a llevar a cabo tareas particulares o resolver tipos particularidades de problemas TI al automatizar un proceso o función de negocio. [ISO/IEC 27000:2014, 2.84]

4. Ataque: intento de destruir, exponer, alterar, inhabilitar, robar u obtener un acceso no autorizado para usar un activo de manera no autorizada. [ISO/IEC 27000:2009]

5. Base de datos personales: conjunto organizado de datos personales, cualquiera sea la forma o modalidad de su creación, almacenamiento, organización y acceso, que permita relacionar los datos entre sí, así como realizar su tratamiento.

6. Buen Uso: se entiende por "buen uso" de los sistemas e información del Consejo, el uso acorde a lo estipulado en las políticas, estándares y procedimientos del organismo.

7. Ciber Ataque: es un ataque contra un sistema informático, una red o una aplicación o dispositivo habilitado para Internet. Los piratas informáticos utilizan una variedad de herramientas para lanzar ataques, incluidos malware, ransomware, kits de explotación y otros métodos.

8. Cibercrimen: actividad criminal que implica que los servicios o aplicaciones en el Ciberespacio se utilicen o sean blanco de un crimen, lo que significa que el Ciberespacio es la fuente, herramienta, blanco o lugar de un crimen. [ISO- 27032:2015, 4.18]

9. Ciberespacio: entorno complejo que resulta de la interacción de personas, softwares y servicios en Internet por medio de dispositivos y redes de tecnología conectados a éste, los que no existen en forma física. [ISO- 27032:2015, 4.21]

10. Ciberocupa: individuos u organizaciones que registran y se aferran a URLs que se parecen a referencias o nombres de otras organizaciones en el mundo real o en el Ciberespacio. [ISO-27032:2015, 4.23]

11. Ciberprotección: condición de estar protegido en contra de las consecuencias físicas, sociales, espirituales, financieras, emocionales, ocupacionales, psicológicas, educacionales o de otro tipo que resultan del fallo, daño, error, accidentes, perjuicios o cualquier otro evento en el Ciberespacio que se pueda considerar no deseable. [ISO- 27032:2015, 4.19].

12. Confidencialidad: propiedad de la información por la que se mantiene inaccesible y no se revela a individuos, entidades o procesos no autorizados. [ISO/IEC 27000:2014, 2.12]. Asegurar

que la información es accesible sólo por las personas autorizadas a tener acceso. [ISO/IEC 27000:2014, 2.9]. Asegurar que los usuarios autorizados tengan acceso a la información y los activos asociados cuando sean requeridos.

13. Continuidad de la Seguridad de la Información: procesos y procedimientos para garantizar la continuidad de las operaciones de seguridad de la información.

14. Control: medida que modifica un riesgo. [ISO/IEC 27000:2014, 2.16]

15. Crimen de internet: actividad criminal que implica que los servicios o aplicaciones en Internet se utilizan o son blanco de un crimen, lo que significa que Internet es la fuente, herramienta, blanco o lugar de un crimen. [ISO- 27032:2015, 4.30]

16. Dato caduco: el que ha perdido actualidad por disposición de la ley, por el cumplimiento de la condición o la expiración del plazo señalado para su vigencia o, si no hubiese norma expresa, por el cambio de los hechos o circunstancias que consigna.

17. Dato estadístico: el dato que, en su origen, o como consecuencia de su tratamiento, no puede ser asociado a un titular identificado o identificable.

18. Dato personal: cualquier información vinculada o referida a una persona natural identificada o identificable. Se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante uno o más identificadores, tales como el nombre, el número de cédula de identidad, el análisis de elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona, excluyendo aquellos casos en que el esfuerzo de identificación sea desproporcionado.

19. Datos personales sensibles: tendrán esta condición sólo aquellos datos personales que revelen el origen étnico o racial, la afiliación política, sindical o gremial, las convicciones ideológicas o filosóficas, las creencias religiosas, los datos relativos a la salud, al perfil biológico humano, los datos biométricos, y la información relativa a la vida sexual, a la orientación sexual y a la identidad de género de una persona natural.

20. Gestión de Incidentes de la Seguridad de la Información: Conjunto de procesos para detectar, informar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

21. Gestión del Riesgo: actividades coordinadas para dirigir y controlar la organización con relación al riesgo. [ISO/IEC 27000:2014, 2.76]

22. Hackeo: acceder intencionalmente al sistema de un computador sin la autorización del usuario o dueño. [ISO- 27032:2015, 4.25]

23. Hacktivismo: hackear por motivos políticos o sociales. [ISO- 27032:2015, 4.26]

24. Información: datos que poseen significado. [ISO 9000:2015, 3.8.2]. Son los datos que individualmente o en su conjunto tienen sentido para quién los accede, los que pueden residir en medios electromagnéticos, físicos o en el conocimiento de las personas como, por ejemplo, puede estar impresa, manuscrita, almacenada electrónicamente, grabada en videos, almacenadas en medios ópticos, electromagnéticos, en la nube, sistemas de transferencia de

archivos y/o transferida en dispositivos de cualquier tipo como pendrives, CD, DVD y similares. Independiente de la forma en que exista o se transmita la información, siempre debe ser protegida adecuadamente.

25. Información Pública: toda aquella información no catalogada como secreta o reservada, tal como lo establece el ordenamiento jurídico vigente.

26. Información Reservada (conocimiento reservado): son aquellos documentos cuyo conocimiento está circunscrito al ámbito de la respectiva unidad del órgano a que sean remitidos, en virtud de una ley o de una norma administrativa dictada en conformidad a ella, que les confiere tal carácter, cuando la naturaleza misma de la información requiera ser tratada de manera reservada.

27. Malware, software malicioso: software diseñado con un propósito malicioso que contiene características o capacidades que pueden potencialmente causar un perjuicio de manera directa o indirecta al usuario y/o al sistema computacional del usuario. Ejemplo: Virus, gusanos, troyanos. [ISO- 27032:2015, 4.35]

28. Parte Interesada: persona u organización que puede afectar, verse afectada, o percibirse como afectada por una decisión o actividad. [ISO/IEC 27000:2014, 2.82].

29. Propiedad de la Información: es el usuario responsable de la información y de los procesos que la manipulan sean estos mecánicos o electrónicos. Las funciones principales son:

a) Definir qué datos son correctos.

b) Definir los procedimientos de captura, procesos y salidas de la información.

c) Definir los controles que deben existir para asegurar el correcto proceso de la información. Autorizar o revocar el acceso a la información por los usuarios.

d) Definir los roles y atributos de acceso de los usuarios.

e) Asegurar el cumplimiento de lo establecido anteriormente.

30. Propietario del Riesgo: persona o entidad que tiene la responsabilidad y autoridad para gestionar un riesgo. [ISO/IEC 27000:2014, 2.78].

31. Protección de Internet: condición de estar protegido en contra de consecuencias físicas, sociales, espirituales, financieras, emocionales, ocupacionales, psicológicas, educacionales o de otro tipo que resultan del fallo, daño, error, accidentes, perjuicios o cualquier otro evento en Internet que se pueda considerar no deseable. [ISO- 27032:2015, 4.31]

32. Responsable de datos o responsable: toda persona natural o jurídica, pública o privada, que decide acerca de los fines y medios del tratamiento de datos personales, con independencia de si los datos son tratados directamente por ella o a través de un tercero mandatario o encargado.

33. Responsable de la Información: es el usuario a cargo de la información y de los procesos que la manipulan sean estos manuales, mecánicos o electrónicos.

34. Riesgo: efecto de la incertidumbre sobre los objetivos. [ISO/IEC 27000:2018, 3.61]

35. Seguridad de internet: conservación de la confidencialidad, integridad y disponibilidad de la información en Internet [ISO- 27032:2015, 4.32]

36. Seguridad de la Información: Preservación de la confidencialidad (2.12), la integridad (2.40) y la disponibilidad (2.9) de la información. [ISO 27000:2013, 2.33]. Es el conjunto de medidas que protegen el recurso de información de una amplia gama de amenazas con el fin de asegurar la continuidad operativa de la Institución y minimizar el daño.

37. Servicios de Internet: servicios entregados a un usuario para habilitar el acceso a Internet por medio de una dirección IP asignada, la que normalmente incluye autentificación, autorización y servicios de nombre de dominio. [ISO- 27032:2015, 4.33]

38. Software engañoso: software que realiza actividades en el computador de un usuario sin antes notificar al usuario de lo que va a hacer exactamente en el computador o sin pedir el consentimiento del usuario para llevar a cabo estas acciones. [ISO- 27032:2015, 4.24]

39. Spam: abuso a los sistemas de mensajería electrónica llevados a cabo para mandar mensajes no solicitados de manera indiscriminada y en masa. [ISO- 27032:2015, 4.42]

40. Spyware: software engañoso que recolecta información privada o confidencial desde un usuario de computador. [ISO- 27032:2015, 4.43]

41. Suplantación de identidad: proceso fraudulento para intentar adquirir información privada o confidencial al disfrazarse como una entidad de confianza en una comunicación electrónica.

42. Titular de datos o titular: persona natural, identificada o identificable, a quien conciernen o se refieren los datos personales.

43. Tratamiento de datos: cualquier operación o conjunto de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, procesar, almacenar, comunicar, transmitir o utilizar de cualquier forma datos personales o conjuntos de datos personales.

Párrafo 3°

Objetivos y alcance

Artículo 5°. Objetivos generales de la gestión de seguridad de la información. Asegurar la continuidad operativa de los procesos de la institución, mediante mecanismos que permitan proteger la integridad, confidencialidad y disponibilidad de sus activos de información, considerando el adecuado cumplimiento de las funciones que la ley asigna al Consejo para la Transparencia, en las materias de su competencia, y garantizando en todo momento los derechos de los titulares de datos de carácter personal.

Artículo 6°. Objetivos específicos de la gestión de seguridad de la información. Estos objetivos son los siguientes:

a) Identificar la totalidad de los activos de información considerados relevantes para todos los procesos que afecten la operación de la institución.

b) Identificar los procesos y subprocesos que contemplen activos de información (incluyendo el tratamiento de datos personales y/o sensibles), con la finalidad de establecer medidas adecuadas de seguridad, tanto a nivel técnico como organizativo.

c) Ejecutar un programa de identificación, análisis y gestión de los riesgos que afecten los activos de información, en base a las metodologías dispuestas según las definiciones de la norma ISO 27001:2013.

d) Establecer para todo el personal de la organización, interno y externo, el deber de resguardar la seguridad de los activos de información institucionales y promover la comprensión de sus responsabilidades individuales.

e) Formalizar las responsabilidades y gobernabilidad para la implementación efectiva de esta política.

f) Diseñar, mantener e implementar normas y procedimientos basándose en estándares idóneos en materia de seguridad de la información.

g) Determinar las medidas esenciales de seguridad de la información que el Consejo debe adoptar, para proteger apropiadamente dichos activos contra amenazas que podrían afectar en alguna medida la confidencialidad, integridad y disponibilidad de los mismos; para esto se determinará la elaboración e implementación de planes de contingencia en los siguientes ámbitos: (i) La ocurrencia de hechos que afecten los activos de información y que generen como consecuencia una interrupción de la continuidad operativa de la institución; (ii) Afectación de los derechos de los titulares de datos personales que estén contenidos en las bases o registros de los cuales sea responsable el Consejo; (iii) Situaciones que impidan al Consejo dar cumplimiento a las normas legales sobre transparencia y acceso a la información pública o a cualquier otra que sea obligatoria para este; (iv) Pérdida o mal uso de los activos de información (datos, equipos, documentación impresa, fuga de información digital, entre otros); y (v) Pérdida de imagen/reputación como organismo estratégico respecto al acceso a la información pública y la transparencia.

h) Concientizar y capacitar a los funcionarios y terceros que se relacionan con el Consejo acerca de su responsabilidad en la mantención de la seguridad de la información y su uso adecuado; para lo cual se debe implementar y fomentar una cultura de seguridad de la información al interior del Consejo y con terceros con los que se relaciona.

Artículo 7°. Alcance de la Política. La presente política promueve la fijación de estándares de seguridad respecto de distintos tipos de información, incluyendo la información pública, reservada y los datos personales y sensibles, entre otros. Esta política debe ser conocida y cumplida por todos los funcionarios del Consejo para la Transparencia; las personas contratadas a honorarios y los terceros (personas naturales y jurídicas) que presten servicios al Consejo, dentro de sus oficinas o remotamente.

La política tiene como alcance toda la información, entre otros, la digital, la impresa o escrita en papel, almacenada electrónicamente, almacenada en la nube, transmitida por correo, usando medios electrónicos o transmitida a través de medios digitales. Asimismo, dicha política es aplicable a los actuales activos de información de la organización y aquéllos que posea en el futuro, aun cuando no se incluyan de forma explícita en el presente documento.

La gestión de la seguridad de la información se realizará mediante un proceso sistemático, documentado y conocido por toda la organización basándose en metodologías de mejora continua. Este proceso de gestión deberá ser aplicado a todos los procesos estratégicos y de soporte de la organización de manera progresiva que la Alta Dirección (Consejo Directivo o director o directora general) defina, a través de programas de trabajo anuales.

Adicionalmente, a esta política general, se desarrollarán normas y procedimientos considerando las particularidades de cada ámbito del estándar ISO 27001:2013.

Cada norma deberá contar con procedimientos asociados, identificación de riesgos, mecanismos de control o mitigación, planes de acción y sanciones asociadas al no cumplimiento.

Artículo 8°. Documentos relacionados con la Política. Estos se pueden dividir en políticas, y normas y procedimientos.

a) Políticas: A continuación, se indican las políticas del Consejo que proporcionan principios y directrices en aspectos específicos de la seguridad de la información:

(i) Política de Gestión de Riesgos.

(ii) Política de Ciberseguridad.

(iii) Política de Seguridad y Salud Ocupacional.

(iv) Política de Privacidad de los Sistemas.

(v) Política de Participación de Funcionarias y Funcionarios.

(vi) Política de Uso Computacional.

(vii) Política de Gestión Documental.

(viii) Política de Gestión del Conocimiento.

b) Normas y procedimientos: Se definirán normas, reglamentos y procedimientos, que serán desarrollados progresivamente y reglamentarán aspectos específicos de la seguridad de la información.

TÍTULO II

ROLES Y RESPONSABILIDADES

Artículo 9°. Director o directora general. Responsable ante el Presidente o Presidenta del Consejo para la Transparencia y los Consejeros, por la existencia y cumplimiento de las medidas adecuadas que mantengan un nivel de seguridad de la información acorde con el rol de la organización y los recursos disponibles.

Tiene la responsabilidad de apoyar y difundir activamente la implementación y ciclo de mejora continua del "Sistema de Gestión de la Seguridad de la Información"; proveer y gestionar los recursos necesarios que permitan su implementación progresiva, de acuerdo con las definiciones adoptadas por el propio Consejo; y, dirimir los conflictos que se generen al interior de este sobre los riesgos que, para la seguridad de la información, se derivan de determinadas situaciones

Artículo 10. Coordinador de datos y seguridad de la información (CDSI). Le corresponden las siguientes funciones:

a) Gestionar el desarrollo de la Política General de Seguridad de la Información al interior del Consejo y controlar su implementación.

b) Supervisar la implementación de normas, procedimientos y estándares que se desprenden de la Política General de Seguridad de la Información.

c) Proponer a la Alta Dirección (Consejo Directivo o director o directora general) un plan anual de implementación del Sistema de Gestión de Seguridad de la Información, que considere los procesos a los que se aplicará el diagnóstico de riesgo, la planificación e implementación de mejoras y determine los procesos con los que se trabajará la etapa de evaluación según su nivel de criticidad.

d) Monitorear el avance general de la implementación del plan anual de seguridad de la información.

e) Adoptar las medidas necesarias para resguardar y asegurar la continuidad operativa del Consejo frente a incidentes de seguridad.

f) Establecer relaciones con los encargados de seguridad de otros organismos públicos y especialistas externos que le permitan mantenerse actualizado sobre nuevas tendencias, normas y métodos de seguridad de la información.

g) Implementar y mantener herramientas de gestión de la seguridad de la información, para garantizar la integridad, la confidencialidad y la disponibilidad de la información, y definir las directrices internas de seguridad de la información, realizando las coordinaciones necesarias para realizar estas tareas.

h) Gestionar riesgos de la seguridad de la información, y evaluar y dar seguimiento a sus controles.

i) Gestionar los incidentes de seguridad de la información, las notificaciones y respuestas a éstos y las lecciones aprendidas que dejan los incidentes de seguridad de la información y su gestión.

j) Proponer estrategias y soluciones específicas para la implantación de los controles necesarios para materializar las políticas de seguridad establecidas y la debida solución de las situaciones de riesgo detectadas.

k) Presentar al Director o Directora General, para su resolución, los conflictos en materia de seguridad de la información y los riesgos asociados, y proponer soluciones respecto de ellos.

l) Promover la difusión y apoyo a la seguridad de la información dentro del Consejo.

Artículo 11. Jefa o jefe de unidad. Es responsable de la protección, clasificación y uso de la información que comparte su Unidad, debiendo desarrollar las siguientes tareas:

a) Mantener actualizada la clasificación de la información, informando al Coordinador(a) Datos y de Seguridad de la Información, cualquier modificación de aquélla.

b) Adoptar las medidas adecuadas para evitar que la información se divulgue o use sin autorización.

c) Comunicar a la brevedad, los incidentes relativos a la seguridad de la información, al Coordinador(a) de Datos y Seguridad de la Información.

Artículo 12. Usuario de la información. Es el conjunto de personas internas y/o externas que, con la debida autorización del Director o Directora; Jefe o Jefa de Unidad; pueden utilizar, consultar, ingresar, modificar o borrar la información almacenada en los sistemas informáticos del Consejo u otros medios de almacenamiento.

Las principales responsabilidades de los usuarios de información son:

a) Utilizar la información sólo para el propósito para el que recibió autorización de uso.

b) Conocer las políticas y procedimientos de Seguridad de la Información del Consejo.

c) Cumplir con los controles establecidos en las políticas y procedimientos definidos en el Sistema de Gestión de Seguridad de la Información.

d) Adoptar las medidas adecuadas para evitar que la información se divulgue o use sin autorización.

e) Comunicar los incidentes relativos a la seguridad de la información, al Coordinador o Coordinadora de Datos y Seguridad de la Información.

Artículo 13. Restricciones de acceso para los usuarios de la información. Los usuarios tendrán restringido el acceso a la información que, por motivos operacionales, determine el Jefe o Jefa de Unidad o Director o Directora para evitar modificaciones indebidas o preservar la confidencialidad durante el periodo en el que la información es procesada o generada.

Paralelamente, los usuarios tendrán restringido el acceso a la información cuya reserva, secreto o confidencialidad se encuentren expresamente indicada en alguna ley, tal como la Ley N°19.628, sobre protección de la vida privada, y la Ley N°20.285, sobre acceso a la información pública.

Las autorizaciones que se otorguen limitarán la capacidad de los usuarios en los entornos informáticos, restringiendo el acceso a la información en los sistemas informáticos, de forma que no puedan realizar actividades diferentes a las autorizadas.

TÍTULO III

DE LA INFORMACIÓN DEL CONSEJO PARA LA TRANSPARENCIA

Artículo 14. Generalidades. La Política General de Seguridad de la Información ha sido elaborada en concordancia con la legislación vigente en el país, considerando además su compatibilidad con las prácticas sugeridas en la ISO 27001:2013.

Esta política será obligatoria aun cuando exceda o vaya más que lo requerido por el ordenamiento jurídico. En aquellos casos en que, por una modificación legal u otra causa, alguna sección de esta política se encuentre en conflicto con una norma legal obligatoria para el Consejo, tendrá preeminencia la normativa legal no obstante tener que darse inmediato aviso al Coordinador o Coordinadora de Datos y Seguridad de la Información para que proceda a gestionar los ajustes que correspondan.

Párrafo 1°

Sobre determinada información

Artículo 15. De la información interna. La información es un activo institucional, de manera tal que su acceso, uso y procesamiento, deberán ser consistentes con las políticas y estándares emitidos por el Consejo en cada ámbito.

La información debe ser protegida, por sus custodios, de una manera consistente con su importancia, valor y criticidad, siguiendo las reglas establecidas en las políticas específicas de seguridad de la información, sus procedimientos asociados y en las recomendaciones dadas por el responsable designado de dicha información. Para ello, la Alta Dirección (Consejo Directivo o director o directora general) del Consejo deberá proveer los recursos que permitan implementar los controles necesarios para otorgar el nivel de protección correspondiente al valor de los activos.

El Consejo proveerá los mecanismos para que la información sea accedida y utilizada por el personal que de acuerdo con sus funciones así lo requiera. Igualmente podrá restringir el acceso a la información y tecnologías que la soportan, si la situación y las condiciones lo ameritan.

Artículo 16. De la información de los usuarios externos. Si la institución procesa y mantiene información que sean datos personales y/o sensibles de acuerdo con la normativa vigente, la organización se compromete a implementar los mecanismos necesarios, para disminuir el riesgo y realizar las acciones razonables de acuerdo con el tipo de información. En el caso que la información de usuarios externos no constituya datos personales o sensibles, ésta podrá ser divulgada contando con la autorización respectiva y dando cumplimiento a las políticas y procedimientos respectivos.

Cuando una entidad externa requiera que el Consejo le transfiera o comunique datos personales para realizar su tratamiento en calidad de responsable de datos y el Consejo lo autorice; se establecerán, además de los resguardos que puedan indicarse en otras políticas del Consejo, mecanismos adecuados para proteger la confidencialidad, integridad y disponibilidad de la información por parte de estas entidades o instituciones públicas. En estos casos, y previo a la entrega de los datos, se deberá establecer alguno de los siguientes documentos:

a) La firma de un convenio entre el Consejo y el organismo público receptor, que establezca las condiciones de seguridad y protección de datos personales que debe considerar el organismo que vaya a realizar el tratamiento. Excepcionalmente, la entrega de los datos podrá efectuarse sin la necesidad de suscribir un convenio en tanto la transferencia se encuentre expresamente establecida en una norma de rango legal.

b) La firma de un contrato o acuerdo complementario con una cláusula de confidencialidad y tratamiento de datos personales. Adicionalmente, se deberá firmar un acuerdo de confidencialidad y de tratamiento de datos personales anexo al contrato o acuerdo complementario.

Los datos personales serán conservados únicamente durante el tiempo necesario para cumplir con la finalidad para la que fueron recabados, luego del cual serán cancelados, en conformidad a la ley.

A los datos personales que el Consejo trate, aplicará los mecanismos adecuados con el objetivo de garantizar el ejercicio de los derechos ARCO de los titulares de los datos personales consagrados en la Ley N°19.628.

Los datos personales y sensibles que el Consejo trate deberán ser resguardados para efectos de mantener su debida confidencialidad y no los comunicará a terceros, salvo cuando ello sea procedente de acuerdo con la normativa legal aplicable.

Artículo 17. De la información con los proveedores. Con el fin de mantener un nivel de seguridad adecuado con los proveedores, el Consejo para la Transparencia se compromete a generar y establecer cláusulas de confidencialidad y tratamiento de datos personales y/o acuerdos de confidencialidad y de tratamiento de datos personales con todos sus proveedores que brinden servicios a la Institución y que accedan a activos de información y/o realicen tratamiento de datos personales, datos sensibles y/o datos reservados, cuya información haya sido entregada por el Consejo para la Transparencia al proveedor.

Artículo 18. De la información con otros organismos públicos. Sujeto a lo dispuesto en el artículo 10, con el fin de mantener un nivel de seguridad adecuado con otros organismos públicos en el intercambio de información, el Consejo para la Transparencia se compromete a generar convenios con los organismos a los cuales se le entregue información reservada o se le entregue datos personales y/o datos sensibles para tratar. El convenio tendrá cláusulas de confidencialidad y de tratamiento de datos adecuados para proteger la confidencialidad, integridad y disponibilidad de los datos.

Párrafo 2°

Sobre otros aspectos relevantes

Artículo 19. De las auditorías. Con el fin de velar por el correcto uso de sus activos de información, el Consejo para la Transparencia dispondrá la realización de auditorías internas en cualquier momento y sin previo aviso, las cuales estarán destinadas a verificar el cumplimiento de las políticas vigentes y que dicen relación con el acceso y uso que los usuarios hacen de los activos de información, tanto lógicos, electrónicos como físicos.

Artículo 20. Del compromiso de la Alta Dirección del Consejo. Con el fin de mantener el nivel de seguridad adecuado, la Alta Dirección(Consejo Directivo o director o directora general) se asegura que:

a) La Alta Dirección del Consejo velará por la existencia por parte de la Unidad de Comunicaciones, de un plan formal de difusión de esta política y las políticas específicas que la sustenten.

b) La Alta Dirección del Consejo, mediante la estructura que se defina en la política específica "Aspectos Organizativos de la Seguridad de la Información", procurará que todo el personal reciba un entrenamiento suficiente en materia de seguridad y ciberseguridad, consistente con sus necesidades y su rol dentro del Consejo.

c) La Alta Dirección del Consejo propiciará la existencia de mecanismos o procedimientos formales que permitan asegurar la continuidad operativa de los procesos ante situaciones que impidan el acceso a la información imprescindible para el funcionamiento de la organización.

d) Establecer la seguridad desde el diseño en los procesos y procedimientos que se realicen en el Consejo.

e) Establecer, implementar, mantener y continuamente mejorar el Sistema de Gestión de Seguridad de la Información de acuerdo con los requerimientos de la norma internacional ISO/IEC 27001.

f) Cumplir la legislación vigente, respecto de la manipulación y resguardo de la información y materias afines, así como también de los acuerdos alcanzados contractualmente con empresas externas y funcionarios.

g) Adoptar, de acuerdo con los recursos disponibles, el nivel de seguridad que cumpla estándares internacionales, que garanticen un tratamiento integral en la administración de la seguridad de los recursos de información, tanto al interior del Consejo como en sus comunicaciones con el exterior.

h) Definir un estándar mínimo de seguridad a todos los recursos de información.

i) Aplicar niveles de seguridad a los recursos de información, proporcionales a su criticidad y riesgo.

j) Generar los procedimientos adecuados para que la información se pueda acceder sólo por los usuarios debidamente autorizados, acreditados y autenticados para ello, con los privilegios necesarios para el desempeño de sus funciones.

k) Estar informado de los proyectos relacionados con recursos informáticos del Consejo, desde la perspectiva de la seguridad de la información.

l) Proveer los recursos necesarios para crear, modificar y mejorar continuamente los sistemas, la arquitectura tecnológica, realizar capacitación técnica y en las tecnologías necesarias para cumplir con las políticas, con los estándares de seguridad, y de protección de datos personales por diseño.

m) Proveer los recursos necesarios para gestionar de forma adecuada los requerimientos de la política de seguridad de la información para el establecimiento, implementación, mantención y mejora del sistema de gestión de seguridad de la Información (SGSI).

Artículo 21. De las responsabilidades y deberes de los usuarios (funcionarios). Con el fin de mantener el nivel de seguridad adecuado, se establecen los siguientes deberes y responsabilidades de los usuarios:

a) La información y las tecnologías de información deben ser usadas sólo para propósitos relacionados con las actividades propias del servicio y del funcionamiento del Consejo y autorizados por la Dirección a la que pertenece, debiéndose aplicar criterios de buen uso en su utilización.

b) Las claves de acceso a la información y a las tecnologías de información son individuales, intransferibles y de responsabilidad única de su propietario.

c) El personal está en la obligación de alertar, de manera oportuna y adecuada, cualquier incidente que atente contra lo establecido en esta política según procedimientos establecidos en el manejo de incidentes.

d) Mantener debida reserva y bajo resguardo la información a la cual tuviese acceso.

e) Abstenerse de acceder sin autorización escrita o indebidamente a estaciones de trabajo, archivos, documentación o datos del Consejo, y de otros organismos; así como también

de instalar software o conectar equipos personales u otros elementos no autorizados, a la red de datos.

f) Proteger la confidencialidad, integridad y disponibilidad de la información del Consejo. Dar aviso al Coordinador o Coordinadora de Datos y Seguridad de la Información de cualquier problema que pueda afectar la vulneración de los sistemas, la protección de datos personales u otras circunstancias que podrían indicar riesgos de seguridad.

g) Abstenerse de realizar actos contrarios a la propiedad intelectual del Consejo y terceros, vulnerar contratos de licenciamiento de software y similares, suscritos por el Consejo con sus proveedores de tecnologías de información.

h) Utilizar los recursos informáticos solo para desempeñar las funciones que le fueron asignadas.

i) Mantener en adecuadas condiciones los elementos de tecnología de información entregados para el desempeño de su trabajo. Conocer y cumplir las normas y procedimientos asociadas al uso de los recursos tecnológicos y activos de información a los que se le otorgue acceso, como, por ejemplo, aquellas asociadas al uso de contraseñas, del correo electrónico y del acceso a redes públicas como internet.

j) Colaborar con los controles y procesos de auditoría orientados a verificar el cumplimiento de las políticas vigentes y que dicen relación con el acceso y uso que los usuarios hacen de los recursos de información, tanto lógicos como físicos.

k) Está absolutamente prohibido a los funcionarios divulgar cualquier información que, según la clasificación de información del Consejo, sea clasificada como "reservada" o contenga "datos personales", sin la correspondiente autorización.

Artículo 22. Difusión. Será responsabilidad del director o directora general apoyar la difusión de los temas relevantes en materia de seguridad. Las políticas de seguridad de la información serán comunicadas a todo el personal del Consejo y a los terceros que presten servicios para éste.

Para la difusión de los contenidos de la Políticas de Seguridad de la Información al interior del Consejo se deberán utilizar los medios de difusión que la institución disponga (intranet, boletín, correos etc.), así como también instancias de capacitación llevadas a cabo para este efecto.

Será responsabilidad del Coordinador o Coordinadora de Datos y Seguridad de la Información, en conjunto con la Unidad de Gestión Personas, definir, implementar y evaluar un Plan de Difusión y Concientización en materia de seguridad de la información.

Se definirá e implementará un Plan de Capacitación en materia de seguridad de la información y en materias de ciberseguridad.

Artículo 23. Obligación de cumplimiento. Todos los funcionarios y autoridades del Consejo y las personas que presten servicios a honorarios; los asesores, consultores y alumnos en práctica; y cualquier persona que tenga acceso a los activos de información del Consejo, están obligados a cumplir esta Política General de Seguridad de la Información, sus normas específicas y los procedimientos relacionados.

Tratándose de los procesos de compras del Consejo, deberá incorporarse tal obligación en las bases de licitación y/o en los contratos que se suscriban con los proveedores. Tratándose de

procesos de contratación de personal, deberá incorporarse tal obligación en los contratos de trabajo.

Todas las medidas dispuestas en esta política que se refieran a datos personales y sensibles deberán ser consistentes con las políticas y procedimientos generales sobre protección de datos personales que haya definido el Consejo. Por especialidad, en caso de conflicto o contradicción, prevalecerán, en lo que a datos personales concierne, aquellas relativas a protección de datos personales; esto, sin perjuicio de aquellos ajustes que corresponda realizar para mantener una adecuada coordinación entre todas las políticas institucionales.

TÍTULO IV

ASPECTOS FINALES

Artículo 24. Sistema de gestión. La presente política se integra y coordina con las restantes políticas del Sistema de Gestión de Seguridad de la Información del Consejo para la Transparencia, cuya finalidad es mejorar los niveles de eficiencia y aportar al cumplimiento de los objetivos de la institución:

a) Política de Calidad, basada en la norma ISO 9001.

b) Política de Riesgos, basada en la norma ISO 31000.

c) Política de Gestión Documental, basada en la norma ISO 15489.

d) Política de Ciberseguridad.

e) Política de Participación de Funcionarias y Funcionarios.

f) Políticas de Privacidad de los Sistemas.

Artículo 25. Revisión, medición y mejoras. La Política General de Seguridad de la Información será revisada al menos una vez cada dos años y, además, cada vez que el o la Director(a) General lo requiera, ya sea debido a cambios en el Consejo, que afecten el enfoque de la seguridad de la información, la disponibilidad de recursos, cambios en la infraestructura técnica o modificaciones en las disposiciones legales aplicables a la Institución.

La Alta Dirección (Consejo Directivo o director o directora general) es responsable del involucramiento de los distintos niveles de la organización, estableciendo diferentes criterios y métodos en la definición del alcance de la implementación del Sistema de Gestión de Seguridad de la Información (SGSI).

Se deberá revisar el desempeño del Sistema de Gestión de Seguridad de la Información, para lo cual se establecerán auditorías internas o externas propuestas por el Coordinador(a) de Datos y Seguridad de la Información al director o directora general, a lo menos cada dos años.

Estas auditorías deberán estar de acorde a lo establecido en la Norma Internacional ISO/IEC 27001.

El Consejo se compromete a reconocer cuáles son las oportunidades de mejora continua y las actualizaciones necesarias para los diferentes aspectos del SGSI. Para tal efecto, la Alta Dirección (Consejo Directivo o Director(a) General) debe dar prioridad al control y revisión de los resultados de la evaluación del desempeño del SGSI.

A partir de la medición del desempeño del SGSI o del resultado de las auditorías que se apliquen al SGSI, puede surgir la necesidad de modificar la política con el objetivo de incluir cambios o mejoras en aspectos de la seguridad de la información.

La modificación del presente documento está a cargo del Coordinador(a) de Datos y Seguridad de la Información y será aprobado por el director o directora general.

Artículo 26. Normativa aplicable.

Leyes	
21.459	Establece normas sobre delitos informáticos, deroga la ley N°19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest.
19.628	Sobre protección de la vida privada.
17.336	De propiedad intelectual.
	Código del Trabajo.
18.575	Orgánica constitucional de Bases Generales de la Administración del Estado, contenido en el decreto con fuerza de ley N°1/19.653, de 2000, del Ministerio Secretaría General de la Presidencia, que fija su texto refundido, coordinado y sistematizado.
19.880	Establece bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado.
21.180	Transformación digital del Estado.
18.834	Estatuto Administrativo, contenido en el decreto con fuerza de ley N°29, de 2004, del Ministerio de Hacienda, que fija su texto refundido, coordinado y sistematizado.
20.285	Sobre Acceso a la información Pública.
18.799	Sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.
Otros	
Decreto N°4, de 2021, del Ministerio Secretaría General de la Presidencia, Reglamento que regula la forma en que los procedimientos administrativos deberán expresarse a través de medios electrónicos, en las materias que indica, según lo dispuesto en la Ley N°21.180 sobre transformación digital del Estado.	
Decreto N°1, de 2015, del Ministerio Secretaría General de la Presidencia, que Aprueba Norma Técnica sobre sistemas y sitios web de los órganos de la Administración del Estado.	

Decreto Supremo N°83, de 2004, del Ministerio Secretaría General de la Presidencia, que Aprueba Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos.
Instrucción General del Consejo para la Transparencia, sobre Transparencia Activa.
Instrucción General N°10 del Consejo para la Transparencia, sobre Procedimiento Administrativo de Acceso a la Información.
Instructivo Presidencial N°8 sobre Ciberseguridad.

Artículo 27. Control de cambios. En caso de existir versiones anteriores al documento se deben especificar e identificar los cambios o modificaciones realizadas e incorporadas en la versión vigente.

Nombre del Documento		**Procedimiento de control de documentos**	
Versión	**Fecha**	**Motivo de la Revisión**	**Cambios realizados por:**
1.0	29-09-2016	Creación inicial de documento	José Luis Villesca Bustos
1.1	04-10-2016	Requerimientos de mejoras propuestos por Director de Desarrollo y Procesos: ajustes de redacción, modificación de puntos 2, 7.2 y punto 7.3 "e)". Mejoras propuestas por Jefa de Gestión Documental, se agrega punto 9. Sistema de Gestión.	José Luis Villesca Bustos
1.2	13-10-2016	Mejoras propuestas por Jefe de Sistema. Se modifica punto 7.5 y agrega punto 7.6.	José Luis Villesca Bustos
1.3	18-10-2016	Mejoras propuestas por Jefa de Planificación y Calidad. Se modifican puntos 2, 4.2, 7.2 y 9.	José Luis Villesca Bustos
1.4	16-11-2016	Mejoras propuestas por la Directora de Estudios, Director de Administración, Finanzas y Personas, Jefa de Unidad de Gestión Documental, Jefe Unidad de Normativa y Regulación y la Analista Leslie Montoya.	José Luis Villesca Bustos
1.9	30-09-2022	Generación de Política General de Seguridad de la Información versión 2.0. Se reestructura el documento y se incorporan nuevos capítulos y párrafos. Se actualizan las políticas y procedimientos mencionados.	Emerson Cristian Suárez Stuardo
2.0	27-02-2023	Se incorporan cambios y sugerencias solicitadas por la Dirección Jurídica.	Emerson Cristian Suárez Stuardo

ARTÍCULO SEGUNDO: DISPÓNGASE que esta Política General de Seguridad de la Información del Consejo para la Transparencia comenzará a regir a partir de la fecha en que se dicte la presente resolución que la aprueba.

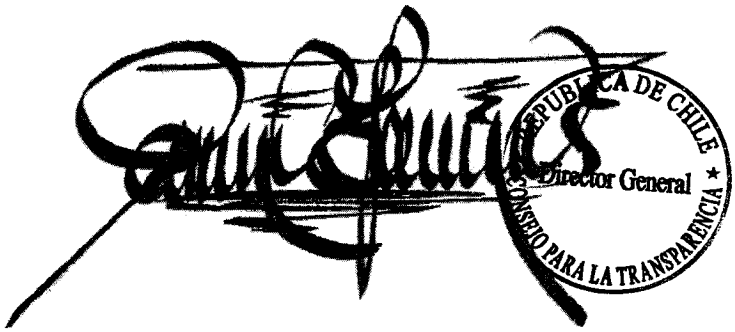
consejo para la
Transparencia

ARTÍCULO TERCERO: DERÓGASE y déjase sin efecto la resolución exenta N°803, de 27 de diciembre de 2016, del Consejo para la Transparencia que aprueba Política General de Seguridad de la Información del Consejo para la Transparencia; anotándose esta derogación al margen de dicha resolución y dejándose constancia de su derogación en los registros y sistemas internos del Consejo para la Transparencia.

ARTÍCULO CUARTO: PUBLÍQUESE en el sitio electrónico de transparencia activa del Consejo para la Transparencia, en el apartado "Actos y resoluciones que tengan efectos sobre terceros", y en la intranet institucional de esta Corporación.

ARTÍCULO QUINTO: NOTIFÍQUESE electrónicamente la presente resolución, mediante copia digital, a los directores del Consejo para la Transparencia, a las jefas y jefes de unidad del Consejo para Transparencia y al Coordinador de Datos y Seguridad de la Información.

ANÓTESE, COMUNÍQUESE, PUBLÍQUESE, en el sitio electrónico de Transparencia activa del Consejo para la Transparencia, **Y ARCHÍVESE.**



DAVID IBACETA MEDINA
Director General
Consejo para la Transparencia

AMM/CBD
DISTRIBUCIÓN:
- Dirección General del Consejo para la Transparencia.
- Dirección Jurídica del Consejo para la Transparencia.
- Dirección de Desarrollo del Consejo para la Transparencia.
- Dirección de Fiscalización y Promoción del Consejo para la Transparencia.
- Dirección de Estudios del Consejo para la Transparencia.
- Unidad de Planificación y Control de Gestión del Consejo para la Transparencia.
- Unidad de Administración y Finanzas del Consejo para la Transparencia.
- Unidad de Desarrollo y Gestión de Personas del Consejo para la Transparencia.
- Unidad de Sumarios del Consejo para la Transparencia.
- Unidad de Atención Integral a Personas del Consejo para la Transparencia.
- Unidad de Comunicaciones del Consejo para la Transparencia.
- Unidad de Normativa y Regulación del Consejo para la Transparencia.
- Unidad de Análisis de Fondo del Consejo para la Transparencia.
- Unidad de Análisis y Estrategia Jurídica y Judicial del Consejo para la Transparencia.
- Unidad de Análisis de Admisibilidad y SARC del Consejo para la Transparencia.

- Unidad de Asuntos Jurídicos Internos del Consejo para la Transparencia.
- Unidad de Sistemas del Consejo para la Transparencia.
- Unidad de Infraestructura y Soporte del Consejo para la Transparencia.
- Unidad de Portal de Transparencia del Estado del Consejo para la Transparencia.
- Unidad de Promoción y Formación del Consejo para la Transparencia.
- Unidad de Fiscalización del Consejo para la Transparencia.
- Unidad de Investigación y Análisis del Consejo para la Transparencia.
- Coordinación de Oficina de Partes del Consejo para la Transparencia.
- Coordinación de Datos y Seguridad de la Información del Consejo para la Transparencia.
- Coordinación de Procesos y Gestión de Riesgos del Consejo para la Transparencia.
- Oficina de Partes.
- Archivo.