MIC/FTO/PBC/CBC/MGC/AHM

APRUEBA POLÍTICA DE CONTINUIDAD OPERACIONAL, AL INTERIOR DE LA SUPERINTENDENCIA DE EDUCACIÓN.

RESOLUCIÓN EXENTA N° 0751

SANTIAGO, 26 DIC 2019

Superintendencia de Educación
TOTALMENTE TRAMITADO

VISTO:

Lo dispuesto 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; la Ley N° 19.880, de 2003, del Ministerio Secretaría General de la Presidencia, que establece las Bases de los Procedimientos Administrativos que rigen los Procedimientos Administrativos que rigen los actos de los Órganos de la Administración del Estado; en el Decreto con Fuerza de Ley N° 29, de 2004, del Ministerio de Hacienda, que fija el texto refundido, coordinado y sistematizado de la Ley N° 18.834, sobre Estatuto Administrativo; en la Ley N° 20.529, de 2011, del Ministerio de Educación, sobre el Sistema Nacional de Aseguramiento de la Calidad de la Educación parvulario, básica y media y su fiscalización; en el Decreto con Fuerza de Ley N° 5, de 2012, del Ministerio de Educación; en el Decreto de nombramiento del Superintendente de Educación, actualmente en trámite, del Ministerio de Educación; en las Resoluciones Exentas N°s 674 y 723, ambas de 2019, de la Superintendencia de Educación; y en la Resolución Nº 6 y 7, de 2019, de la Contraloría General de la República, que fija normas sobre exención del trámite de toma de razón.

CONSIDERANDO:

1. Que, la Ley Nº 20.529, crea la Superintendencia de Educación, en adelante la "Superintendencia", como un servicio público funcionalmente descentralizado y territorialmente desconcentrado, dotado de personalidad jurídica y patrimonio propio y que se relaciona con el Presidente de la República por intermedio del Ministerio de Educación.

2. Que, la Superintendencia tiene por objeto fiscalizar, de conformidad a la ley, que los sostenedores de establecimientos educacionales reconocidos oficialmente por el Estado se ajusten a las leyes, reglamentos e instrucciones que dicte la Superintendencia, en adelante "la normativa educacional". Asimismo, fiscalizará la legalidad del uso de los recursos por los sostenedores de los establecimientos subvencionados y que reciban aporte estatal y, respecto de los sostenedores de los establecimientos particulares pagados, fiscalizará la referida legalidad sólo en caso de denuncia. Además, proporcionará información, en el ámbito de su competencia, a las comunidades educativas y otros usuarios e interesados, y atenderá las denuncias y reclamos de éstos, aplicando las sanciones que en cada caso corresponda.

3. Que, mediante Resolución Exenta N° 289, de fecha 24 de abril de 2019, se dispone la nueva organización interna de la División de Administración General, creándose el Departamento de Tecnología y Procesos.

4. Que, mediante Resolución Exenta N° 0698, de fecha 10 de diciembre de 2019 se nombró al Comité de Seguridad de la Información Institucional, para que, en función del marco legal y tecnológico, proponga a este Jefe de Servicio, un Sistema de Seguridad de la Información y Ciberseguridad lo mantenga y mejore en el tiempo.

5. Que, se ha estimado necesario establecer lineamientos y directrices generales para que las Divisiones, Intendencia de Educación Parvularia y Direcciones Regionales de la Superintendencia cuenten con planes de continuidad operacional para sus procesos de negocio críticos, validados técnicamente según corresponda a sus funciones y responsabilidades, por el Departamento de Tecnología y Procesos, para así contrarrestar o mitigar el impacto de eventos o incidentes de seguridad de la información que puedan provocar interrupciones en dichos procesos.

6. Que, finalmente resulta necesario aprobar mediante el presente acto administrativo la Política de Continuidad Operacional al interior de la Superintendencia de Educación.

RESUELVO:

1° APRUÉBASE, la Política de Continuidad Operacional, al interior de la Superintendencia de Educación, cuyo texto es el siguiente:

Política de Continuidad Operacional

Tabla de Contenidos

ELABORADO POR	REVISADO POR	APROBADO POR
Mauricio Godoy Cisterna **Jefe Departamento de Tecnología y Procesos**	**Claudio Borges Castillo** **Jefe División de Administración General**	**Cristián O'Ryan Squella** **Superintendente de Educación (S)**

1. Declaración institucional:

La Superintendencia de Educación (SIE) se compromete a mantener políticas en el ámbito de la seguridad de la información, específicamente, en el ámbito de la continuidad operacional, con el fin de propender a que los procesos que sustentan sus objetivos estratégicos permitan brindar servicios a la comunidad de manera permanente e ininterrumpida.

2. Objetivo:

Establecer los lineamientos y alcances de la continuidad operacional de la SIE, respecto de sus procesos operacionales, sistemas, aplicaciones y servicios de la organización. En este sentido, se definirán directrices generales para que las Divisiones, Intendencia de Educación Parvularia y Direcciones Regionales de la SIE cuenten con planes de continuidad operacional para sus procesos de negocio críticos validados técnicamente, según corresponda a sus funciones y responsabilidades, por el Departamento de Tecnología y Procesos, con el propósito de contrarrestar o mitigar el impacto de eventos o incidentes de seguridad de la información que puedan provocar interrupciones en dichos procesos.

3. Alcance:

El ámbito de aplicación de la Política de Continuidad Operacional, contempla el siguiente control contenido en la Nch-ISO 27002:2013:

- A.17.01.01 Planificación de la continuidad de la seguridad de la información.

Su alcance contempla los procesos que las Divisiones, Intendencia de Educación Parvularia y Direcciones Regionales hayan identificados como relevantes, críticos o de negocio, en el marco de las Definiciones Estratégicas institucionales (Formulario A19 y en la Matriz de Riesgo Institucional, así como los activos de información relacionados con estos, sean documentos en formato físico (papel), electrónicos, sistemas de información o personas vinculadas a los procesos.

La presente política, y aquellas políticas y procedimientos asociados, son aplicables a todas las autoridades de gobierno, funcionarios, personal a honorarios, funcionarios en comisión de servicio que efectivamente se desempeñen en la institución o cualquier persona, clientes y proveedores que estén involucrados con los activos de información institucionales.

4. Referencias normativas:

- Política general de seguridad de la información vigente.
- Política protección de registros en la SIE vigente.
- Política de seguridad que regula la relación con proveedores de bienes y/o servicios vigentes.
- Política gestión de cambios a los servicios del proveedor vigente.
- Política privacidad y protección de información personal identificable vigente.
- Política devolución de activos de información vigente.
- Política de emplazamiento y protección de equipos vigente.
- Política eliminación o reutilización segura de equipos vigente.
- Política respaldo de información vigente.
- Política para el uso de internet y correo electrónico institucional vigente.
- Política uso de medios removibles y dispositivos móviles vigente.

5. Definiciones:

Concepto	Descripción
Activo de información	Recursos del sistema de información que para la institución es considerada importante o de alta validez, que utiliza y son necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección. Una organización incluye diferentes tipos de activos: - Activos relacionados con el entorno (edificios, instalaciones, equipamientos) y personal. - Activos relacionados con los sistemas de tecnologías de información (equipos, software, comunicaciones). - Activos relacionados con la información (datos, metadatos y soportes). - Activos relacionados con las funcionalidades de la organización (servicios). - Activos intangibles (credibilidad, conocimiento acumulado). Corresponde a todos aquellos elementos relevantes en la producción, procesamiento, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución.
Administración de riegos	Se refiere al proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a los activos de información.
Evaluación de riesgos	Evaluación de las amenazas y vulnerabilidades de la información y las instalaciones de procesamiento de la misma, la probabilidad que ocurran y su potencial impacto en la operación de la organización.
Incidente de seguridad	Evento único o una serie de eventos de seguridad de la información indeseados o inesperados, que tienen una probabilidad significativa de comprometer la operación de negocio y de amenazar la seguridad de la información. Por lo tanto, un incidente de seguridad se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información: un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a la Política de Seguridad de la Información del organismo.
Seguridad de los activos de información	Se refiere a la protección, resguardo y aseguramiento de la disponibilidad, privacidad, confidencialidad e integridad de los activos de información y tecnología de la SIE, para su adecuado procesamiento, con el propósito de garantizar la continuidad operacional de la institución.
Dueño o responsable de activo de información	Es la persona designada como responsable de la integridad, confidencialidad y disponibilidad de un activo de información.
Interoperabilidad	Capacidad de que la información provista por un sistema de información pueda ser utilizada por otro,

Concepto	Descripción
	independientemente de la plataforma en que funcione. En Chile, se utiliza principalmente el estándar XML.

6. Roles y Responsabilidades:

Rol	Responsabilidades
Jefaturas de las Divisiones, Intendencia de Educación Parvularia y Direcciones Regionales	a) Identificar los procesos considerados críticos para sus áreas a cargo. b) Identificar los eventos, amenazas y riesgos que puedan afectar la continuidad operacional de sus procesos críticos. c) Definir y supervisar la implementación de las medidas para contrarrestar o mitigar amenazas o riesgos a sus procesos críticos. d) Coordinar, junto a sus equipos internos y otras áreas de la institución, incluyendo al Departamento de Tecnologías y Procesos, el diseño e implementación de los planes de continuidad operacional de cada área.
Jefe/a Departamento de Tecnología y Procesos	a) Diseñar, implementar y mantener actualizado un Plan de Continuidad Operacional de TI de la SIE, con el propósito de asegurar la entrega y provisión adecuada de servicios de Tecnologías de la Información (Servicios TI), administrados por el Departamento a su cargo b) Responsable de establecer la seguridad de la información, una vez que se recupere la operación normal de los sistemas de información. c) Validar los planes de continuidad operacional, cada vez que estos involucren sistemas o información, base de datos, entre otros. d) Coordinar, en conjunto con otras unidades, departamentos, divisiones la implementación del plan de continuidad operacional.
Encargado/a de Seguridad de la Información y Ciberseguridad	a) Revisar y verificar que los planes de continuidad operacional de la SIE cubran de forma razonable los eventos que tienen una alta probabilidad de ocurrencia y que impacten negativamente la continuidad operacional de las Divisiones, Intendencia de Educación Parvularia y Direcciones Regionales. b) Activar un protocolo de comunicación, con el propósito de comunicar y coordinar las actividades necesarias para el desarrollo del plan de continuidad operacional. c) En caso de eventos mayores que afecten a más unidades o divisiones, debe coordinar la ejecución de planes y acciones de mitigación con el Comité Directivo de Seguridad de la Información.
Comité Directivo de Seguridad de la Información	a) Velar por la implantación del Sistema de Gestión de la Seguridad de la Información e impulsar, promover y revisar periódicamente la implementación de las políticas de seguridad de la información de la SIE.

Rol	Responsabilidades
	b) Apoyar, en casos de eventos mayores que afecten una o más unidades o divisiones de la SIE, donde no exista un plan al respecto y se deben tomar medidas de forma inmediata.
Comité Operativo de Seguridad de la Información	a) Identificar riesgos y amenazas que puedan afectar negativamente la continuidad operacional de los servicios y sistemas de apoyo a los procesos de negocio de las Divisiones, Intendencia de Educación Parvularia y Direcciones Regionales de la SIE. b) Apoyar la implementación del Plan de Continuidad Operacional de la SIE para los activos de tecnologías de la información (TI), correspondientes a la Plataforma Informática y de Telecomunicaciones de la SIE. c) Establecer, junto al Departamento de Tecnología y Procesos, los tiempos de recuperación y restablecimiento de Servicios.
Funcionarios/as, personal a honorarios y practicantes	a) Personas, funcionarios, colaboradores, practicantes o personal externo que preste servicio permanente o temporal que trabajan con información y sistemas de la SUPEREDUC. b) En virtud de lo establecido en la siguiente política, apoya el plan de continuidad operacional establecido y diseñado por su unidad, división o departamento. c) Conocer, respetar y acatar permanentemente las políticas de seguridad de la información de la institución, así como la presente política de continuidad operacional.

7. Directrices:

7.1. Disposiciones específicas:

a) Todas las Divisiones, Intendencia de Educación Parvularia y Direcciones Regionales de la SIE deberán contar con un Plan de Continuidad Operacional que considere, al menos, los procesos calificados como críticos o del negocio, de acuerdo al Formulario de Definiciones Estratégicas o en la Matriz de Riesgo Institucional.

b) Todas las Divisiones, Intendencia de Educación Parvularia y Direcciones Regionales deberán diseñar, documentar e implementar un Plan de Continuidad Operacional los cuales, según corresponda, deberán contar con la validación técnica del Departamento de Tecnologías y Procesos.

c) Los Planes de Continuidad Operacional deberán establecer la estructura organizacional de los mismos, con roles y funciones definidas.

d) Los Planes de Continuidad Operacional deberán establecer el protocolo de activación y desactivación.

e) Los Planes de Continuidad Operacional deberán ser evaluados al menos una vez al año, con el propósito de validar su eficacia.

f) Los resultados de las pruebas indicadas en el punto anterior, deberán ser registrados por el Departamento de Tecnologías y Procesos y comunicadas al Encargado/a de Seguridad de la Información y Ciberseguridad.

g) Los Planes de Continuidad Operacional deberán incluir la identificación de los principales eventos que puedan afectar la continuidad del o los procesos considerados como críticos, considerando factores como:

- Impactos en los procesos, costos financieros, cumplimientos normativos, tiempos de interrupción, entre otros.
- Impactos colaterales, tales como el daño a la imagen o credibilidad de la SIE.

h) Si el Plan de Continuidad Operacional de una División, Intendencia de Educación Parvularia o Dirección en particular, depende de la participación de otras Divisiones, Direcciones o áreas institucionales específicas, éstas deberán quedar establecidas en términos del ámbito, alcance, roles, funciones y responsabilidades.

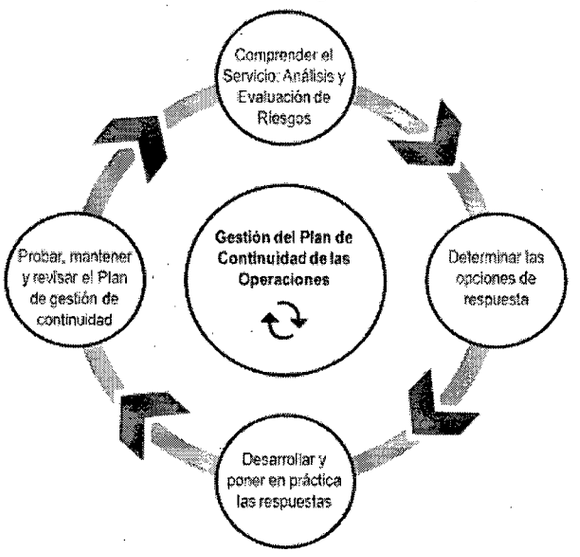
i) Las funciones de apoyo que entregue otro equipo de trabajo, deberán ser previamente acordadas y validadas con el responsable del área, según corresponda.

j) El ámbito, alcance, roles, funciones y responsabilidades que deba cumplir el DTP en relación a los Planes de Continuidad Operacional de las Divisiones, Intendencia de Educación Parvularia o Direcciones, deberán quedar establecidas mediante un acuerdo escrito y firmado con la jefatura de dicho Departamento.

k) A su vez, respecto de la Infraestructura Tecnológica que administra, el Departamento de Tecnología y Procesos deberá implementar uno o más Planes de Continuidad Operacional acordes con esta política, con el objetivo de velar por la continuidad de sus procesos y los procesos de las Divisiones, Intendencia de Educación Parvularia o Direcciones que emplean sistemas o servicio provistos por la plataforma TI y que es administrada por este Departamento.

7.2.Estructura general de la continuidad de operaciones:

La presente política establece una estructura para gestionar la continuidad del negocio. Esta estructura es representada mediante las siguientes etapas:



a) Etapa I: Comprender la organización en base al análisis y evaluación de riesgos:

Esta etapa consiste en identificar aspectos importantes de los activos de información para la entrega de bienes y servicios de la SIE, con el objetivo de preservar la seguridad de la información y, por consiguiente, mantener la continuidad de las operaciones de la institución. Estas actividades se sustentan en una identificación de los activos de información y sus riesgos, de acuerdo al inventario de activos vigente, para luego continuar con una evaluación de los riesgos y un análisis del impacto de tales interrupciones, bajo diversos escenarios en que se materializan estos riesgos.

b) Etapa II: Determinar las opciones de respuesta para gestionar la continuidad de las operaciones:

A partir de los riesgos, es necesario establecer las opciones de respuestas del plan de gestión de continuidad de las operaciones frente a los diferentes escenarios de riesgo que podría repercutir en la continuidad de las actividades de SIE.

c) Etapa III: Desarrollar y poner en práctica las respuestas para la continuidad de las operaciones:

Esta etapa consiste en llevar a cabo las prácticas que permiten recuperar y restaurar las operaciones de la SIE y recobrar la disponibilidad de los activos de información en escalas de tiempo mínimas, mediante las opciones de respuesta mencionadas en la etapa anterior.

d) Etapa IV: Probar, mantener y revisar el Plan de Gestión de Continuidad:

Finalmente, esta etapa consiste en someter a pruebas y actualizar el Plan de gestión de continuidad de las operaciones para asegurar su actualización y mejora en su eficacia frente a potenciales riesgos. Esta actualización deberá ser realizada de forma anual o bien cuando ocurra algún cambio a registrar

7.3.Componentes del Plan de gestión de continuidad de las operaciones:

A partir de las etapas descritas en los puntos anteriores, a continuación, se establecen las materias que el plan de gestión de continuidad operacional debe abordar:

a) Una descripción de la planificación de la continuidad de las operaciones de la SIE, con el objetivo de mantener una sola estructura que permita asegurar que los planes de las Divisiones, Intendencia y Dirección Regional sean consistentes, abordando la seguridad de la información e identificando prioridades para pruebas y mantenimiento de respuestas.

b) Un plan de recuperación ante desastres o emergencias, el cual deberá contener:
   - Análisis de impacto ante potenciales escenarios.
   - Determinación de opciones de recuperación ante desastres o emergencias.
   - Respuesta ante desastres o emergencias, con las respectivas responsabilidades.
   - Prueba y mantenimiento de respuestas.

c) Planes de contingencias por centros de responsabilidad[1], relacionados a la provisión de productos, los cuales deberán contener:
   - Análisis y evaluación de los riesgos en las operaciones del Servicio, en cada proceso del alcance del SGSI.
   - Determinación de opciones de prevención o recuperación ante incidentes, fallas o interrupción de servicios.
   - Desarrollo y puesta en práctica de respuestas para la continuidad de las operaciones.
   - Prueba, mantención y revisión del plan de gestión de continuidad de las operaciones.

7.4.Consideraciones generales:

a) Frente a eventos mayores y que afecten transversalmente a todas las Divisiones, Intendencia de Educación Parvularia o Direcciones Regionales, el/la Encargado/a de Seguridad de la Información y Ciberseguridad, la jefatura del Departamento de Tecnología y Procesos y el Comité Operativo de Seguridad de

[1] Los centros de responsabilidad podrán hacer referencia a las etapas de los procesos transversales en los que participan, específicamente, los procesos identificados en la matriz de riesgos vigente de la SIE.

Información, en caso de que sea necesario, deberán coordinar los planes y acciones de mitigación con el Jefe de Gabinete del Superintendente.

b) El diseño e implementación de los Planes de Continuidad Operacional de las Divisiones, Intendencia de Educación Parvularia y las Direcciones Regionales, deberán contar, al menos, con la participación de las jefaturas o encargados/as de los Departamentos, Unidades o Áreas responsables o involucrados en los procesos considerados en estos planes.

c) Respecto de las pruebas para validar los Planes de Continuidad Operacional, estas deberán ser coordinadas en conjunto con el Departamento de Tecnología y Procesos, cada vez que estas requieran contar con activos de información, tales como sistemas, aplicaciones, respaldos de datos, u otros.

d) Cada plan de continuidad deberá ser difundido entre los funcionarios del área y la responsabilidad de recaerá en el Jefe de División, Intendenta o Director Regional.

e) El Departamento de Tecnologías y Procesos, junto a los Jefes de División, Intendenta y Directores Regionales. deberán definir un protocolo para comunicar y coordinar las actividades tanto de activación, ejecución y desactivación del mismo.

8. Evaluación y difusión:

La presente política será evaluada por el Superintendente de Educación una vez al año, o bien, cuando se produzca un cambio significativo que la impacte, esto con la finalidad de asegurar su continua idoneidad, eficiencia y efectividad.

Una vez que el documento entre en vigencia el/la Encargado/a de Seguridad de la Información y Ciberseguridad, deberá difundir al personal y externos considerado en el alcance, mediante cualquier vía que permita comunicar la creación o modificaciones efectuadas. Estas vías podrán ser intranet, correo electrónico al personal, capacitaciones, difusiones, etc.

9. Revisión del cumplimiento de la política

Con una periodicidad concordante a la de la evaluación definida en el punto anterior, y a través de auditorías, ya sean internas o externas, y en tanto los recursos institucionales se encuentren disponibles para ello, se revisará el cumplimiento de la presente política con la finalidad de recabar información que permita definir modificaciones en pro del cumplimiento de la misma.

10.Aceptación

Todos los usuarios de la SUPEREDUC, sean planta, contrata, honorarios, asesores, consultores, practicantes, y otros trabajadores, deben aceptar ésta política y procedimientos relacionados.

Para el caso de terceros y por solo hecho de participar en algún proceso de compras del servicio, el oferente debe dar cumplimiento a la política, manuales y procedimientos vigentes de seguridad de la información de la SUPEREDUC, publicados en el sitio web www.supereduc.cl y sus correspondientes modificaciones, la cuales se presumen conocidas por el contratista o adjudicatario para todos los efectos legales.

11.Sanciones

El incumplimiento o violación a esta Política, de las Políticas específicas del Sistema, Procedimientos u otros documentos que se deriven de éstos, debidamente acreditado, conlleva a la aplicación de medidas disciplinarias previstas en el Estatuto Administrativo, respecto a los funcionarios/as de la SUPEREDUC, o al término anticipado del contrato por incumplimiento de obligaciones, cuando se trate de personas que no tengan responsabilidad administrativa o empresas que se encuentren dentro del alcance de la presente política, sin perjuicio de las responsabilidades civiles y penales que se deriven de tales infracciones.

12.Excepciones

La presente Política, y las Políticas específicas asociadas, admitirán excepciones en su aplicación, siempre y cuando, existan casos con razones fundadas, los cuales serán documentados por el/la Encargado/a de Seguridad de la Información y Ciberseguridad y debidamente autorizados por la Jefatura de Gabinete.

REVISIONES DE LA POLÍTICA			
Nº Versión	**Fecha**	**Motivo de la revisión**	**Paginas elaboradas o modificadas**
Versión 0	18-12-2019	Versión inicial	Todas las páginas

2° ESTABLÉZCASE, que la política que por medio de la presente Resolución Exenta se aprueba, comenzará a regir de manera inmediata una vez que esta haya quedado totalmente tramitada.

3° DÉJASE, expresa constancia que la presente Resolución Exenta no irroga gasto alguno para esta Superintendencia de Educación.

4° DÉJASE, sin efecto toda Resolución Exenta o acto administrativo que regule de forma específica la materia, en la Superintendencia de Educación.

5° REMÍTASE, copia de la presente Resolución Exenta todas las Divisiones, Intendencia, Direcciones Regionales, Departamentos, Unidades y de la Superintendencia de Educación, de acuerdo con la distribución indicada en la presente resolución

6° PUBLÍQUESE, una vez totalmente tramitada la presente Resolución Exenta, en la Intranet institucional y el sitio web www.supereduc.cl.

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE.

REPUBLICA DE CHILE
SUPERINTENDENCIA DE EDUCACION
SUPERINTENDENTE

CRISTIÁN O'RYAN SQUELLA
SUPERINTENDENTE DE EDUCACIÓN

Distribución:

- Gabinete Superintendente.
- Jefes/as de División.
- Intendente/a de Educación Parvularia.
- Directores Regionales I a XVI región.
- Jefe/a Departamento de Finanzas.
- Jefe/a Departamento Gestión y Desarrollo de Personas.
- Jefe/a Departamento de Administración.
- Jefe/a Departamento de Tecnologías y Procesos de Información.
- Departamento de Gestión Institucional.
- Departamento de Auditoria.
- Unidad de Transparencia.
- Encargado de Ciberseguridad de la Información.
- Oficina de Partes