POR EL CUIDADO Y BUEN USO
DE LOS RECURSOS PÚBLICOS

DEPARTAMENTO DE AUDITORÍAS ESPECIALES

UNIDAD DE AUDITORÍAS DE SISTEMAS

INFORME FINAL

SUBSECRETARÍA DEL MEDIO AMBIENTE

INFORME N° 630 / 2021

OBJETIVOS
DE DESARROLLO
SOSTENIBLE

OBJETIVOS DE DESARROLLO SOSTENIBLE

POR EL CUIDADO Y BUEN USO
DE LOS RECURSOS PÚBLICOS

ÍNDICE

GLOSARIO

TÉRMINO	CONCEPTO
Antispam	Es una solución de software que permite a los usuarios prevenir o restringir la entrega de spam (correos no deseados). Analiza automáticamente todos los correos electrónicos entrantes enviados a un buzón de correo. Aplicación o herramienta informática que se encarga de detectar y eliminar el spam y los correos no deseados. [1]
API	Del inglés application programming interface, o interfaz de programación de aplicaciones, es un conjunto de subrutinas, funciones y procedimientos que ofrece cierta biblioteca de funcionalidades para ser utilizada por otro software.[2]
Aplicativos	Es una alternativa adecuada en español para referirse a app, un acortamiento del término inglés application, que se utiliza para aludir a un "tipo de programa informático diseñado como herramienta que permite al usuario realizar diversos trabajos".[3]
AVAMAR	Sistema de hardware/software de respaldo y recuperación que permite eliminar los datos de respaldo redundantes en un cliente antes del almacenamiento de los datos. [4]
Business Intelligence	Es la habilidad para transformar los datos en información, y la información en conocimiento, de forma que se pueda optimizar el proceso de toma de decisiones en los negocios.[5]
Cloud	Sitios externos donde se ejecutan aplicaciones o almacena información. [6]
Delegado de sistemas	Usuario que ha sido designado por el encargado del establecimiento, otorgándole los permisos necesarios para acceder al sistema sectorial específico de un establecimiento. [7]
Encargado de Establecimiento o Encargado	Cargo responsable en materias ambientales dentro del establecimiento, quien deberá informar las modificaciones del mismo en el Sistema Ventanilla Única del RETC; tales como, actualización de razón social, cambio de titularidad, cese de funciones, administración de usuarios delegados; cambio de encargado del establecimiento y representante legal. [8].
Grupo Nacional Coordinador, GNC	Es un comité operativo que se encuentra a cargo de la coordinación, análisis y gestión en la operación del RETC, integrado por representantes de los distintos servicios o instituciones públicas que incluye al sector privado, la sociedad civil organizada y el sector académico. [9]

1 Fuente: https://es.wikipedia.org/wiki/Antispam.
2 Fuente: https://es.wikipedia.org/wiki/Interfaz_de_programaci%C3%B3n_de_aplicaciones.
3 Fuente: https://www.fundeu.es/recomendacion/aplicacion-alternativa-a-app/.
4 Fuente: https://www.dell.com/support/home/es-cl/product-support/product/avamar-server/docs.
5 Fuente: https://www.sinnexus.com/business_intelligence/
6 Fuente: https://www.redhat.com/es/topics/cloud.
7 Fuente: https://vu.mma.gob.cl/manuals/vu/manual_vu.pdf.
8 Fuente: En base a la documentación proporcionada por el organismo mediante correo de 24 de marzo de 2021.
9 Fuente: https://retc.mma.gob.cl/gnc/.

TÉRMINO	CONCEPTO
Enlaces del RETC.	Aquellos funcionarios de un órgano de la Administración del Estado que sean parte del GNC, a los cuales se les asigne la labor de enviar, recibir, generar, recopilar, obtener y validar la información de emisiones, residuos, transferencias de contaminantes y productos prioritarios. [10]
ETL, Extract - Transform – Load	Extraer, Transformar, Cargar: Es un método en el que los datos extraídos se cargan primero en el sistema de destino. Las transformaciones se realizan después de cargarlos en el almacén. En lugar de transformarlos antes de que se escriban, ELT permite que el sistema de destino realice la transformación. [11]
Exploit	Es un programa informático, una parte de un software o una secuencia de comandos que se aprovecha de un error o vulnerabilidad para provocar un comportamiento no intencionado o imprevisto en un software, hardware o en cualquier dispositivo electrónico. Estos comportamientos incluyen, por lo general, la toma del control de un sistema, la concesión de privilegios de administrador al intruso o el lanzamiento de un ataque de denegación de servicio. [12]
Firewall	Un cortafuego es la parte de un sistema informático o una red que está diseñada para bloquear el acceso no reconocido, permitiendo al mismo tiempo comunicaciones autorizadas. Pueden ser implementados en hardware o software, o en una combinación de ambos.[13]
Framework	Es una estructura base utilizada como punto de partida para elaborar un proyecto con objetivos específicos. [14]
GET/POST	Son dos técnicas que pueden enviar los datos a un servidor o navegador para su comunicación. [15]
Inyección SQL	Es un método de infiltración de código intruso que se vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar operaciones sobre una base de datos. [16]
JWT	JSON Web Token (JWT) es un estándar abierto (RFC 7519) que define una forma compacta y autónoma de transmitir información de forma segura entre las partes como un objeto JSON -notación de objeto de lenguaje JavaScript-. Esta información puede ser verificada y confiable porque está firmada digitalmente. [17]

10 Fuente: En base a la documentación proporcionada por el organismo mediante correo de 24 de marzo de 2021.
11 Fuente: https://www.baoss.es/elt-o-etl-que-es-mejor/
12 Fuente: https://www.pandasecurity.com/es/security-info/exploit/
13 Fuente: https://es.wikipedia.org/wiki/Cortafuegos_(inform%C3%A1tica)
14 Fuente: https://rockcontent.com/es/blog/framework/
15 Fuente: https://pc-solucion.es/2018/06/06/diferencias-entre-el-metodo-get-y-post/
16 Fuente: https://es.wikipedia.org/wiki/Inyecci%C3%B3n_SQL
17 Fuente: https://jwt.io/introduction

TÉRMINO	CONCEPTO
Malware	Se llama programa malicioso, programa maligno, programa malintencionado, en inglés malware (acortamiento de malicious software), a cualquier tipo de software que realiza acciones dañinas en un sistema informático de forma intencionada y sin el conocimiento del usuario. [18]
Nodo	Es un punto de intersección, conexión o unión de varios elementos que confluyen en el mismo lugar.[19]
NGF	Los Next-Generation Firewall filtran el tráfico de red para proteger a una organización de amenazas internas y externas. Además de mantener las características de los cortafuegos con estado, como el filtrado de paquetes, la compatibilidad con IPsec y VPN SSL, la supervisión de la red y las funciones de mapeo de IP.[20]
OAuth2	Es un estándar abierto para la autorización de APIs, que permite compartir información entre sitios sin tener que compartir la identidad. Es un mecanismo utilizado al día de hoy por compañías como Google, Facebook, Microsoft, Twitter, GitHub o LinkedIn, entre otras muchas. [21]
PMG	Los Programas de Mejoramiento de la Gestión, PMG, en los servicios públicos tienen su origen en la ley N° 19.553, que Concede Asignación de Modernización y otros Beneficios que Indica; y asocian el cumplimiento de objetivos de gestión a un incentivo de carácter monetario para los funcionarios. [22]
PRTG	Software de monitorización proactiva de red, que monitoriza continuamente dispositivos, sistemas y aplicaciones de tu infraestructura TI, proporcionando informes de estado y permitiendo generar alertas cuando se produce un error o los umbrales críticos se sobrepasan. [23]
SLA	Es un acuerdo escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio, también conocidas por las siglas SLA (del inglés Service Level Agreement)..[24]
Stakeholder	Es una persona, entidad o empresa que tiene interés en una organización.[25]

18 Fuente: En base a lo indicado en https://es.wikipedia.org/wiki/Malware.
19 Fuente: https://es.wikipedia.org/wiki/Nodo_(inform%C3%A1tica)
20 Fuente: https://www.fortinet.com/lat/products/next-generation-firewall.
21 Fuente: https://openwebinars.net/blog/que-es-oauth2/.
22 Fuente: https://www.dipres.gob.cl/598/w3-propertyvalue-15230.html.
23 Fuente: https://www.danysoft.com/prtg/.
24 Fuente: https://es.wikipedia.org/wiki/Acuerdo_de_nivel_de_servicio.
25 Fuente: https://es.wikipedia.org/wiki/Interesado (empresa)

TÉRMINO	CONCEPTO
RETC	El Registro de Emisiones y Transferencias de Contaminantes es una base de datos accesible al público, destinada a capturar, recopilar, sistematizar, conservar, analizar y difundir la información sobre emisiones, residuos y transferencias de contaminantes potencialmente dañinos para la salud y el medio ambiente que son emitidos al entorno, generados en actividades industriales o no industriales o transferidos para su valorización o eliminación. [26]
RUEA	Reporte Único de Emisiones Atmosféricas, y corresponde a la actualización del sistema de declaración F138. El objetivo de este módulo es realizar la cuantificación de emisiones mediante factores de emisión o con información precargada desde otros sistemas de reporte (tanto de la Superintendencia del Medio Ambiente y de los Ministerios de Salud y del Medio Ambiente, tales como; Sistema de Centrales Termoeléctricas, Sistema de Impuestos Verdes y Formulario Electrónico - F138. [27]
Sistema sectorial	Sistema en el cual se debe reportar la información para dar cumplimiento a la normativa ambiental vigente, los cuales son administrados por distintos servicios públicos con competencia en la materia. [28]
UPS	Un UPS llamado en inglés Uninterruptible Power Supply, es una fuente de alimentación ininterrumpida, contiene una batería que mantiene una computadora o un sistema eléctrico en funcionamiento cuando existe un corte de energía. [29]
Ventanilla Única	VU, Sistema electrónico que contempla un formulario único disponible en el portal electrónico del RETC y a través del cual se accederá a los sistemas de declaración de los órganos fiscalizadores, para dar cumplimiento a la obligación de reporte de los establecimientos emisores o generadores. [30]
VMWare	Sistema que permite operar con software, emulando a un sistema físico (un computador, un hardware, etc.) con características de hardware determinadas. Cuando se ejecuta el programa (simulador) proporciona un ambiente de ejecución similar a todos los efectos de un computador físico (excepto en el puro acceso físico al hardware simulado), con CPU (puede ser más de una), BIOS, tarjeta gráfica, memoria RAM, tarjeta de red, sistema de sonido, conexión USB, disco duro (pueden ser más de uno), etc. [31]
Webservice	Un servicio web (en inglés, web service o web services) es una tecnología que utiliza un conjunto de protocolos y estándares que sirven para intercambiar datos entre aplicaciones. [32]

26 Fuente: Artículo 1°, del decreto N° 1 de 2013, del Ministerio de Medio ambiente, que Aprueba Reglamento del Registro de Emisiones y Transferencias de Contaminantes.
27 Fuente: Manual de usuario, https://vu.mma.gob.cl/manuals/ruea/manual_RUEA.pdf.
28 Fuente: https://vu.mma.gob.cl/manuals/vu/manual_vu.pdf
29 Fuente: https://www.worldcomputers.com.ec/que-es-un-ups/
30 Fuente: https://vu.mma.gob.cl/manuals/vu/manual_vu.pdf
31 Fuente: https://es.wikipedia.org/wiki/VMware.
32 Fuente: https://es.wikipedia.org/wiki/Servicio_web.

CONTRALORÍA GENERAL DE LA REPÚBLICA
DEPARTAMENTO DE AUDITORÍAS ESPECIALES
UNIDAD DE AUDITORÍA DE SISTEMAS

Resumen Ejecutivo Informe Final N° 630, de 2021.

Auditoría a la plataforma del Registro de Emisiones y Transferencias de Contaminantes, RETC.

Subsecretaría del Medio Ambiente

Objetivo: Efectuar una auditoría a la plataforma del Registro de Emisiones y Transferencias de Contaminantes, RETC[33], de la Subsecretaría del Medio Ambiente, SMA.

El examen tuvo por finalidad verificar su operación, seguridad, disponibilidad, confidencialidad, como, asimismo, su interoperabilidad con otras plataformas tanto internas como externas.

Además, de manera complementaria, revisar el cumplimiento administrativo de los contratos denominados "Actualización Sistema Ventanilla Única 2.0 del RETC y sistemas asociados", con la empresa Blue Company S.A.; y "Actualización del Reporte Único de Emisiones Atmoféricas (RUEA), y nodo central del RETC", con la compañía TIC BLUE Limitada.

Todo lo anterior, durante el período comprendido entre el 1 de enero y 31 de diciembre de 2020.

Preguntas de la Auditoría:

- ¿Ha implementado la SMA medidas para garantizar la continuidad operacional?
- ¿Cuenta la plataforma tecnológica de la repartición con controles generales que permitan resguardar los sistemas?
- ¿Posee la entidad controles tendientes a proteger la seguridad física del centro de procesamiento de datos?
- ¿Existen procedimientos para la validación de la integridad del sistema RETC?
- ¿Se encuentra la plataforma auditada en operación de acuerdo con los requerimientos técnicos y a la normativa vigente que lo regula?
- ¿Ha desarrollado e implementado la institución una política de seguridad de la información que le permita resguardar la integridad, confidencialidad y disponibilidad de los sistemas?

Principales Resultados:

- Se advirtió que el "Procedimiento de Gestión de Eventos e Incidentes de Seguridad de la Información" no establece mecanismos tendientes a contrarrestar interrupciones a las actividades del negocio y proteger sus procesos críticos frente a los efectos de fallas importantes en los sistemas de información o contra desastres, de manera de asegurar su restauración oportuna, generando un

33 Base de datos destinada a capturar, recopilar, sistematizar, conservar, analizar y difundir la información sobre emisiones, residuos y transferencias de contaminantes potencialmente dañinos para la salud y el medio ambiente.

eventual riesgo de indisponibilidad de los servicios provistos por la infraestructura de la SMA.

Corresponde que la repartición remita la mejora de los procedimientos actuales y del control en el monitoreo, especialmente en lo referido al respaldo y restauración de información, en el término de 60 días hábiles, a contar desde la recepción del presente documento.

Asimismo, se constató que el Departamento de Tecnologías de la Información y las Comunicaciones de la repartición no ha confeccionado un plan de contingencia que permita asegurar el funcionamiento de los sistemas de información ante un eventual desastre en las salas de servidores a causa de un terremoto, incendio, inundación u otro evento imprevisto, con el propósito de recuperar los aplicativos que soportan las operaciones críticas de la institución.

La SMA deberá elaborar dicho instrumento e informar sobre su estado de avance en el plazo de 60 días hábiles contado desde la recepción del presente informe final.

- La repartición indicó que no se registraron incidentes de seguridad en el período fiscalizado, sin embargo, esta no acompañó información y reportes que comprueben el monitoreo de la actividad de red, detección de intrusos e intentos de accesos no permitidos a la plataforma institucional.

  Al respecto, el referido "Procedimiento de Gestión de Eventos e Incidentes de Seguridad de la Información" señala que se deben elaborar el "Reporte trimestral de la gestión de eventos e incidentes de seguridad de la información" y el "Reporte de incidentes de seguridad de la información", los que no fueron proporcionados por la entidad auditada.

  La omisión de los reportes mencionados no permite advertir las debilidades de seguridad de la información y detectar incidentes de seguridad de la misma y que puedan causar daños en la infraestructura tecnológica de la institución.

  La SMA deberá remitir el documento sancionado que contenga la calendarización de las fechas de recopilación de los reportes, evidencias y registros periódicos, conforme lo contemplado en el Compromiso de Desempeño Colectivo, en el plazo de 60 días hábiles contado desde la recepción del presente informe final.

  Además, se constató que si bien la SMA cuenta con el "Procedimiento de Control de Instalación de Softwares", el cual describe las actividades a realizar en en estaciones de trabajo y notebooks de la repartición, a fin de evitar que sea afectada la disponibilidad, confidencialidad o integridad de los activos de información por el ataque a las vulnerabilidades que estos puedan sufrir o infecciones por malware, en dicho documento solo se establecen procedimientos de configuración para equipamiento menor y equipos de usuarios finales, no considerando en sus definiciones, los parámetros que dicha configuración debe tener para asegurar el correcto funcionamiento de los aplicativos instalados en los equipos de los funcionarios.

Adicionalmente, la SMA cuenta con una "Política de Seguridad para las Operaciones" donde se disponen las reglas generales para garantizar las operaciones correctas y seguras de las instalaciones de procesamiento de datos, y define directrices para el resguardo de la información soportada en su plataforma tecnológica, y el aseguramiento de la integridad de los sistemas operacionales.

Sin embargo, dicha política no considera los procedimientos para aplicar la configuración y modificación de los parámetros de los sistemas operativos, bases de datos, cortafuegos, enrutadores, entre otros, y que establezcan las responsabilidades y procedimientos formales que le permitan asegurar su correcto funcionamiento y puesta a punto para el RETC, con el consiguiente riesgo de que se realicen modificaciones no aprobadas o autorizadas determinando fallas o indisponibilidad de la plataforma informática y sus servicios.

La entidad deberá complementar su Política de Seguridad para las Operaciones, de manera de incorporar las omisiones advertidas por esta Entidad de Control, suministrando un informe de avance en el plazo de 60 días hábiles contado desde la recepción del presente documento.

- A través de la visita efectuada por esta Entidad de Fiscalización al Datacenter del Ministerio de Medio Ambiente, el 21 de julio de 2021, se confirmó que no existe un procedimiento oficial para ingresar al Centro de Procesamiento de Datos, con el consiguiente riesgo de no contar con un protocolo de acceso a la sala de servidores que evite que personal no autorizado entre a la misma provocando daño intencional o involuntario a las dependencias y/o a la información.

  Asimismo, se advirtió que la repartición no cuenta con un registro del personal que ingresa a las instalaciones, información que permite efectuar un seguimiento a las actividades ejecutadas al interior de la aludida sala y esclarecer responsabilidades administrativas ante eventuales amenazas y/o hechos consumados.

  La SMA deberá implementar un registro formal para la gestión de acceso, y bitácoras de ingreso a los espacios restringidos, para su continuo monitoreo, informando documentadamente en el plazo de 60 días hábiles contado desde la recepción del presente informe final.

  También se advirtió que, al momento de la visita a terreno, en las oficinas de la repartición existían baterías en desuso correspondientes a los equipos UPS[34], dispuestas en el pasillo que conduce a la entrada, situación que dificulta el desplazamiento y/o el escape en situaciones de emergencia, además del peligro de tener ese tipo de residuos sin las medidas mínimas de seguridad. Ello, además de vulnerar lo estipulado en el decreto N° 83, de 2004, del Ministerio Secretaría General de la Presidencia, sobre la gestión de las operaciones y las comunicaciones, transgrede lo estipulado en el artículo 6°, del decreto N° 148, de 2004, del Ministerio de Salud, que aprueba el reglamento sanitario sobre manejo de residuos peligrosos.

34 UPS: Es una fuente de alimentación ininterrumpida, contiene una batería que mantiene una computadora o un sistema eléctrico en funcionamiento cuando existe un corte de energía.

La entidad fiscalizada deberá gestionar el retiro de las baterías en desuso desde las dependencias del datacenter y su traslado a una entidad certificada que cumpla con la normativa vigente, respaldando dicha labor, en el plazo de 60 días hábiles contado desde la recepción del presente documento.

- La institución fiscalizada no cuenta con procedimientos formales relacionados con el proceso de verificación de eventuales errores en la estructura de los datos obtenidos de los sistemas que integran el RETC. Ello imposibilita diagnosticar la calidad de los datos y el eventual impacto en aquellos procesos automatizados que hacen uso de dicha información y que forman parte del RETC, en cuanto a la facilitar el acceso a la información sobre emisiones, residuos y transferencias de contaminantes.

  La entidad deberá desarrollar y remitir el procedimiento formalizado que incorpore las etapas y actividades de control que permitan la validación de la integridad de la información del aludido sistema, en el plazo de 60 días hábiles contado desde la recepción del presente informe final.

- La SMA cuenta con un procedimiento que entrega lineamientos generales para garantizar que el desarrollo y/o las mantenciones se realicen e implementen bajo entornos resguardados, con ejecución de pruebas de seguridad y aceptación a través de los criterios relacionados con las reglas y normas de su política. Tal documento, también establece qué requisitos del negocio son satisfechos por los sistemas existentes y cuáles lo serán en las nuevas propuestas o modificaciones antes de que sea aprobado el desarrollo, implementación o modificación del proyecto.

  Además, la entidad dispone de documentos que definen las características de nivel de aplicación, la integración y comunicación con los sistemas sectoriales, ambientes de desarrollo y de producción, asimismo cuenta con un documento que escribe los procesos y requisitos que deben cumplir esos sistemas para la integración con la Ventanilla Única 2.0 del RETC del Ministerio del Medio Ambiente.

  En tal sentido y a través de las pruebas realizadas por esta Entidad de Fiscalización a la plataforma, se constató que la operación del RETC sigue los lineamientos establecidos en la documentación revisada, acorde a los requerimientos técnicos y a la normativa vigente que lo regula no determinándose observaciones sobre la materia.

- La subsecretaría auditada cuenta con una "Política de Seguridad para las Comunicaciones", la cual establece los requerimientos de seguridad para una adecuada administración, implementación, diseño y protección de las redes de comunicación informática de la institución, así como de sus instalaciones de procesamiento de información de apoyo.

Por su parte, los sistemas informáticos en análisis poseen autenticación al servidor de Ministerio Secretaría General de la Presidencia[35], a través del protocolo OAuth2[36], lo que permite generar sesiones JWT[37] independientes, únicas y descentralizadas en materia de contraseñas.

Por lo anteriormente expuesto, no se advierten observaciones respecto a la implementación de una política de seguridad de la información.

35 Para validar el acceso mediante Clave Única.
36 OAuth2: Es un estándar abierto para la autorización de APIs, que permite compartir información entre sitios sin tener que compartir la identidad.
37 Es un estándar abierto que define una forma de transmisión de información compacta y autónoma, de forma segura entre las partes. Esta información puede ser verificada y confiable porque está firmada digitalmente.

CONTRALORÍA GENERAL DE LA REPÚBLICA
DEPARTAMENTO DE AUDITORÍAS ESPECIALES
UNIDAD DE AUDITORÍA DE SISTEMAS

PMET N° 34.021/2021

INFORME FINAL N° 630, DE 2021, SOBRE AUDITORÍA A LA PLATAFORMA DEL REGISTRO DE EMISIONES Y TRANSFERENCIAS DE CONTAMINANTES, RETC, DE LA SUBSECRETARÍA DEL MEDIO AMBIENTE, SMA.

SANTIAGO,

En cumplimiento del plan anual de fiscalización de esta Contraloría General para el año 2021, y en conformidad con lo establecido en la ley N° 10.336, de Organización y Atribuciones de la Contraloría General de la República, se efectuó una auditoría a la plataforma del Registro de Emisiones y Transferencia de Contaminantes y servicios asociados, RETC, administrada por la Subsecretaría del Medio Ambiente, para el período comprendido entre el 1 de enero y el 31 de diciembre de 2020.

JUSTIFICACIÓN

La ejecución de la presente auditoría se argumenta en la complejidad del proceso de Registro de Emisiones y Transferencias de Contaminantes, el cual contempla actividades automatizadas y manuales; la participación de múltiples usuarios, así como de diversos aplicativos informáticos, todos circunscritos a la plataforma RETC, situación que implica riesgo de deficiencias en su operación, asociadas a las cada una de las etapas del proceso, lo que puede derivar en reportes con información incompleta o errores, que no reflejen la realidad en la materia y por tanto, que impidan una adecuada fiscalización por parte de las entidades correspondientes o una apropiada toma de decisiones en el diseño de la política de gestión ambiental, con el impacto que ello puede generar a nuestro ecosistema, entre otros problemas.

Se consideró, además, la matriz de riesgo del Ministerio del Medio Ambiente, asociada a los procesos del RETC, donde se advierten situaciones relativas a la Ventanilla Única RETC y a la elaboración de los informes consolidados de emisiones y transferencias de contaminantes, con alta probabilidad de ocurrencia e impacto alto y severidad extrema. Como también, el informe institucional de auditoría N° 4, aseguramiento N° 9, sobre el RETC, de 2020, de la Oficina de Auditoría Interna de la SMA, el cual establece que el Sistema de Control

A LA SEÑORA
MARÍA REGINA RAMÍREZ VERGARA
JEFA DEL DEPARTAMENTO DE AUDITORÍAS ESPECIALES
PRESENTE

Contralor General de la República

Interno requiere mejoras, por cuanto la materia auditada da cuenta de debilidades de control que deben ser abordados por la institución, a efecto de que, una vez implementadas, éstas garanticen el control permanente y resguardo de los recursos públicos.

Asimismo, a través de la presente auditoría, esta Contraloría General busca contribuir a la implementación y cumplimiento de los 17 Objetivos de Desarrollo Sostenible, ODS, aprobados por la Asamblea General de las Naciones Unidas en su Agenda 2030, para la erradicación de la pobreza, la protección del planeta y la prosperidad de toda la humanidad.

En tal sentido, esta revisión se enmarca en los ODS Nºs. 11 Ciudades y Comunidades Sostenibles, 12 Producción y Consumo Responsable, 14 Vida Submarina, y 16, Paz, Justicia e Instituciones Sólidas, específicamente, con las metas 11.6, De aquí a 2030, reducir el impacto ambiental negativo per cápita de las ciudades, incluso prestando especial atención a la calidad del aire y la gestión de los desechos municipales y de otro tipo; 12.4 De aquí a 2020, lograr la gestión ecológicamente racional de los productos químicos y de todos los desechos a lo largo de su ciclo de vida, de conformidad con los marcos internacionales convenidos, y reducir significativamente su liberación a la atmósfera, el agua y el suelo a fin de minimizar sus efectos adversos en la salud humana y el medio ambiente; 14.3 Minimizar y abordar los efectos de la acidificación de los océanos, incluso mediante una mayor cooperación científica a todos los niveles; y 16.b Promover y aplicar leyes y políticas no discriminatorias en favor del desarrollo sostenible.

ANTECEDENTES GENERALES

Corresponde al Ministerio del Medio Ambiente liderar el desarrollo sustentable, a través de la generación de políticas públicas y regulaciones eficientes, promoviendo buenas prácticas y mejorando la educación ambiental ciudadana.

En este sentido, la ley N° 19.300, de Bases Generales del Medio ambiente, establece en el artículo 69 la creación del Ministerio del Medio Ambiente, como una Secretaría de Estado encargada de colaborar con el Presidente de la República en el diseño y aplicación de políticas, planes y programas en materia ambiental, así como en la protección y conservación de la diversidad biológica y de los recursos naturales renovables e hídricos, promoviendo el desarrollo sustentable, la integridad de la política ambiental y su regulación normativa.

Conforme a la letra p) del artículo 70 de ese cuerpo legal, corresponderá especialmente al Ministerio administrar un Registro de Emisiones y Transferencias de Contaminantes en el cual se registrará y sistematizará, por fuente o agrupación de fuentes de un mismo establecimiento, la naturaleza, caudal y concentración de emisiones de contaminantes que sean objeto de una norma de emisión, y la naturaleza, volumen y destino de los residuos sólidos generados que señale el reglamento.

Por último, dicho texto legal en el artículo 74 dispone la organización del Ministerio, y que será la siguiente:

a) El Ministro del Medio Ambiente.

b) El Subsecretario.

c) Las Secretarías Regionales Ministeriales del Medio Ambiente.

d) El Consejo Consultivo Nacional y los Consejos Consultivos Regionales.

Se instaura que un reglamento determinará la distribución temática en las divisiones del Ministerio, de conformidad a lo señalado en la ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado, cuyo texto refundido, coordinado y sistematizado ha sido fijado mediante el decreto con fuerza de ley N° 1, de 2001, del Ministerio Secretaría General de la Presidencia, las que deberán contemplar, a lo menos, las siguientes materias: Regulación Ambiental; Información y Economía Ambiental; Educación, Participación y Gestión Local; Recursos Naturales y Biodiversidad; Cambio Climático y Cumplimiento de Convenios Internacionales, y Planificación y Gestión.

En este sentido, por la resolución exenta N° 874, de 2018, se indica la Estructura y Organización de Oficinas del Ministerio del Medio Ambiente y Deja sin Efecto la resolución exenta N° 278, de igual año, del mismo ministerio, disponiendo en el artículo I las oficinas de a) De Planificación, Presupuesto y Control de Gestión; b) De Auditoría Interna; c) De Asuntos Internacionales; d) De Comunicaciones y Prensa; e) De Implementación Legislativa y Economía Circular; f) De Evaluación Ambiental; y g) De Cambio Climático.

Además, mediante la resolución exenta N° 873, de 2018, se establece y aprueba la estructura y Organización Interna para las Divisiones del Ministerio del Medio Ambiente y deja sin efecto la resolución exenta N° 345, de la misma anualidad y cartera de Estado.

Complementariamente, en los casos y forma que establezca el reglamento, el registro sistematizará y estimará el tipo, caudal y concentración total y por tipo de fuente, de las emisiones que no sean materia de una norma de emisión vigente. Para tal efecto, el Ministerio requerirá de los servicios y organismos estatales que corresponda, información general sobre actividades productivas, materias primas, procesos productivos, tecnología, volúmenes de producción y cualquiera otra disponible y útil a los fines de la estimación.

En este contexto, el decreto N° 1, de 2013, del Ministerio de Medio Ambiente, que Aprueba Reglamento del Registro de Emisiones y Transferencias de Contaminantes, indica que el RETC es una base de datos accesible al público, destinada a capturar, recopilar, sistematizar, conservar, analizar y difundir la información sobre emisiones, residuos y transferencias de contaminantes potencialmente dañinos para la salud y el medio ambiente que son emitidos al entorno, generados en actividades industriales o no industriales o transferidos para su valorización o eliminación.

Asimismo, el reglamento señala que el RETC dispondrá de manera sistematizada, por fuente o agrupación de fuentes, la naturaleza, caudal y concentración de emisiones de contaminantes que sean objeto de una norma de emisión.

Además, el registro incluye la declaración o estimación de emisiones, residuos y transferencias de aquellos contaminantes que no se encuentran regulados en una norma de emisión, plan de descontaminación, u otra regulación vigente, cuando se trate de emisiones que corresponden a fuentes difusas, o que se estiman debido a que se encuentran en convenios internacionales suscritos por Chile. Las estimaciones las realizará el Ministerio del Medio Ambiente mediante la información que entreguen los diferentes órganos de la Administración del Estado.

De igual modo, el registro contempla la cantidad, naturaleza, características, origen, destino y la gestión de los residuos generados por los establecimientos, de conformidad a lo dispuesto en el presente reglamento y, en particular, de los residuos de productos prioritarios.

Mediante el oficio N° E139948, de 20 de septiembre de 2021, de este origen, fue puesto en conocimiento del Subsecretario del Medio Ambiente, de manera reservada, el Preinforme de Observaciones N° 630 de la misma anualidad, con la finalidad de que formulará los alcances y precisiones que, a su juicio, procedieran, lo que aconteció a través del oficio Ord. N° 213.743, de 6 de octubre de 2021, de la Subsecretaria del Medio Ambiente.

OBJETIVO

Efectuar una auditoría a la plataforma del Registro de Emisiones y Transferencias de Contaminantes, RETC, de la Subsecretaría del Medio Ambiente, para el período comprendido entre el 1 de enero y el 31 de diciembre de 2020.

El examen tuvo por finalidad verificar su operación, seguridad, disponibilidad, confidencialidad, como, asimismo, su interoperabilidad con otras plataformas tanto internas como externas.

Además, revisar el cumplimiento de los contratos suscritos con las empresas proveedoras para la actualización de la Ventanilla Única y sistemas asociados, con la empresa Blue Company S.A.; y para la actualización del Reporte Único de Emisiones Atmoféricas, RUEA, y nodo central del RETC, con la compañía Tic Blue limitada.

Cabe precisar que ambos desarrollos interoperan con la aludida plataforma. El detalle del proceso del RETC se muestra en el Anexo N° 1, y el de los contratos aludidos en los Anexos N^{os} 2 y 3.

La revisión incluyó la verificación del cumplimiento de las funciones de supervisión de los procedimientos y operaciones que se realizan en dicho contexto, para comprobar que estos cumplan con lo establecido en la normativa que regula la materia.

También se evaluó el cumplimiento de la normativa relacionada con las TIC, de conformidad con lo dispuesto en los decretos Nos 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; y 181, de 2002, que Aprueba Reglamento de la Ley N° 19.799, sobre Documentos Electrónicos, Firma Electrónica y la Certificación de dicha Firma, del entonces Ministerio de Economía, Fomento y Reconstrucción, actual Ministerio de Economía, Fomento y Turismo.

METODOLOGÍA

La revisión se realizó de acuerdo con las disposiciones contenidas en la resolución N° 20, de 2015, que Fija Normas que Regulan las Auditorías Efectuadas por la Contraloría General de la República, y con los procedimientos sancionados por la resolución exenta N° 1.485, de 1996, que Aprueba Normas de Control Interno, de este origen, considerando la evaluación de control interno, la ejecución de pruebas de validación, análisis de la información recopilada, y entrevistas con el personal responsable, entre otras pruebas de auditoría, en la medida que se estimaron necesarias.

Las observaciones que la Contraloría General formula con ocasión de las fiscalizaciones que realiza se clasifican en diversas categorías, de acuerdo con su grado de complejidad. En efecto, se entiende por Altamente complejas (AC)/Complejas (C), aquellas observaciones que, de acuerdo con su magnitud, reiteración, detrimento patrimonial, graves debilidades de control interno, eventuales responsabilidades funcionarias, son consideradas de especial relevancia por la Contraloría General; en tanto, se clasifican como Medianamente complejas (MC)/Levemente complejas (LC), aquellas que tienen menor impacto en esos criterios.

UNIVERSO Y MUESTRA

El examen contempló la revisión de la operación, seguridad, disponibilidad, confidencialidad, y la interoperabilidad de la plataforma RETC.

Además, mediante un muestreo analítico, se eligieron dos aplicativos que interactúan con dicha plataforma RETC, considerando el *impacto que deficiencias presentadas en ellos pueden ocasionar en el control de los* contaminantes atmosféricos, lo que equivale al 16,67% del universo de los sistemas institucionales.

Tabla N° 1: Universo y Muestra

Materia Específica	Universo		Muestra Estadística		Total Examinado	
	$	#	$	#	$	%
Sistemas Institucionales	0	12	0	2	0	16,67

Fuente: Elaborado en base a información suministrada mediante correo electrónico de la Jefa de Auditoría Interna de la institución fiscalizada, del 18 de febrero de 2021.

RESULTADO DE LA AUDITORÍA

El resultado de la auditoría practicada se expone a continuación:

I. ASPECTOS DE CONTROL INTERNO

Como cuestión previa, es útil indicar que el control interno es un proceso integral y dinámico que se adapta constantemente a los cambios que enfrenta la organización, es efectuado por la alta administración y los funcionarios de la entidad, está diseñado para enfrentar los riesgos y para dar una seguridad razonable del logro de la misión y objetivos de la entidad; cumplir con las leyes y regulaciones vigentes; entregar protección a los recursos de la entidad contra pérdidas por mal uso, abuso, mala administración, errores, fraude e irregularidades, así como también, para la información y documentación, que también corren el riesgo de ser mal utilizados o destruidos.

En este contexto, el estudio de la estructura de control interno de la entidad y de sus factores de riesgo, permitió obtener una comprensión del entorno en que se ejecutan las operaciones relacionadas con la materia auditada, del cual se desprenden las siguientes observaciones:

1. Situaciones de riesgo no controlados por el servicio

1.1 Falta de procedimientos de recuperación de desastres.

Mediante correo electrónico de 22 de marzo de 2021, la Oficina de Auditoría Interna de la Subsecretaría del Medio Ambiente remitió el documento titulado "Política de Seguridad de las Operaciones", Código: SSI.PO.12, Versión noviembre 2019, que entrega las reglas generales para garantizar las operaciones correctas y seguras de las instalaciones de procesamiento de información, definiendo las directrices para el adecuado resguardo de la información soportada en la plataforma tecnológica de esa subsecretaría.

De dicha documentación no se advirtió que el Departamento de Tecnologías de la Información y las Comunicaciones haya confeccionado un plan de contingencia que permita asegurar el funcionamiento de los sistemas de información ante un eventual desastre en las salas de servidores a causa de un terremoto, incendio, inundación u otro evento imprevisto, con el propósito de recuperar los aplicativos que soportan las operaciones críticas de la institución.

Por ello, se solicitó a ese servicio información al respecto, la que fue remitida a través del correo electrónico de 1 de septiembre de 2021, de la Oficina de Auditoría Interna de la mencionada subsecretaría, donde se acompaña el Procedimiento Gestión de Eventos e Incidentes de Seguridad de la Información mediante el cual se describen los pasos necesarios para atender de forma rápida y eficaz los eventos e incidentes de seguridad de la información que afecten o puedan afectar la integridad, confidencialidad y disponibilidad de la información crítica de la Subsecretaría del Ministerio del Medio Ambiente, incluyendo el contacto con las

autoridades pertinentes, a fin de controlar la situación, evitar propagación de los daños y tomar acciones para evitar su recurrencia.

Del análisis de los antecedentes antes mencionados, se advierte que en dicho procedimiento no se establecen los pasos a seguir tendientes a contrarrestar interrupciones a las actividades del negocio y proteger los procesos críticos del negocio de la entidad, contra los efectos de fallas importantes en los sistemas o contra desastres, y asegurar su restauración oportuna, generando un eventual riesgo de indisponibilidad de los servicios provistos por la infraestructura de la Subsecretaria del Medio Ambiente.

Lo anterior no se alinea con el principio de control previsto en el artículo 24, letra c), del citado decreto N° 83, de 2004, que señala que deberá garantizarse la disponibilidad de infraestructura adecuada de respaldo, para asegurar que éstos estén disponibles incluso después de un desastre o la falla de un dispositivo.

Asimismo, contraviene lo dispuesto en el acápite 14.1.3, de la Norma Chilena NCh-ISO N° 27.002, de 2009, el cual señala que se deberían desarrollar e implementar planes para mantener o restaurar las operaciones y asegurar la disponibilidad de la información en el grado y la escala de tiempo requeridos, después de la interrupción o la falla de los procesos críticos.

Tampoco se ajusta con lo estipulado en los numerales 38 y 39, de la resolución exenta N° 1.485, de 1996, de esta Contraloría General, que establecen que los directivos deben vigilar continuamente sus operaciones y adoptar inmediatamente las medidas oportunas ante cualquier evidencia de irregularidad o de actuación contraria a los principios de economía, eficiencia o eficacia, y que la vigilancia de las operaciones asegura que los controles internos contribuyen a la consecución de los resultados pretendidos, agregando que esta tarea debe incluirse dentro de los métodos y procedimientos seleccionados por la dirección para controlar las operaciones y garantizar que las actividades cumplan los objetivos de la organización.

La repartición indicó en su respuesta que actualmente existe en la institución el procedimiento de respaldo y restauración de información (Código: SSI.PR.12.03.01), tanto de los servidores físicos como virtuales, y que se definirá uno de recuperación ante desastre que incluirá roles y responsabilidades, estructura comunicacional, acciones a seguir, tiempos o SLA y criticidad de los sistemas, por lo cual se está trabajando en planificar su implementación para el primer semestre del año 2022.

Agregó que en el caso de los sistemas y, en particular, con el área de negocios de Información Ambiental, también se está trabajando en planificar para el año 2022, la implementación y calendarización del procedimiento existente, teniendo como insumo la documentación entregada por el área mencionada, para llevar el control de las actividades por parte de TI, dado que ella es independiente y cuenta con profesionales que desarrollan y mantienen sus sistemas, por lo cual se hace necesario definir los alcances de las actividades de

recuperación ante desastres, para lo cual, se debe establecer la criticidad de los sistemas a su cargo.

Considerando que lo manifestado por la institución auditada contempla una medida que no ha sido implementada, corresponde mantener lo objetado, por lo que la repartición deberá elaborar dicho instrumento e informar sobre su estado de avance en el plazo de 60 días hábiles contado desde la recepción del presente informe final.

1.2 Ausencia de un procedimiento para el control de los cambios realizados en los sistemas informáticos en operación en el RETC.

Por el precitado correo electrónico de 22 de marzo de 2021, la oficina de Auditoría Interna remitió el documento titulado "Procedimiento para el Desarrollo de Sistemas de Información Seguros", Código: SSI_PR_1_40206_1_40208_1_40209, versión de octubre 2019, que entrega los lineamientos generales para garantizar que el desarrollo de sistemas de información y/o mantenciones de estos se diseñen e implementen bajo entornos de desarrollo seguro, ejecución de pruebas de seguridad, y aceptación los mencionados aplicativos a través de los criterios relacionados a las reglas y normas de su política que lo contiene, dando cumplimiento a un desarrollo seguro y establece qué requisitos del negocio son satisfechos por los sistemas existentes y cuáles lo serán en las nuevas propuestas o modificaciones a los mismos (programas, datos e infraestructura) antes de que sea aprobado el desarrollo, implementación o cambios del proyecto.

Asimismo, se tuvo a la vista el "Procedimiento de Control de Instalación de Software", Código: SSI_PR_12_05_01, de noviembre 2019, mediante el cual de describen las actividades para controlar la instalación de softwares en estaciones de trabajo y notebooks de la Subsecretaría del Medio Ambiente, a fin de evitar que se pueda ver afectada la disponibilidad, confidencialidad o integridad de los activos de información por el ataque a las vulnerabilidades que estos puedan generar (exploits) o infecciones por malware.

Adicionalmente, mediante la "Política de Seguridad para las Operaciones" se instauran las reglas generales para garantizar las operaciones correctas y seguras de las instalaciones de procesamiento de información, definiendo las directrices para el adecuado resguardo de la plataforma tecnológica de la Subsecretaría del Medio Ambiente, así como asegurar la integridad de los sistemas operacionales. En este documento se define bajo el punto 9. Instalación del Software en Sistemas de Producción, que la subsecretaría para controlar los cambios de software en los sistemas operacionales debe considerar entre otras medidas, utilizar un aplicativo para mantener el control de todo el software implementado, así como también la documentación del sistema.

No obstante, lo anterior, la entidad auditada no ha elaborado un procedimiento para gestionar el control de los cambios efectuados en los sistemas operativos, bases de datos, cortafuegos, enrutadores, entre otros, que establezca las responsabilidades de los usuarios que permitan asegurar el control de las modificaciones ejecutadas producto de mejoramientos, parches, actualización de versiones u otras actividades que involucren intervención del software instalado y en

operación. Lo anterior implica el riesgo de que se realicen modificaciones no aprobadas o autorizadas determinando fallas o indisponibilidad de la plataforma informática y sus servicios.

La omisión expuesta no se aviene con lo estipulado en los numerales 38 y 39, de la citada resolución exenta N° 1.485, de 1996, de este origen, que establece que los directivos deben vigilar continuamente sus operaciones y adoptar inmediatamente las medidas oportunas ante cualquier evidencia de irregularidad o de actuación contraria a los principios de economía, eficiencia o eficacia, e igualmente señala que la vigilancia de las operaciones asegura que los controles internos contribuyen a la consecución de los resultados pretendidos. Esta tarea debe incluirse dentro de los métodos y procedimientos seleccionados por la dirección para controlar las operaciones y garantizar que las actividades cumplan los objetivos de la organización.

Asimismo, vulnera el referido artículo 37 letra f), del citado decreto N° 83, de 2004, en concordancia a lo estipulado en el acápite 10.1.2, de la Norma Chilena NCh-ISO N° 27.002, de 2009, en orden a que se deberían controlar los cambios en los sistemas e instalaciones de procesamiento de información.

Sobre esta situación la entidad fiscalizada manifiesta en su respuesta que actualmente existen procedimientos para gestionar registros de eventos de usuarios, administradores y operadores (Código: SSI 6.01.05.06.01.03); de desarrollo de sistemas de información seguro (Código: SSI.PR.1 40206.140208.1 40209); y de gestión de derechos de accesos privilegiados de los sistemas e infraestructura soportada por el Departamento de Tecnología de la Información, TI (Código: SSI.PR.09.02.03).

Agrega que, adicionalmente se está planificando para el año 2022, la implementación, adopción, calendarización y puesta en marcha en los sistemas que lleva el área de negocios de Información Ambiental, para llevar el control de dichas actividades por parte de TI, y en la creación de un procedimiento que incorpore el control de los cambios realizados en los sistemas de la institución, tanto en el código, bases de datos y servidores.

Considerando que el servicio señala una medida que aún no se ha concretado, corresponde mantener lo objetado, por lo que la entidad tendrá que confeccionar la documentación técnica del citado sistema, comunicando su estado de avance en el término de 60 días hábiles a contar de la recepción del presente documento.

2. Inexistencia de acuerdos de confidencialidad en los contratos.

Del análisis de las propuestas presentadas por las empresas Blue Company S.A., para la "Actualización de Sistema Ventanilla Única 2.0 y sus Sistemas Asociados", y Tic Blue Limitada, a cargo de la "Actualización del Reporte Único de Emisiones Atmosféricas (RUEA) y Actualización de Nodo Central RETC", se advirtió que los acuerdos no contemplan cláusulas de confidencialidad de los datos con el proveedor del servicio, con el consiguiente riesgo

que los empleados de las precitadas empresa tengan acceso a información confidencial y no la resguarden.

Al respecto, en lo que concierne a los aspectos de confidencialidad y resguardo de la información contenida en un sistema en línea, resulta pertinente mencionar que los organismos públicos deben adoptar las medidas técnicas y de organización necesarias para garantizar la autenticidad, confidencialidad, integridad e inviolabilidad y conservación de la información consagradas en el decreto N° 181, de 2002, del entonces Ministerio de Economía, Fomento y Reconstrucción, que aprueba el reglamento de la ley N° 19.799, sobre Documentos Electrónicos, Firma Electrónica y la Certificación de dicha Firma, como asimismo, la veracidad y resguardo de la información, contenido en la ley N° 19.628, sobre Protección de la Vida Privada, que regula el tratamiento de datos de carácter personal en registros o bancos de datos por organismos públicos o particulares (aplica el criterio contenido en el dictamen N° 36.764, de 2008, de este origen).

Asimismo, no se dio cumplimiento a lo establecido en los artículos 6°, literal a), y 8°, del decreto N° 83, de 2004, sobre la confidencialidad del documento electrónico en general.

Además, la situación advertida se contrapone con lo estipulado en los numerales 38 y 39, de la resolución exenta N° 1.485, de 1996, de este origen, que establece que los directivos deben vigilar continuamente sus operaciones y adoptar inmediatamente las medidas oportunas ante cualquier evidencia de irregularidad o de actuación contraria a los principios de economía, eficiencia o eficacia, e igualmente señala que la vigilancia de las operaciones asegura que los controles internos contribuyen a la consecución de los resultados pretendidos. Esta tarea debe incluirse dentro de los métodos y procedimientos seleccionados por la dirección para controlar las operaciones y garantizar que las actividades cumplan los objetivos de la organización.

Tampoco se aviene con lo indicado en la Norma Chilena NCh-ISO N° 27.002, de 2009, numeral 6.1.5 sobre Acuerdos de Confidencialidad, en cuanto a identificar y revisar con regularidad los requisitos para los acuerdos de confidencialidad o de no-divulgación, que reflejan las necesidades de la organización para la protección de la información.

En su respuesta, la subsecretaría fiscalizada indicó que se gestionará la incorporación de las cláusulas de confidencialidad de los datos en los contratos contraídos o en las intenciones de compra y su posterior acuerdo complementario con empresas externas. Agregó que, actualmente existe una política, por lo que en el año 2022 se trabajará en la gestión de los procedimientos.

Considerando que la repartición no aporta antecedentes que den cuenta de las medidas anunciadas, se mantiene la observación formulada.

Por lo expuesto, el servicio deberá incorporar acuerdos de confidencialidad en los contratos que elabore a futuro.

3. Falta de procedimientos para la validación de la integridad de la información recepcionada por el RETC.

A través del referido correo electrónico de 22 de marzo de 2021, la oficina de Auditoría Interna suministró la "Política de Desarrollo Seguro", Código: SSI.POL14, de noviembre 2019, que fija las normas y reglas para el correcto desarrollo de software y sistemas de información, sus servicios y arquitecturas asociadas de acuerdo a los requisitos de seguridad dispuestos por la Subsecretaría del Medio Ambiente, y que en su numeral 12, sobre Pruebas de validación de datos, establece una validación adecuada de las entradas procedentes del cliente o del entorno de la aplicación, sin embargo, de la documentación revisada se advirtió que la repartición no cuenta con procedimientos formales relacionados con el proceso de verificación de eventuales errores en la estructura de los datos obtenidos de los sistemas que integran el RETC.

Lo expuesto imposibilita diagnosticar la calidad de los datos y el eventual impacto en aquellos procesos automatizados que hacen uso de dicha información y que forman parte del RETC, en cuanto a la facilitar el acceso a la información sobre emisiones, residuos y transferencias de contaminantes.

Lo señalado transgrede el principio de control consagrado en el artículo 3°, inciso segundo, de la ley N° 18.575, y lo estipulado en los numerales 38 y 43, de la citada resolución exenta N° 1.485, de 1996, en lo referido, el primero, al deber de los directivos de vigilar continuamente las operaciones, y el segundo, a que las estructuras de control interno y las transacciones y hechos significativos, deben estar claramente documentados y disponible para su verificación.

De igual manera incumple lo estipulado en los artículos 6°, letras a) y b), y 8° del decreto N° 83, de 2004, como también, lo indicado en el acápite 12.2.1, literales a) y b), de la Norma Chilena NCh-ISO N° 27.002, de 2009, sobre comprobación y validación de datos de entrada, que dispone la revisión periódica del contenido de campos clave o archivos de datos para confirmar su validez e integridad.

Sobre la materia, la entidad corrobora que es necesario un procedimiento que abarque el punto asociado a la verificación de eventuales errores en la estructura de los datos obtenidos de los sistemas que integran el RETC, precisando que es de responsabilidad del profesional Encargado del Sistema Ventanilla Única del RETC, cargo que se mantiene vacante y por ello no existen avances en estos aspectos, lo que impacta en la operación del citado aplicativo en su conjunto, ya que no se cuenta con un responsable a nivel del negocio que levante este tipo de riesgos, que son relevantes para la información que administra el sistema.

Agrega que durante el año 2022 se avanzará en el desarrollo de un procedimiento que permita la verificación de la información que requiere el RETC, para los distintos fines establecidos en el reglamento, lo que se supedita a la capacidad y carga de trabajo de los profesionales actuales del

Departamento de Información Ambiental que podrían colaborar con esta actividad, mientras no se ocupe dicha vacante.

Dado que la repartición auditada confirma lo anotado y que las medidas señaladas no se han concretado, atañe mantener lo observado, por lo que corresponde que la entidad desarrolle y remita el procedimiento formalizado que incorpore las etapas y actividades de control que permitan la validación de la integridad de la información del aludido sistema, en el plazo de 60 días hábiles a contar de la recepción del presente informe final.

II. EXAMEN DE LA MATERIA AUDITADA

Revisión de los controles generales de la plataforma tecnológica.

4. Inexistencia de evidencia que dé cuenta de la realización de las reuniones del Comité de Seguridad de la Información.

Mediante el oficio DAE N° 112/2021, de 9 de marzo de 2021, esta Entidad de Fiscalización requirió a la Jefa de la Oficina de Auditoría Interna de la Subsecretaría del Medio Ambiente, documentación y antecedentes relacionados con la implementación de procedimientos de seguridad de la información y de sistemas. Al efecto, a través de correo electrónico de 22 de igual mes y año, esa oficina de Auditoría Interna remitió link con los datos requeridos.

De los antecedentes revisados, se comprobó que mediante la resolución exenta N° 973, de 24 de septiembre de 2015, se creó el Comité de Seguridad de los Activos de la Información de la Subsecretaría del Medio Ambiente, la cual señala que el Comité de Seguridad de la Información designará un Secretario, quien llevará un registro de actas de las reuniones periódicas del mismo, con su respectivo control de asistencia y que el Encargado de Seguridad velará por la mantención actualizada de estos registros .

También se detectó que según lo establecido en la "Política de Organización de la Seguridad", del año 2019, sancionada mediante la resolución exenta N° 1.614, de 12 de diciembre de 2019, se definió la creación del Comité de Seguridad de la Información, que tiene por objetivo aprobar las responsabilidades que se definan para aquellos roles que pudieran intervenir en riesgos de seguridad de la información y en particular para la aceptación de los riesgos residuales sobre la base de los procesos institucionales y la orientación a sistemas de información o sitios web definidos como críticos para la Subsecretaría de Medio Ambiente, además de revisar las responsabilidades sobre las bases de la política general de seguridad de la información para la protección de los activos.

Dicha política indica que dentro de las labores del referido comité se encuentran aprobar las metodologías sobre evaluación de riesgos y clasificación de la información, identificar los cambios significativos en las amenazas y la exposición de las instalaciones de procesamiento, evaluar la adecuación y coordinación de los controles de seguridad, promover en forma efectiva

la educación, formación y concientización de la seguridad a través de la organización y evaluar la información recibida de los seguimientos y revisiones de los incidentes de seguridad y las acciones recomendadas en respuesta de los mismos, entre otras materias.

No obstante lo expuesto, en la información suministrada por la entidad, no se evidenció el funcionamiento de un comité que organice y coordine las actividades para la protección de los activos de información, el cual debe estar integrado por directivos de los diferentes estamentos de la organización con funciones y roles definidos.

Por lo anterior, se solicitó a la entidad información al respecto, la que mediante el citado correo electrónico de 1 de septiembre de 2021, solo acompañó el Acta Comité de Seguridad de la Información, realizada con el 29 de octubre de 2019, y que tuvo por objetivo revisar la actualización y/o elaboración de los documentos de políticas a ese año y proceder a su aprobación y formalización, no aportando otros documentos o actas que den cuenta de la realización de reuniones periódicas, compromisos adquiridos y seguimiento de los mismos.

Ello, pese a que la mencionada "Política de Organización de la Seguridad" establece que las políticas de seguridad de la información deben revisarse cada vez que ocurra un cambio que afecte a los controles de seguridad involucrados, con la finalidad de verificar su conveniencia, suficiencia y efectividad. Agrega que, el período de reevaluación de todas las políticas de seguridad de la información será cada año, debiendo el Comité de Seguridad aprobar todos los cambios que se realicen en éstas, situación que no se evidencia de la información analizada.

La ausencia de reuniones del referido comité implica que no se coordinan ni supervisan las labores antes mencionadas, incumpliendo lo previsto en el artículo 37, letra b), sobre seguridad organizacional, del citado decreto N° 83, de 2004.

Adicionalmente, la situación planteada no se encuentra en concordancia a lo estipulado en el acápite 4, de la Norma Chilena NCh-ISO N° 27.002, de 2009, sobre Evaluación y tratamiento del riesgo, en orden a que las evaluaciones del riesgo también se deberían realizar periódicamente para tratar cambios en los requisitos de la seguridad y en la situación del riesgo, por ejemplo, en los activos, las amenazas, las vulnerabilidades, los impactos, la valoración del riesgo, y cuando ocurran cambios significativos. Estas evaluaciones del riesgo se deben emprender de una manera metódica capaz de producir resultados comparables y reproducibles.

La repartición señaló en su respuesta que debido a los hechos acontecidos en el año 2019, la pandemia del año 2020, sumado al término del PMG de Seguridad de la Información, no fue posible reunir al equipo técnico de seguridad de la información para la coordinación de la reunión del Comité de Seguridad. Esto sumado al poco personal con que ha contado durante el año 2021 el Departamento de TI.

Complementa indicando que para el año 2022 calendarizaría con las nuevas autoridades las respectivas reuniones.

Debido a que la repartición auditada confirmó lo anotado y a que las acciones enunciadas no se han concretado, corresponde mantener lo objetado.

Por lo anteriormente expuesto, la Subsecretaría del Medio Ambiente deberá remitir el documento que contiene la calendarización de las respectivas reuniones, debidamente formalizado en el plazo de 60 días hábiles a contar de la recepción del presente informe final.

5. Inexistencia de procedimientos que garanticen la continuidad operacional.

A través del citado correo electrónico de 22 de marzo de 2021, la Oficina de Auditoría Interna suministró el documento titulado "Procedimiento de Gestión de Eventos e Incidentes de Seguridad de la Información" mediante el cual se describen los pasos necesarios para atender de forma rápida y eficaz los eventos e incidentes de seguridad que afecten o puedan afectar la integridad, confidencialidad y disponibilidad de la información crítica de la Subsecretaría del Ministerio del Medio Ambiente, incluyendo el contacto con las autoridades pertinentes, a fin de controlar la situación, evitar propagación de los daños y tomar acciones para evitar su recurrencia.

Del análisis de la información remitida por el servicio, se advierte que dicho procedimiento no establece mecanismos tendientes a contrarrestar interrupciones a las actividades del negocio y proteger los procesos críticos del negocio de la entidad, contra los efectos de fallas importantes en los sistemas de información o contra desastres, y asegurar su restauración oportuna, generando un eventual riesgo de indisponibilidad de los servicios provistos por la infraestructura de la Subsecretaría del Medio Ambiente.

Por lo expuesto se solicitó al servicio información al respecto, la que fue remitida vía el aludido correo electrónico de 1 de septiembre de 2021, donde acompañó nuevamente el procedimiento de gestión de eventos.

La omisión de aspectos que garanticen la continuidad operacional de la entidad vulnera lo establecido en los artículos 35, en orden a que el encargado de seguridad deberá formular un plan de contingencia para asegurar la continuidad de operaciones críticas para la entidad, y 37, letra i), sobre la gestión de la continuidad del negocio, ambos del decreto N° 83, de 2004.

En este sentido, la Norma Chilena NCh-ISO N° 27.002, de 2009, señala que se deberían identificar los eventos que pueden ocasionar interrupciones en los procesos del negocio junto con la probabilidad y el impacto de dichas interrupciones, así como sus consecuencias para la seguridad de la información.

La entidad manifestó en su respuesta que actualmente cuenta con los procedimientos para gestionar registros de eventos de usuarios, administradores y operadores (Código: SSI 6.01.05.06.01.03); de desarrollo de sistemas de información seguro (Código: SSI.PR.1 40206.140208.1 40209); y de gestión de derechos de accesos privilegiados de los sistemas e infraestructura soportada por el departamento de TI (Código: SSI.PR.09.02.03). Asimismo, señaló que está trabajando en planificar para el año 2022 la implementación, adopción, calendarización y puesta en marcha en los sistemas que lleva el área de negocios de Información Ambiental, para llevar el control de dichas actividades por parte de TI.

Manifestó, además, que la planificación del año 2022 incluirá la mejora de los procedimientos actuales y el control en el monitoreo, especialmente en el de respaldo y restauración de información (Código: SSI.PR.12.03.01).

Considerando que la medida anunciada no se ha concretado se mantiene lo objetado preliminarmente, por lo cual, corresponde que la repartición remita la mejora de los procedimientos actuales y el control en el monitoreo, especialmente en lo referido al respaldo y restauración de información, en el término de 60 días hábiles, a contar desde la recepción del presente documento.

6. Ausencia de monitoreo de la actividad de la red.

Mediante el antes dicho correo electrónico de 22 de marzo de 2021, la oficina de Auditoría Interna indicó, sobre el seguimiento de los casos de incidentes de seguridad informados y las medidas tomadas por el servicio, que no existe información a reportar, por cuanto no se registraron incidentes en el período indicado, sin embargo, no se acompañó información y reportes que comprueben el monitoreo de la actividad de red, detección de intrusos e intentos de accesos no permitidos a la plataforma institucional.

En relación a lo anterior, en el antecedente presentado por la entidad, denominado "Procedimiento de Gestión de Eventos e Incidentes de Seguridad de la Información", Código:SSI. PR.160105.060103, versión de octubre 2019, remitido en la misma fecha, se señala que se debe conformar el "Reporte trimestral de la gestión de eventos e incidentes de seguridad de la información" y el "Reporte de incidentes de seguridad de la información", datos que no se tuvieron a la vista.

La situación expuesta no permite advertir las debilidades de seguridad de la información y detectar incidentes de seguridad de la misma y que puedan causar daños en la infraestructura tecnológica de la institución.

Lo anterior vulnera los principios de eficiencia y eficacia, que rigen a los órganos de la Administración del Estado, en cuanto a que las autoridades y funcionarios deben velar por la idónea administración de los medios públicos y el debido cumplimiento de la función pública y ejercer el control jerárquico permanente dentro del ámbito de su competencia y en los niveles que corresponda, respecto del funcionamiento de los organismos y de la actuación del personal de su dependencia, control que comprende tanto la eficiencia y la eficacia en el

cumplimiento de los fines y objetivos establecidos, como a la legalidad y oportunidad de las actuaciones, según lo previsto en los artículos 3°, 5° y 11 de la referida ley N° 18.575.

Asimismo, incumple lo estipulado en la letra c), del artículo 33, del decreto N° 83, de 2004, que manifiesta que las instituciones regidas por la presente norma impartirán instrucciones relativas al uso de redes y servicios en red que, al menos, especifiquen los controles de gestión y procedimientos para proteger el accesó a las conexiones de la red y servicios de red.

De la misma forma, lo indicado en el acápite 13.2, de la Norma Chilena NCh-ISO N° 27.002, de 2009, sobre Gestión de incidentes y mejoras de seguridad de la información que señala que además de informar los eventos y las debilidades de seguridad de la información, se debería utilizar el monitoreo de sistemas, alertas y vulnerabilidades para detectar incidentes de seguridad de la información.

La repartición informó en su respuesta, que actualmente se cuenta con el citado sistemas de monitoreo de actividad de la red, apoyada en diferentes herramientas tales como la solución PRTG[37] que se utiliza para el monitoreo de la infraestructura general del Ministerio de Medio Ambiente; Herramienta Antispam Barracuda a través de la cual se controla y chequea tanto el correo de entrada como de salida; y Firewall Palo Alto, herramienta de seguridad NGF que nos permite monitorear el tráfico perimetral del ministerio donde se establecen reglas de ingreso y de salida de tráfico.

Complementa indicando que, sin perjuicio de lo señalado, durante el año 2022 se calendarizarán las fechas de recopilación de los reportes, evidencias y registros, que tendrán una periodicidad mensual y un acumulativo trimestral, por lo que se evaluará contemplarlo en un Compromiso de Desempeño Colectivo.

Dado que las medidas enunciadas por la entidad aún no se han concretado, corresponde mantener lo observado preliminarmente.

Por lo expuesto, la repartición deberá remitir el documento sancionado que contenga la calendarización de las fechas de recopilación de los reportes, evidencias y registros periódicos, contemplado en el Compromiso de Desempeño Colectivo, en el plazo de 60 días hábiles contado desde la recepción del presente informe final.

37 Software de monitorización proactiva de red, que monitoriza continuamente dispositivos, sistemas y aplicaciones de tu infraestructura TI, proporcionando informes de estado y permitiendo generar alertas cuando se produce un error o los umbrales críticos se sobrepasan.

7. Falta de un procedimiento de configuración de los sistemas.

El referido "Procedimiento de Control de Instalación de Softwares", de 2019, describe las actividades para controlar la instalación de software en estaciones de trabajo y notebooks de la SMA, a fin de evitar que se pueda ver afectada la disponibilidad, confidencialidad o integridad de los activos de información por el ataque a las vulnerabilidades que estos puedan generar o infecciones por malware.

No obstante, en el mencionado documento solo se establecen procedimientos de configuración para equipamiento menor y equipos de usuarios finales, no considerando en sus definiciones, los parámetros que dicha configuración debe tener para asegurar el correcto funcionamiento de los aplicativos y equipos que los mantienen.

Por otra parte, en la referida "Política de Seguridad para las Operaciones" se disponen las reglas generales para garantizar las operaciones correctas y seguras de las instalaciones de procesamiento de información, definiendo las directrices para el adecuado resguardo de la información soportada en la plataforma tecnológica de la Subsecretaría del Medio Ambiente, así como asegurar la integridad de los sistemas operacionales. Dentro de las definiciones, considera indicaciones para los entornos de desarrollo separados de producción, los tipos y la vigencia de los respaldos, la protección de los activos de información físicos, la condición de los mismos y a la restauración, el registro de eventos, los registros del administrador y el operador, la sincronización de relojes y la instalación del software en producción.

Ahora bien, revisada dicha documentación se advirtió que no se consideran los procedimientos para aplicar la configuración y modificación de los parámetros de los sistemas operativos, bases de datos, cortafuegos, enrutadores, entre otros y que establezcan las responsabilidades y procedimientos formales que le permitan asegurar su correcto funcionamiento y puesta a punto para el RETC, con el consiguiente riesgo de que se realicen modificaciones no aprobadas o autorizadas determinando fallas o indisponibilidad de la plataforma informática y sus servicios.

Lo señalado vulnera el artículo 37 letra f), del citado decreto N° 83, de 2004, en concordancia a lo estipulado en el acápite 10.1.2, de la Norma Chilena NCh-ISO N° 27.002, de 2009, en orden a que se deberían controlar los cambios en los sistemas e instalaciones de procesamiento de información.

La institución fiscalizada señaló en su respuesta que, el Departamento de TI está trabajando en la planificación del año 2022, incluyendo en ella la mejora del proceso de Control de Instalación de Softwares para toda la organización, como también, en la elaboración de los que emanan de la Política de Seguridad para las Operaciones, en los cuales se abordarán las actividades para aplicar la configuración y modificación de parámetros de los aplicativos y equipos.

Agrega que, el área de negocios de Información Ambiental trabajará en la recopilación de información relativa a manuales o procedimientos internos de sus sistemas sectoriales, para su adaptación a los estándares de TI, posterior registro y monitoreo.

Considerando que la elaboración y formalización del precitado documento no se ha materializado, se mantiene lo objetado, por lo que la entidad deberá complementar su Política de Seguridad para las Operaciones, de manera de incorporar las omisiones advertidas por esta Entidad de Control, suministrando un informe de avance en el plazo de 60 días hábiles contado desde la recepción del presente documento.

8. Inexistencia de procedimientos para la autorización, registro, modificación, revocación y revisión periódica de los permisos de acceso de los usuarios.

A través de referido correo electrónico de 22 de marzo de 2021, la oficina de Auditoría Interna remitió el documento titulado "Procedimiento de Gestión de Derechos de Acceso Privilegiados", Código:SSI.PR.09.02.03, versión de octubre de 2019, mediante el cual se describen las solicitudes y asignaciones de los accesos privilegiados a los activos de información institucionales, así como también la gestión de requisitos para el vencimiento de accesos otorgados que comprometan la integridad, disponibilidad y confidencialidad de la información que almacenan.

Adicionalmente, en la misma fecha fue remitido el "Procedimiento de Verificación de Inicio de Sesión Seguro", Código:SSI.PR.09.04.02, Versión: agosto 2019, por el que se establecen los pasos a seguir para implementar y verificar los inicios de sesión seguro en los accesos de los usuarios a los sistemas de información, evitando ingresos no autorizados y mantener la confidencialidad, integridad y disponibilidad de los activos de información de la Subsecretaría del Medio Ambiente, no obstante, la documentación señalada tiene por objetivo verificar que los nuevos programas que se desarrollen internamente o que sean adquiridos, cumplan y se encuentren configurados con los criterios o reglas de complejidad sobre la creación de las contraseñas y tiempos de sesión de conexión a los mismos.

Al respecto, cabe manifestar que de la información proporcionada por la entidad, no fue posible constatar que estén definidos los roles, tipos de usuarios, y los accesos que tendrán cada uno de ellos a los diferentes aplicativos, a qué tipo de información y cuál será el privilegio de ingreso que un rol tendrá definido, lo que advierte que la repartición fiscalizada no ha desarrollado procedimientos para autorizar, registrar, modificar, y revisar periódicamente los permisos de acceso de los usuarios, así como para revocarlos inmediatamente cuando un empleado cambie de función o sea desvinculado de la institución.

Lo anterior podría ocasionar el ingreso de terceros no autorizados, de personas desvinculadas de la institución o que ya no debe utilizar un determinado sistema por cambio de función, con el riesgo de que dañen, eliminen o divulguen la data existente en los aplicativos y, por ende, afecte el análisis y difusión de la información sobre emisiones, residuos y transferencias de

contaminantes potencialmente dañinos para la salud y el medio ambiente que son emitidos al entorno.

La omisión mencionada transgrede lo expresado en el artículo 37, literal g) del mencionado decreto N° 83, de 2004, sobre control de acceso, en concordancia con los acápites 11.2.1, letra g), en cuanto a que el procedimiento de control de acceso para el registro y cancelación de registro del usuario debería incluir el borrado inmediato o bloqueo de los derechos a los usuarios que hayan cambiado roles o tareas o dejado la organización; y 11.2.4, literales a) y b), en orden a que los derechos de acceso de usuarios deberían ser revisados a intervalos regulares, por ejemplo, cada seis meses, y luego de cualquier cambio, tal como una promoción, una degradación, o terminación del empleo, y sujetos a revisión y reasignados, cuando se mueve de un empleo a otro dentro de la misma organización, ambos de la Norma Chilena antes referida.

La repartición fiscalizada indica en su respuesta, que el Departamento de TI desarrollará un protocolo institucional a fin de que cada unidad de negocio que administre un sistema cumpla con los estándares institucionales, para su posterior control, registro y monitoreo.

Agrega que se está trabajando con el Departamento de Personas en un procedimiento de alta, baja o perfil de usuarios.

Dado que las acciones de mejoras detalladas por la subsecretaría no se han concretado, corresponde mantener lo objetado.

Por lo anteriormente expuesto, corresponde que el aludido Departamento de TI desarrolle un protocolo institucional que administre el alta, baja y los perfiles de usuario y elabore un procedimiento formal de revisión de derechos de acceso, remitiendo la documentación que acredite el estado de avance de lo dispuesto, en el plazo de 60 días hábiles contado desde la recepción del presente documento.

9. Inexistencia de un procedimiento sobre el cambio de contraseña después del primer inicio de sesión.

Mediante el aludido correo electrónico de 22 de marzo de 2021, la repartición fiscalizada suministró el documento titulado "Procedimiento de Verificación de Inicio de Sesión Seguro", Código: SSI.PR.09.04.02, Versión: agosto 2019, donde se indican los criterios para contraseñas seguras de cada aplicativo que integra el RETC. Además, se establecen los pasos a seguir para implementar y verificar los inicios de sesión seguro en los accesos de los usuarios a los sistemas de información, evitando ingresos no autorizados y mantener la confidencialidad, integridad y disponibilidad de los activos de información de la Subsecretaría del Medio Ambiente, por cuanto no se detectaron observaciones de la materia analizada.

En el mencionado documento se fija que el profesional asignado de la sección Sistemas del Departamento de Tecnologías de la Información elabora el registro de revisión de inicio de sesión seguro para aplicativos, luego de haber realizado las pruebas de calidad, el cual tiene por objetivo verificar que los nuevos programas que se desarrollen internamente o que son adquiridos, cumplan y se encuentren configurados con los siguientes criterios o reglas de complejidad:

a) No mostrar la contraseña que está siendo ingresada escondiendo caracteres de la contraseña con símbolos.

b) Asignar un tiempo forzoso de espera de a lo menos 3 minutos de espera luego de 3 intentos fallidos de inicio de sesión, antes de permitir un nuevo intento de inicio de sesión.

c) Configurar que al momento de renovar la contraseña tenga que registrar una diferente a las últimas tres registradas.

d) Configurar que el largo de la contraseña no sea inferior a 8 caracteres alfanuméricos.

e) Configurar que la contraseña contenga a lo menos un numero entre (0 y 9) y un carácter especial como por ejemplo: "¡"#$%&/0=?¡'+-/".

No obstante lo anterior, no se ha definido entre las reglas de complejidad la asignación de una clave inicial y la obligación de modificarla por parte del usuario tras el primer inicio de sesión, lo cual fue comprobado por esta Entidad de Control mediante un acceso efectuado al aplicativo el 14 abril de 2021, con las credenciales suministradas por la repartición vía correo electrónico del día anterior, donde el encargado de la Sección de Sistemas de la entidad, habilitó el acceso en modo consulta, a la Ventanilla Única 2.0.

Tales accesos fueron habilitados a través de la generación de credenciales que cumplen con los criterios definidos en el procedimiento de verificación de inicio de sesión seguro, pero que no requiere de manera obligatoria el cambio de contraseña tras iniciar una sesión por primera vez utilizando la clave asignada, lo que puede facilitar el acceso no autorizado de terceros a los sistemas institucionales, y el coincidente riesgo de pérdida, daño o hurto de la información de los mismos.

Lo antes mencionado transgrede lo expresado en el artículo 28, literal j) del decreto N° 83, de 2004, sobre la asignación de los identificadores, que establece la indicación de cambiar el identificador temporal al iniciar la primera sesión.

Además, los acápites 11.2.3, letra b), de la Norma Chilena NCh-ISO N° 27.002, de 2009, sobre gestión de contraseñas de usuarios, señala que se debe exigir a los usuarios mantener sus propias contraseñas, agregando que deben ser provistos inicialmente con una contraseña segura temporal, para que estén forzados a cambiarla inmediatamente.

La repartición manifiesta en su respuesta que, durante el ejercicio de actualización del año 2022, revisará el procedimiento de verificación de inicio de sesión seguro (Código: SSI.PR.09.04.02) de modo de optimizar los criterios o reglas de complejidad, entre otros posibles cambios, y la incorporación en los actuales desarrollos de la institución, incluyendo los de Ventanilla Única, como en los futuros desarrollos tanto interno como externos.

Debido a que las acciones manifestadas por la entidad auditada aún no se han materializado, corresponde mantener lo objetado preliminarmente.

La repartición fiscalizada deberá revisar el procedimiento de verificación de inicio de sesión seguro mencionado, de modo de optimizar los criterios y reglas de complejidad y la incorporación de estos en los actuales desarrollos de la institución, incluyendo tanto los de Ventanilla Única como los futuros desarrollos interno y externos, remitiendo la documentación en el término de 60 días hábiles a contar de la recepción del presente informe final.

10. Ausencia de políticas de uso, almacenamiento, acceso y distribución de mensajes electrónicos.

La mencionada "Política de Seguridad de las Operaciones" dispone las reglas generales para garantizar las operaciones correctas y seguras de las instalaciones de procesamiento de información, definiendo las directrices para el adecuado resguardo de la información soportada en la plataforma tecnológica de la Subsecretaría del Medio Ambiente.

Dicho documento señala en su punto 3, relativo a la vigencia de los respaldos, que esa subsecretaría deberá realizar respaldos de información de los correos institucionales por un período de 5 años, de acuerdo a la resolución exenta N° 931, de 29 de octubre de 2013; que fija Estructura Organizacional y Funcional del Archivo del Ministerio del Medio Ambiente, fijando Procedimientos de Expurgo y Transferencia de Documentos, aunque aquello estará sujeto a la cantidad de espacio de almacenamiento disponible de la institución, no obstante lo anterior, no especifica las características técnicas que deben tener los respaldos mencionados.

Por otra parte, la precitada resolución exenta N° 1.614, de 2019, indica que, dentro de las responsabilidades del Encargado de Seguridad de la Información está "Proponer los procedimientos de manipulación requeridos para cubrir las siguientes actividades de procesamiento de un documento electrónico: copiado, almacenamiento, transmisión por correo electrónico, además de sistemas protocolizados de datos digitales y destrucción de los mismos".

Adicionalmente, fue remitido el documento titulado "Procedimiento de Respaldo y Restauración de Información", Código SSI PR 12.03.01, de octubre 2019, mediante el cual se establecen los pasos a seguir para respaldar y restaurar la información soportada en los servidores que contienen los tipos de activos de información asociados a este de los procesos de provisión de productos estratégicos de la Subsecretaría del Medio Ambiente.

A su turno, en el indicado "Procedimiento de Verificación de Inicio de Sesión Seguro" se fijan los pasos a seguir para implementar y validar los accesos de los usuarios a los sistemas de información, evitando accesos no autorizados y mantener la confidencialidad, integridad y disponibilidad de los activos de información de la subsecretaría, no obstante, tal documentación no establece la forma de acceso a los mensajes electrónicos, y que estos cumplan y se encuentren configurados con los criterios o reglas de complejidad sobre la creación de las contraseñas y tiempos de sesión de conexión.

De acuerdo con lo señalado, de la información proporcionada por la repartición, no fue posible determinar que la entidad fiscalizada haya desarrollado procedimientos para autorizar, registrar, modificar, y revisar periódicamente las políticas de uso, almacenamiento, acceso y distribución de mensajes electrónicos de la institución, debido a que dentro de la documentación remitida no se encontraban dichos elementos.

Complementario a lo anterior, mediante el aludido correo electrónico de 1 de septiembre de 2021, la repartición corroboró que no existen procedimientos destinados a regular el manejo y distribución de los documentos electrónicos.

Lo expuesto podría generar que accedan a información personas no autorizadas, como también, problemas de disponibilidad de servicios, entre otros.

Tal omisión transgrede lo expresado en el artículo 7, literal a) del decreto N° 83, de 2004, sobre seguridad del documento electrónico, que dispone los atributos esenciales que aportan seguridad al documento electrónico se obtienen y sostienen mediante la ejecución permanente de, entre otras acciones, desarrollar y documentar políticas de seguridad de uso, almacenamiento, acceso y distribución del documento electrónico y de los sistemas informáticos utilizados en su procesamiento.

De igual manera, la situación planteada no se encuentra en concordancia con los literales a), y b) y c), del acápite 10.8.4,sobre mensajería electrónica que señala que la información contenida en la mensajería electrónica debería ser apropiadamente protegida mediante consideraciones de seguridad que deberían incluir; asegurar el correcto direccionamiento y transporte de los mensajes; confiabilidad y disponibilidad general del servicio; proteger mensajes del acceso no autorizado, modificación o negación de servicio entre otras, de la Norma Chilena antes referida.

La Subsecretaría del Medio Ambiente manifestó en su respuesta que, actualmente basan sus políticas de uso de correo en la plataforma Office 365, agrega en ese sentido, que se está trabajando en planificar en el año 2022 la declaración de la política de correos de la Institución.

En consideración a que la acción informada no se ha materializado, se mantiene la observación formulada, y corresponde que la entidad elabore un procedimiento formal de la política de correos de la Institución y lo remita en el mismo plazo de 60 días hábiles contado desde la recepción del presente documento.

11. Falta de registro de ejecución y recuperación de respaldos.

Como se indicó, mediante el referido correo electrónico de 22 de marzo de 2021, la oficina de Auditoría Interna remitió el documento titulado "Procedimiento de Respaldo y Restauración de Información", Código: SSI.PR.12.03.01; versión de octubre 2019.

Posteriormente, a través del aludido correo electrónico de 1 de septiembre de 2021, el Jefe(S) de la oficina de Auditoría Interna suministró el archivo denominado "calendario de respaldo y verificación de restauración", en el cual no se encuentra el Sistema Ventanilla Única del RETC y el RUEA.

Si bien la repartición cuenta con procedimientos asociados, no fue posible acreditar la existencia de respaldos de la información relacionada de los aludidos sistemas, ni de una bitácora que demuestre la frecuencia y datos que son respaldados.

Ello conlleva el riesgo de perder información en caso de ocurrencia de algún siniestro en el aplicativo, y con ello, la imposibilidad de realizar un análisis de la misma por parte de la SMA, afectando la difusión de información sobre emisiones, residuos y transferencias de contaminantes potencialmente dañinos para la salud y el medio ambiente que son emitidos al entorno.

La situación expuesta transgrede lo expresado en el artículo 24, del decreto N° 83, de 2004, que indica que deberán realizarse copias de respaldo de la información y las aplicaciones críticas para la misión de la institución en forma periódica.

Asimismo, no se encuentra en concordancia con lo indicado en el acápite 10.5, de la Norma Chilena NCh-ISO N° 27.002, de 2009, sobre Respaldo, indica que se deberían establecer procedimientos de rutina para implementar una política y estrategia acordada de respaldo haciendo copias de respaldo de datos y ensayando sus tiempos de restauración.

La subsecretaría fiscalizada manifestó en su respuesta que cuenta con un sistema de respaldo de los servidores AVAMAR, no obstante ello, señala que queda pendiente el ejercicio de restauración en conjunto con el área de negocio para su verificación. Agrega que se calendarizarán para el año 2022 los trabajos de respaldo, verificación y restauración del aplicativo de RETC, además de dejar el registro correspondiente, tal como lo establece el procedimiento de respaldo de información.

Considerando que conforme lo expuesto por la subsecretaría, los trabajos de respaldo, verificación y restauración del sistema de RETC no se han realizado, se mantiene el hecho objetado, por lo tanto, la repartición deberá confeccionar un ejercicio de restauración para la verificación de los respaldos de los servidores AVAMAR, así como informar la calendarización de los mismos para el año 2022, y remitir los resultados en el término de 60 días hábiles a contar de la recepción del presente informe final.

12. Falta de registros de pruebas de respaldo y recuperación de la información.

En el mencionado Procedimiento de respaldo y restauración de información se definen los pasos a seguir para respaldar y restaurar la información soportada en los servidores que contienen los tipos de activos de información asociados a este, de los procesos de provisión de productos estratégicos de la Subsecretaría del Medio Ambiente, de acuerdo a lo señalado en las reglas de la Política de Seguridad para las Operaciones, a fin de resguardar la información que sustenta el trabajo administrativo u operacional de la institución.

Dicho documento estipula en su numeral 2, sobre Restauración de la Información, que para el caso de los respaldos de servidores que contengan aplicativos, bases de datos u otros relacionados a la Sección de Sistemas, su encargado debe coordinar con la Sección de Operaciones, ambos del Departamento TI, de manera de poner a disposición el respaldo correspondiente para pruebas de consistencia indicado en el calendario inicial.

Posteriormente, la Sección de Sistemas debe acceder al servidor de prueba, con la recuperación del respaldo existente. El funcionario asignado o el Encargado de la Sección mencionada realiza las pruebas de consistencia necesarias para corroborar la información restaurada.

No obstante, es dable reiterar que en el mencionado "calendario de respaldo y verificación de restauración", no se encuentran registros de los sistemas Ventanilla Única del RETC y RUEA, con lo que se genera el mismo riesgo de la observación anterior.

La situación expuesta transgrede lo indicado en el artículo 24, letra c), del decreto N° 83, antes mencionado, que indica que deberá garantizarse la disponibilidad de infraestructura adecuada de respaldo, para asegurar que éstos estén disponibles incluso después de un desastre o la falla de un dispositivo. Las configuraciones de respaldo para los sistemas individuales deberán ser probadas con regularidad, a lo menos cada 2 años, para asegurar que ellas satisfacen los requisitos estipulados en los planes de continuidad institucionales;

Lo anterior tampoco se aviene con lo señalado en el acápite 10.5.1, sobre respaldo de la información, de la citada Norma Chilena, que establece que se deberían hacer regularmente copias de seguridad de la información y del software y probarse regularmente acorde con la política de respaldo, con el fin de asegurar su eficacia y que pueden ser utilizados dentro del tiempo asignado en los procedimientos operacionales para la recuperación.

La institución auditada señala en su respuesta que cuenta con un sistema de respaldo de los servidores, sin embargo, está *pendiente el ejercicio de restauración en conjunto con el área de negocio para su verificación.*

Adicionalmente, manifiesta que se analizará y optimizará la infraestructura tecnológica asociada a los sistemas de Ventanilla Única del RETC, de manera tal que permita mitigar riesgos de pérdida de información.

Por lo anterior y habida consideración que la medida indicada no se ha concretado, procede mantener lo advertido.

La repartición fiscalizada deberá confeccionar un ejercicio de restauración para la verificación de los respaldos de los servidores AVAMAR, así como la calendarización para el año 2022 de los trabajos de respaldo, verificación y restauración del sistema de RETC y remitir los resultados en el término *de 60 días hábiles a contar de la recepción del presente informe final.*

13. Falta de implementación de un sitio externo de almacenamiento que cumpla al menos con las mismas características de seguridad que el sitio principal.

Se advirtió que el procedimiento de respaldo y restauración de información no considera los pasos a seguir para la protección de la *información soportada en los servidores al interior del servicio, lo que genera el riesgo* de que, en el caso de algún siniestro en las instalaciones, los aludidos respaldo se dañen y por lo tanto, perder toda la información de los sistemas institucionales.

La situación señalada, fue corroborada, mediante correo electrónico de 1 de septiembre de 2021, del Jefe(S) de la oficina de Auditoría Interna.

La omisión expuesta transgrede lo expresado en el inciso e) del artículo 24, del decreto N° 83, de 2004, que estipula que los respaldos deberán cumplir con un nivel apropiado de protección física de los medios, consistente con las prácticas aplicadas en el sitio principal. Los controles asociados a los dispositivos del sitio de producción deberán extenderse para abarcar el sitio de respaldo.

Por otra parte, lo indicado en el acápite 10.5.1, letra e), de la Norma Chilena NCh-ISO N° 27.002, de 2009, sobre Respaldo, que confirma lo indicado en la normativa señalada en el párrafo anterior.

En su contestación, la repartición indicó que se está trabajando en la búsqueda de soluciones en Cloud, para dar respuesta a los sistemas críticos priorizados por ella. Agrega que se analizará la factibilidad y se gestionarán los recursos para la disposición de un sitio de respaldo secundario que permita mantener la continuidad de operaciones cuando el primario no esté disponible.

Considerando que las medidas comunicadas no se han concretado, se mantiene lo advertido, por lo que la entidad deberá desarrollar una solución para dar respuesta a los sistemas críticos priorizados por la misma, así como el análisis de factibilidad y recursos para la disposición de un sitio secundario, informando sobre el estado de avance de ello, remitiendo dicho antecedente en el plazo de 60 días hábiles contado desde la recepción del presente documento.

Deficiencias en la seguridad física del Centro de Procesamiento de Datos.

En el marco de la auditoría, el 21 de julio de 2021 se efectuó una revisión a la sala de servidores del Ministerio de Medio Ambiente, ubicada en calle San Martín N° 73, Santiago, advirtiéndose las situaciones que se detallan a continuación:

14. Falta del protocolo de ingreso a las salas de servidores.

Mediante el referido correo electrónico de 22 de marzo de 2021, la oficina de Auditoría Interna remitió el documento titulado "Procedimiento para gestionar registros de eventos de usuarios, administradores y operadores", que tiene por objetivo describir los pasos necesarios para generar, mantener y revisar de forma regular los registros de las actividades de los usuarios, administradores y operadores de los activos de información críticos de la Subsecretaría del Medio Ambiente, a fin de detectar posibles eventos o incidentes de seguridad de la información relacionados con intentos de acceso no autorizados, uso no apropiado de recursos, fallas, cambios no autorizados, entre otros, que puedan poner en riesgo la integridad, confidencialidad y disponibilidad de los activos de información.

Del análisis realizado al procedimiento de esa entidad, se pudo establecer que, dentro de las actividades definidas no se cuenta con un protocolo formalizado para autorizar y registrar los ingresos y salidas del personal externo de las salas de servidores del Departamento de Tecnologías de la Información y Comunicaciones.

Posteriormente, a través de la aludida visita al Datacenter del Ministerio de Medio Ambiente, se confirmó mediante entrevista con el encargado José Yáñez Torres, que no se ha creado y formalizado un procedimiento oficial para acceder al Centro de Procesamiento de Datos, con el consiguiente riesgo de no contar con protocolo de acceso a la sala de servidores, con lo que podría acceder personal no autorizado y daño intencional o involuntario de las dependencias y la información.

Esta situación constituye una vulneración de la letra e), del artículo 37, del decreto N° 83, de 2004, sobre seguridad física y del ambiente.

A su vez, la Norma Chilena NCh-ISO N° 27.002, de 2009, indica en este sentido que las instalaciones de procesamiento de información crítica o sensible de la organización deberían estar ubicadas en áreas

seguras y resguardadas por un perímetro de seguridad definido, con barreras de seguridad y controles de acceso apropiados, agregando que para conseguir lo anterior, deberían estar físicamente protegidas contra accesos no autorizados, daños e interferencias.

La repartición manifestó en su respuesta que durante el primer semestre del año 2022, se trabajará en la elaboración de los registros y bitácoras de acceso a los espacios restringidos, para su continuo monitoreo.

Considerando que lo manifestado por la repartición auditada da cuenta de medidas que no se han concretado, corresponde mantener lo observado, por lo que la entidad auditada deberá implementar un registro formal para la gestión de acceso, y bitácoras de ingreso a los espacios restringidos, para su continuo monitoreo, informando documentadamente en el plazo de 60 días hábiles contado desde la recepción del presente documento.

15. Ausencia de registros de ingreso al datacenter.

La repartición no cuenta con un registro del personal que ingresa a las instalaciones, lo cual es información útil para llevar a cabo un seguimiento de las actividades ejecutadas al interior de la aludida sala y esclarecer responsabilidades administrativas ante eventuales amenazas y/o hechos consumados.

En relación con lo expuesto, la repartición fiscalizada manifestó, a través del correo electrónico de 1 de septiembre de 2021, del Jefe(S) de la oficina de Auditoría Interna, que cada persona externa que entra al edificio es registrada por los recepcionistas en planilla Excel con nombre y RUT, y por otra, los funcionarios registran su acceso a la repartición en reloj control. Agregó que, actualmente, a causa de la pandemia por COVID-19, el acceso es registrado en formato papel con información de síntomas y toma de temperatura tanto a personas externas a la institución como a funcionarios.

Sobre lo señalado, es dable indicar que el registro de inducción de control de síntomas y temperatura para la prevención del contagio del COVID-19, que se encuentra dentro del Plan de acción para el coronavirus, registra solamente temperatura y síntomas, sin almacenar el RUT o labores a realizar como se indicó previamente. Ver detalle del registro en Imagen N° 1.

Imagen N° 1: Registro de acceso a las dependencias de la Subsecretaría de Medio Ambiente.

CHILE LO HACEMOS TODOS	REGISTRO INDUCCIÓN CONTROL DE SÍNTOMAS Y TEMPERATURA PREVENCIÓN CONTAGIO COVID-19	PLAN DE ACCIÓN CORONAVIRUS COVID-19
	Subsecretaría del Medio Ambiente	Versión 01
		Fecha 06/2020

NOMBRE EVALUADOR: Patricia Solar
FECHA: 21/07/2021

N°	NOMBRE	RUT	T°	Ha tenido contacto con caso positivo o viaje al extranjero en los últimos 14 días		SINTOMAS											
						Tos		Dificultad Respiratoria		Dolor de Garganta		Perdida de olfato o gusto		Dolor Muscular		Nauseas / Vomito	
				SI	NO	✓	X	✓	X	✓	X	✓	X	✓	X	✓	X
	Renata Roman		36,1	SI	NO		X		X		X		X		X		X
	Tatiana Garcia		36,2	SI	NO		X		X		X		X		X		X
	Jose Yañez		36,3	SI	NO		X		X		X		X		X		X
	Melin Yan		32	SI	NO		X		X		X		X		X		X
	Loreto Cobarrubias		36,4	SI	NO		X		X		X		X		X		X
	Felipe Valencia		35,7	SI	NO		X		X		X		X		X		X
	Javier Vargas		31,4	SI	NO		X		X		X		X		X		X
	Marcelo Fernandez		36,2	SI	NO		X		X		X		X		X		X
	Hector Miranda		32,2		X		X		X		X		X		X		X
	Javier Naranjo		35,7		X		X		X		X		X		X		X
	Angel Retamal		36,3		X		X		✓		✓		X		X		X

Fuente: información suministrada mediante correo electrónico de 1 de septiembre de 2021, de del Jefe(S) de la oficina de Auditoria Interna.

En cuanto al hecho de que los funcionarios registren su entrada al servicio mediante reloj control, ello no permite llevar el registro de la labor que realizaron en el datacenter, del período en el que permanecieron al interior del mismo.

La omisión expuesta transgrede lo estipulado en el artículo 19, letra a), del decreto N° 83, de 2004, en lo que interesa, sobre que los documentos electrónicos deberán almacenarse en áreas seguras, protegidos por un perímetro de seguridad definido, con barreras apropiadas de resguardo y controles de entrada. Estos tendrán que estar físicamente protegidos del acceso no autorizado, daño e interferencia.

El servicio fiscalizado señaló en su respuesta que a partir del primer semestre del año 2022, se trabajará en la elaboración de los registros y bitácoras de acceso a los espacios restringidos, para su monitoreo continuo.

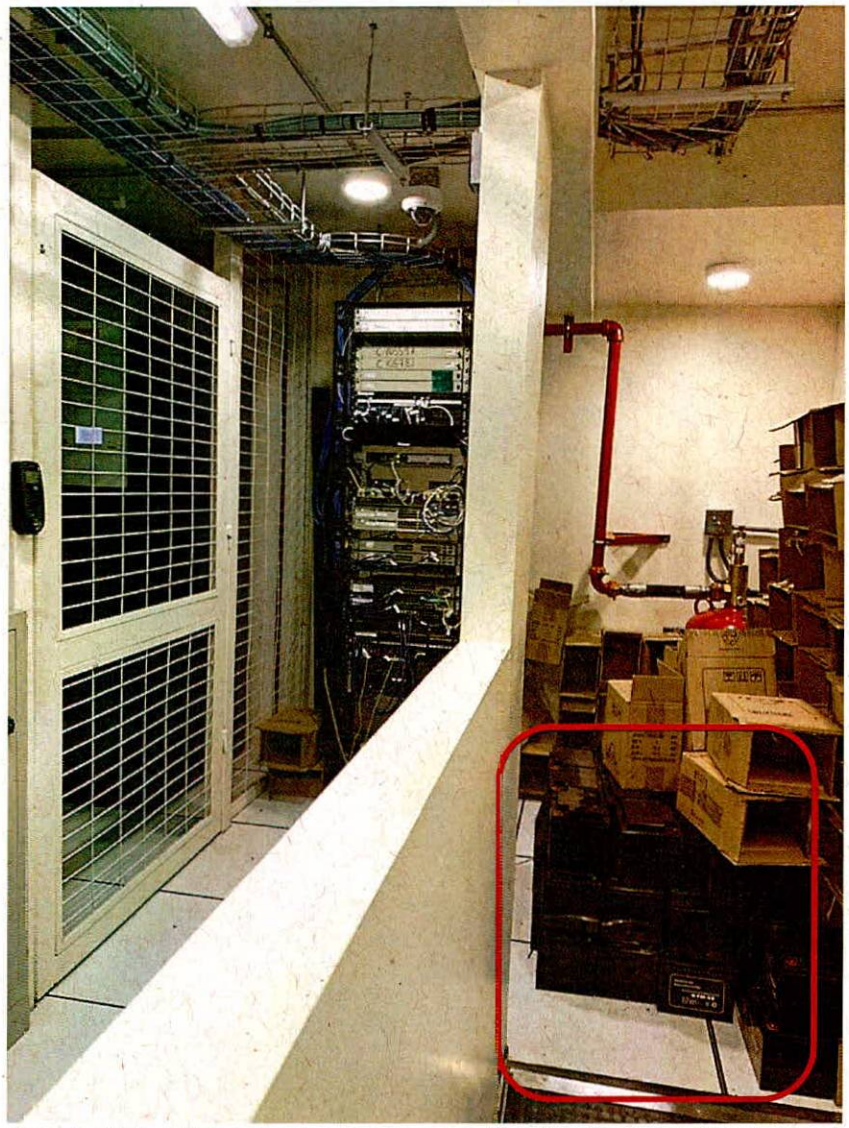
Dado que las medidas señaladas no se han materializado corresponde mantener lo objetado preliminarmente, por lo que la entidad auditada deberá implementar un registro formal para la gestión de acceso, y

bitácoras de ingreso a los espacios restringidos, para su continuo monitoreo, informando documentadamente en el plazo de 60 días hábiles contado desde la recepción del presente documento.

16. Residuos peligrosos en dependencias institucionales.

Cabe manifestar que, al momento de la visita a terreno, se advirtió que, en las oficinas de la repartición, existían baterías en desuso correspondientes a los equipos UPS, dispuestas en el pasillo que conduce a la entrada, situación que evita el normal desplazamiento en condiciones normales y dificulta el escape en situaciones de emergencia, junto con el peligro de tener ese tipo de residuos sin las medidas mínimas de seguridad, como se aprecia en la Imagen N° 2.

Imagen N° 2: Baterías de las UPS, en las dependencias institucionales.



Fuente: Fotografía tomada por el equipo fiscalizador, en visita a terreno del día 21 de julio de 2021.

Lo indicado vulnera lo estipulado en el artículo 17, que establece que los equipos deberán protegerse físicamente de las amenazas de riesgo del ambiente externo, pérdida o daño, y que la ubicación del mismo deberá disminuir las posibilidades de amenazas de humedad y agua, entre otros, decreto N° 83, de 2004, sobre la gestión de las operaciones y las comunicaciones.

Adicionalmente transgrede lo estipulado en el artículo 6°, del decreto N° 148, de 2004, del Ministerio de Salud, mediante el cual se aprueba el reglamento sanitario sobre manejo de residuos peligrosos, que señala que durante el manejo de los residuos peligrosos se deberán tomar todas las precauciones necesarias para prevenir su inflamación o reacción, entre ellas su separación y protección frente a cualquier fuente de riesgo capaz de provocar tales efectos; además señala que, durante las diferentes etapas del manejo de tales residuos, se deberán tomar todas las medidas necesarias para evitar derrames, descargas o emanaciones de sustancias peligrosas al medio ambiente.

Las SMA señaló en su respuesta que gestionará el retiro de las baterías en desuso desde las dependencias del datacenter y se verá la posibilidad de traslado de ellas a una entidad certificada que cumpla con la normativa vigente.

Teniendo en consideración que la solución planteada no se ha materializado, corresponde mantener el hecho objetado, por lo que la entidad fiscalizada deberá gestionar el retiro de las baterías en desuso desde las dependencias del datacenter y su traslado a una entidad certificada que cumpla con la normativa vigente, respaldando dicha labor, en el plazo de 60 días hábiles contado desde la recepción del presente documento.

Otras revisiones efectuadas

17. Sobre el proceso de emisiones y transferencia de contaminantes.

Mediante correo electrónico de 22 de marzo de 2021, la oficina de Auditoría Interna de la institución fiscalizada remitió el documento titulado "Procedimiento para el Desarrollo de Sistemas de Información Seguro", Código: SSI.PR.1 40206.1 40208.1 40209, de octubre 2019, que entrega los lineamientos generales para garantizar que ellos se diseñen e implementen de acuerdo con los requerimientos y políticas definidos y conforme a la normativa y a los objetivos descritos por la institución.

Además, dicho procedimiento establece criterios relacionados a las reglas y normas de su política, dando cumplimiento a un desarrollo seguro y estableciendo qué requisitos del negocio son satisfechos por los sistemas existentes y cuáles lo serán en las nuevas propuestas de implementación o modificación de proyectos.

En ese contexto, desde el punto de vista de los requerimientos técnicos, la documentación "Seguridad Sistema Ventanilla Única 2" define las características de nivel de aplicación, la integración y comunicación con

los sistemas sectoriales, los ambientes de desarrollo y producción y la comunicación con la interfaz de Clave Única.

Luego, desde la perspectiva de negocio, el documento "Integración sistemas sectoriales a VU2.0" describe los procesos y requisitos necesarios que debe cumplir un sistema sectorial para realizar la integración con la Ventanilla Única 2.0 del RETC del Ministerio del Medio Ambiente.

Por lo señalado y través de las pruebas realizadas por esta Entidad de Fiscalización a la plataforma RETC, se constató que la operación del aplicativo sigue los lineamientos establecidos en la documentación revisada, no determinándose observaciones sobre la materia.

18. Sobre Políticas de Seguridad de la Información.

A través de correo electrónico de 22 de marzo de 2021, la oficina de Auditoría Interna de la SMA remitió el documento titulado "Política de Seguridad para las Comunicaciones", Código: SSI.PO.13, Versión: Noviembre 2019, la cual establece los requerimientos de seguridad para la administración, implementación y diseño de las redes de comunicación informática de la institución garantizando la protección de la información en estas, así como en las instalaciones de procesamiento de información de apoyo en la Subsecretaría del Medio Ambiente.

Dentro de los procesos que se definen en el citado documento están el control de los servicios de red, los dominios de seguridad y la *conexión con terceros*. Adicionalmente, la información contenida en el antecedente "Integración sistemas sectoriales a VU2.0" establece la implementación de la integración con VU2.0 bajo el estándar Api Rest, con paquetes de mensajería en JSON.

Requerida información al respecto, la entidad indicó vía correo electrónico de 1 de septiembre de 2021, que utilizan diversas técnicas de seguridad digital de los datos del Programa RETC y sus sistemas en su conjunto, como el protocolo seguro en el servicio HTTP para una comunicación cifrada punto a punto entre el cliente y el servidor.

Asimismo, agregó que los sistemas cuentan con acceso a través de ese medio, al servidor del MINSEGPRES mediante el protocolo OAuth2, que permite generar sesiones JWT independientes, únicas y descentralizadas en materia de contraseñas.

También explicó que, para disminuir el margen de error en relación con la manipulación de datos y visualizaciones no autorizadas, se han implementado capas del Framework Laravel que controlan e impiden la inyección SQL a través de parámetros GET/POST y para el caso de las visualizaciones no autorizadas, los sistemas cuentan con roles y perfiles estructurados y programados.

Además, expuso que los servicios web utilizados permiten la comunicación Machine To Machine entre sistemas del Ministerio de Salud, del Servicio de Impuestos Internos y de la Secretaría General de la Presidencia.

De lo anteriormente expuesto, y del análisis de las características de la tecnología señalada por la repartición, no se advierten situaciones que observar.

19. Sobre los contratos revisados.

Los contratos revisados en el presente examen corresponden a los siguientes:

Tabla N° 2: Detalle de los contratos analizados.

PROVEEDOR	SERVICIO CONTRATADO	N° ORDEN DE COMPRA	FECHA	MONTO UF
Blue Company S.A.	Actualización de Sistema Ventanilla Única 2.0 y sus sistemas asociados	608897-50-CM20	26-02-2020	1.744
Tic Blue Limitada	Actualización del Reporte Único de Emisiones Atmosféricas (RUEA) y actualización de Nodo Central RETC	608897-73-CM20	12-03-2020	1.742,4

Fuente: Elaborado en base a información suministrada mediante correo electrónico de la Jefa de Auditoría Interna de la institución fiscalizada, del 11 de mayo de 2021.

Al respecto, es dable señalar que ambas órdenes de compras se encuentran bajo el convenio marco aprobado por la resolución N° 31, de 10 de septiembre de 2015, que adjudica la Propuesta Pública de Convenio Marco ID N° 2239-3-LP15, para Perfiles para el Desarrollo y Mantención de Sistemas Informáticos.

De la revisión de la información remitida durante el presente examen por la jefa de Auditoría Interna del Ministerio de Medio Ambiente, y de antecedentes descargados del portal Mercado Público, sobre los contratos analizados, es del caso señalar lo siguiente:

- Acuerdo suscrito con la empresa Blue Company S.A. para la "Actualización del Sistema Ventanilla Única 2.0 y sus Sistemas Asociados".

Los términos de referencia de esta contratación establecieron que se requería el apoyo externo para la realización de distintas labores de configuración, actualización y acompañamiento, las cuales incluían mejoras en las bases de datos históricas de los sistemas sectoriales de la Ventanilla Única del RETC y poblamiento de la información con la versión 1.0.

En ese contexto, dichos términos de referencia plantean necesario adquirir servicios de reconfiguración y actualización del Sistema Ventanilla Única 2.0 del RETC para mantener un funcionamiento continuo de la plataforma, señalando como objetivos:

- Actualización Sistema de Tickets.
- Carga de datos desde Ventanilla Única 1.0 a Ventanilla Única 2.0.
- Preparación del servidor de producción.
- Configuración y adecuación de servicios Web.
- Integración de VU 2.0 con sistemas vinculados.
- Integración con Nodo Central de RETC.
- Test de funcionamiento de integridad de módulos.

En el mencionado documento se definieron los siguientes productos a entregar:

- Implementación y actualización de las actividades del punto 5.
- Procedimientos de revisión y prueba del sistema.
- Diccionario de datos y documentación actualizadas.
- Productos cargados en la plataforma Gitlab del Ministerio del Medio Ambiente.

La descripción del servicio, el detalle de los códigos y los valores bajo convenio marco son los que se indican a continuación:

Tabla N° 3: Detalle de los términos de referencia del Sistema de Ventanilla Única.

CÓDIGO / ID	CANTIDAD HORAS HOMBRE	COSTO HORAS HOMBRE (UF)	COSTO TOTAL UF
1155144	2.880	0,3	864
1155146	1.760	0,5	880
Total	4.640		1.744

Fuente: Elaboración propia en base a la información descargada el 26 de abril de 2021 desde la plataforma electrónica de Mercado Público.

El plazo máximo señalado en los términos de referencia para la entrega de los productos se estableció en 8 meses, desde la fecha de emisión de la orden de compra correspondiente.

La forma de pago fijada entre las partes fue de 4 cuotas contra aprobación de los informes que se exponen a continuación:

- Pago 1: Después de entregado y aprobado el primer informe de actividades, correspondiendo al 30% del presupuesto total.
- Pago 2: Después de entregado y aprobado el segundo informe de actividades, siendo el 30% del presupuesto total.
- Pago 3: Después de entregado y aprobado el tercer informe de actividades, fijándose en el 30% del presupuesto total.

- Pago 4: Después de entregado y aprobado el informe final de actividades, recepcionado conforme con todos los productos y resultados esperados indicados en el punto N° 5, correspondiendo al 10% del presupuesto total.

Del análisis de los antecedentes remitidos por ese servicio, se acreditaron 4 pagos realizados a partir de la entrega por parte de la empresa de los informes de avance correspondientes al primer, tercer, sexto y octavo mes del desarrollo de las funciones requeridas.

Sobre el particular, es dable señalar que de la información revisada correspondiente al contrato establecido con la empresa Blue Company S.A, relacionado con la "Actualización de Sistema Ventanilla Única 2.0 y sus Sistemas Asociados", no se advirtieron situaciones que observar.

- Acuerdo suscrito con la empresa TIC Blue Limitada para la "Actualización del Reporte Único de Emisiones Atmosféricas (RUEA) y Actualización de Nodo Central RETC".

Los términos de referencia relativos a esta contratación indican que con la tramitación en el Congreso de la Ley de Cambio Climático, se requería información base para insumir los elementos técnicos relacionados con las variables requeridas para la cuantificación de las emisiones de GEI[38] del sector industrial, y que están directamente vinculados con la operatividad del aplicativo RUEA - GEI, mediante la integración de todos los sistemas de reportes a esa fecha -Sistema F138, Sistema Impuestos Verdes (SIV), Norma de Termoeléctrica, Norma de Fundición, Norma de Incineración y Co-incineración, y los Planes de Descontaminación-, de manera de contar con un solo dato oficial.

Agregan dichos términos que el RUEA - GEI consta de tres etapas:

- Registro de Fuentes y Procesos: Permitirá entregar antecedentes relevantes para el módulo de cuantificación de emisiones en forma actualizada, subsanando el problema de temporalidad en los informes, producto de los diferentes periodos de reporte en cada sistema a la fecha de adquisición -F138, SICTER[39], SIV[40], Registro de Calderas y Turbinas-. Esta información será registrada en el Ministerio del Medio Ambiente y reenviada mediante web services a los distintos sistemas de cuantificación de emisiones para el cumplimiento de la normativa vigente, lo cual subsana las brechas e inconsistencias existentes entre los sistemas que administran la Subsecretaría de Medio Ambiente y el Ministerio de Salud.
- Módulo de Cuantificación de Emisiones: Cada uno de los módulos de cuantificación asociados al cumplimiento de normas de emisión, planes de descontaminación e impuestos verdes recibirá previamente la información procedente del Registro de Fuentes y Procesos.

38 GEI: Emisiones y absorciones de gases de efecto invernadero.
39 Sistema de Centrales Termoeléctricas.
40 Sistema de Impuestos Verdes..

- Módulo de Informes: Corresponde a un módulo de generación de reportes, tanto de emisiones como de fuentes, al cual tendrán acceso todos los stakeholders vinculados con la información de carácter ambiental relacionada a las emisiones de fuentes fijas -Ministerio de Medio Ambiente, Subsecretaría de Medio Ambiente, Ministerio de Salud y Ministerio de Energía-.

Relacionado con el trabajo de mejoras en la gestión y calidad de información, los términos de referencia requirieron dimensionar diversos aspectos que condicionan su manejo, tales como; nuevas normativas o requerimientos de datos que demandan la captura de una gran cantidad de antecedentes por parte del Ministerio de Medio Ambiente y de otras instituciones públicas para la actualización de esta infraestructura, a partir de un enfoque de Business Intelligence, con el objetivo de abordar el manejo y análisis de antecedentes acorde a las exigencias de un análisis del tipo descriptivos, predictivo y prescriptivo.

La actualización del Nodo Central se enfocó en los siguientes componentes:

- Sistemas transaccionales.
- Repositorio analítico (Data Mart/Data Warehouse).
- Análisis multidimensional (OLAP por su sigla en inglés).

Como descripción del servicio, se estableció el detalle de códigos y valores bajo convenio marco son los que se indican a continuación:

Tabla N° 4: Detalle de los términos de referencias del Sistema Reporte Único de Emisiones Atmosféricas, RUEA.

CÓDIGO / ID	CANTIDAD HORAS HOMBRE	COSTO HORAS HOMBRE UF	COSTO TOTAL UF
1155010	320	0,72	230,4
1155146	1.760	0,45	792
1155144	640	0,3	192
1155036	1.600	0,33	528
Total	4.320		1.742,4

Fuente: Elaboración propia de acuerdo con la información descargada el 26 de abril de 2021 desde la plataforma electrónica de mercado público.

El plazo máximo de entrega, señalado en los referidos términos de referencia correspondió a 8 meses, desde la fecha de emisión de la orden de compra correspondiente.

Para efectos de comunicación entre las partes, dicho documento definió como contraparte técnica a Juan Pizarro Miranda, profesional del Departamento de Información Ambiental de la División de Información y Economía Ambiental.

Asimismo, se estableció en el punto N° 10, del requerimiento de compra, que el pago se realizaría en pesos chilenos, de acuerdo con la siguiente forma:

- Pago 1: por 522,72 UF con la recepción conforme de la contraparte técnica del informe.
- Pago 2: por 522,72 UF con la recepción conforme de la contraparte técnica del informe.
- Pago 3: por 522.72, UF con la recepción conforme de la contraparte técnica del informe.
- Pago 4: por 174,24, UF con la recepción conforme con todos los productos y resultados esperados indicados en estos requerimientos por la contraparte técnica del informe final.

Sobre lo anterior, se debe señalar que del análisis de la información relacionada con el referido contrato suscrito con la empresa TIC BLUE Limitada, por el servicio de "Actualización del Reporte Único de Emisiones Atmosféricas (RUEA) y Actualización de Nodo Central RETC", no se advirtieron observaciones.

CONCLUSIONES

Atendidas las consideraciones expuestas durante el desarrollo del presente trabajo, el Ministerio de Medio Ambiente no ha aportado antecedentes e iniciado acciones que permitan salvar las observaciones formuladas en el Preinforme de Observaciones N° 630, de 2021, de esta Contraloría General.

Sobre las observaciones que se mantienen, se deberán adoptar medidas con el objeto de dar estricto cumplimiento a las normas legales y reglamentarias pertinentes, entre las cuales se estima necesario considerar, a lo menos, las siguientes:

1. En relación con el punto 1.1, Falta de procedimientos de recuperación de desastres (C), la repartición deberá elaborar dicho instrumento e informar sobre su estado de avance en el plazo de 60 días hábiles contado desde la recepción del presente informe final.

Sobre el punto 1.2, Ausencia de un procedimiento para el control de los cambios realizados en los sistemas informáticos en operación en el RETC (C), la entidad tendrá que confeccionar la documentación técnica del citado sistema, comunicando su estado de avance en el término de 60 días hábiles a contar de la recepción del presente documento.

Para lo manifestado en el numeral 2, Inexistencia de acuerdos de confidencialidad en los contratos (C), la repartición deberá incorporar acuerdos de confidencialidad en los acuerdos que elabore a futuro.

En lo que atañe al numeral 3. Falta de procedimientos para la validación de la integridad de la información recepcionada por el RETC (C), corresponde que la entidad desarrolle y remita el proceso formalizado que incorpore las etapas y actividades de control que permitan la validación de la integridad de la información del aludido sistema, en el mismo plazo ya anotado.

2. En lo concerniente a lo observado en el numeral 4, Inexistencia de evidencia que dé cuenta de la realización de las reuniones del Comité de Seguridad de la Información (C), la repartición deberá remitir el documento que contiene la calendarización de las respectivas reuniones, debidamente formalizado, en el plazo de 60 días hábiles a contar de la recepción del presente informe final.

En cuanto a lo expuesto en el numeral 5, Inexistencia de procedimientos que garanticen la continuidad operacional (C), corresponde que la repartición remita la mejora de los procedimientos actuales y el control en el monitoreo, especialmente en lo referido al respaldo y restauración de información, en el término de 60 días hábiles, a contar desde la recepción del presente documento.

Acerca de lo objetado en el numeral 6, Ausencia de monitoreo de la actividad de la red (C), la repartición deberá remitir el documento sancionado que contenga la calendarización de las fechas de recopilación de los reportes, evidencias y registros periódicos, contemplado en el Compromiso de Desempeño Colectivo, en el plazo de 60 días hábiles contado desde la recepción del presente informe final.

En lo que atañe al numeral 7, Falta de un procedimiento de configuración de los sistemas (C), la entidad deberá complementar su Política de Seguridad para las Operaciones, de manera de incorporar las omisiones advertidas por esta Entidad de Control, suministrando un informe de avance en el plazo de 60 días hábiles contado desde la recepción del presente documento.

Respecto de lo advertido en el numeral 8, Inexistencia de procedimientos para la autorización, registro, modificación, revocación y revisión periódica de los permisos de acceso de los usuarios (C), corresponde que el Departamento de TI de esa subsecretaría desarrolle un protocolo institucional que administre el alta, baja y los perfiles de usuario y elabore un procedimiento formal de revisión de derechos de acceso, remitiendo la documentación que acredite el estado de avance de lo dispuesto, en el plazo de 60 días hábiles contado desde la recepción del presente documento.

Para lo manifestado en el numeral 9, Inexistencia de un procedimiento sobre el cambio de contraseña después del primer inicio de sesión (C), la repartición fiscalizada deberá revisar el procedimiento de verificación de inicio de sesión seguro (Código:SSI.PR.09.04.02), de modo de

optimizar los criterios y reglas de complejidad y la incorporación de estos en los actuales desarrollos de la institución, incluyendo tanto los de Ventanilla Única, como los futuros desarrollos interno y externos, remitiendo la documentación en el término de 60 días hábiles a contar de la recepción del presente informe final.

En cuanto a lo manifestado en el numeral 10, Ausencia de políticas de uso, almacenamiento, acceso y distribución de mensajes electrónicos (C), corresponde que la entidad elabore un procedimiento formal de la política de correos de la Institución y lo remita en el mismo plazo antes anotado.

En lo que atañe a lo objetado en los numerales 11, Falta de registro de ejecución y recuperación de respaldos (C) y numeral 12, Falta de registros de pruebas de respaldo y recuperación de la información (C), la repartición deberá confeccionar un ejercicio de restauración para la verificación de los respaldos de los servidores AVAMAR, así como la calendarización para el año 2022 de los trabajos de respaldo, verificación y restauración del sistema de RETC y remitir los resultados en el término de 60 días hábiles a contar de la recepción del presente informe final.

Sobre lo observado en el numeral 13, Falta de implementación de un sitio externo de almacenamiento que cumpla al menos con las mismas características de seguridad que el sitio principal. (C), la entidad deberá desarrollar una solución para dar respuesta a los sistemas críticos priorizados por la institución, así como el análisis de factibilidad y recursos para la disposición de un sitio secundario, informando sobre el estado de avance de ello, remitiendo dicho antecedente en el mismo plazo ya señalado.

En lo que toca a lo expuesto en los numerales 14, Falta del protocolo de ingreso a las salas de servidores. (C), y 15, Ausencia de registros de ingreso al datacenter (C), la repartición deberá implementar un registro formal para la gestión de acceso, y bitácoras de ingreso a los espacios restringidos, para su continuo monitoreo, informando documentadamente en el plazo de 60 días hábiles contado desde la recepción del presente informe final.

En lo referente a lo indicado en el punto 16, Residuos peligrosos en dependencias institucionales (C), corresponde que la entidad gestione el retiro de las baterías en desuso desde las dependencias del datacenter y su traslado a una entidad certificada que cumpla con la normativa vigente en el plazo de 60 días hábiles contado desde la recepción del presente documento.

Finalmente, para aquellas observaciones que se mantienen, que fueron catalogadas como C, identificadas en el "Informe de Estado de Observaciones", de acuerdo al formato adjunto en el Anexo N° 4, las medidas que al efecto implemente el servicio deberán acreditarse y documentarse en el Sistema de Seguimiento y Apoyo CGR, que esta Entidad de Control puso a disposición de las entidades públicas, según lo dispuesto en el oficio N° 14.100, de 2018, de este origen, en un plazo de 60 días hábiles contado desde la recepción de este informe.

Remítase el presente informe final a la Ministra del Medio Ambiente, a la Jefa de la Oficina de Auditoria Interna de dicho ministerio, y al Subsecretario de Medio Ambiente.

Saluda atentamente a Ud.,

DANIEL CAVIEDES GONZALEZ
Jefe Unidad de Auditorías de Sistemas
Departamento de Auditorías Especiales
CONTRALORÍA GENERAL DE LA REPÚBLICA

ANEXO N° 1: Plataforma Registro de Emisiones y Transferencias de Contaminantes.

Principales ojetivos del RETC:

a) Facilitar el acceso a la información sobre emisiones, residuos y transferencias de contaminantes;

b) Promover el conocimiento de la información, por parte de la ciudadanía;

c) Constituir una herramienta de apoyo para la adopción de políticas públicas y de regulación;

d) Constituir una herramienta que favorezca la toma de decisiones en el diseño de la política de gestión ambiental encaminada a reducir la contaminación, prevenir la generación de residuos y promover su valorización, y avanzar hacia un desarrollo sustentable;

e) Facilitar a los sujetos regulados la entrega de la información sobre las emisiones, residuos, transferencias de contaminantes y productos prioritarios;

f) Propender a generar una gestión ambiental más adecuada de las emisiones, residuos y transferencias de contaminantes por parte de la industria y municipalidades;

g) Generar el Sistema de Ventanilla Única como formulario único de acceso y reporte con el fin de concentrar la información objeto de reporte en una base de datos que permita la homologación y facilite su entrega por parte de los sujetos obligados a reportar.

Sistema Ventanilla Única del RETC, VU.

Corresponde a un aplicativo electrónico que contempla un formulario único disponible en el portal electrónico del RETC y a través del cual se accede[42] a los sistemas de declaración[43] de los órganos fiscalizadores para dar cumplimiento a la obligación de reporte de los establecimientos emisores o generadores.

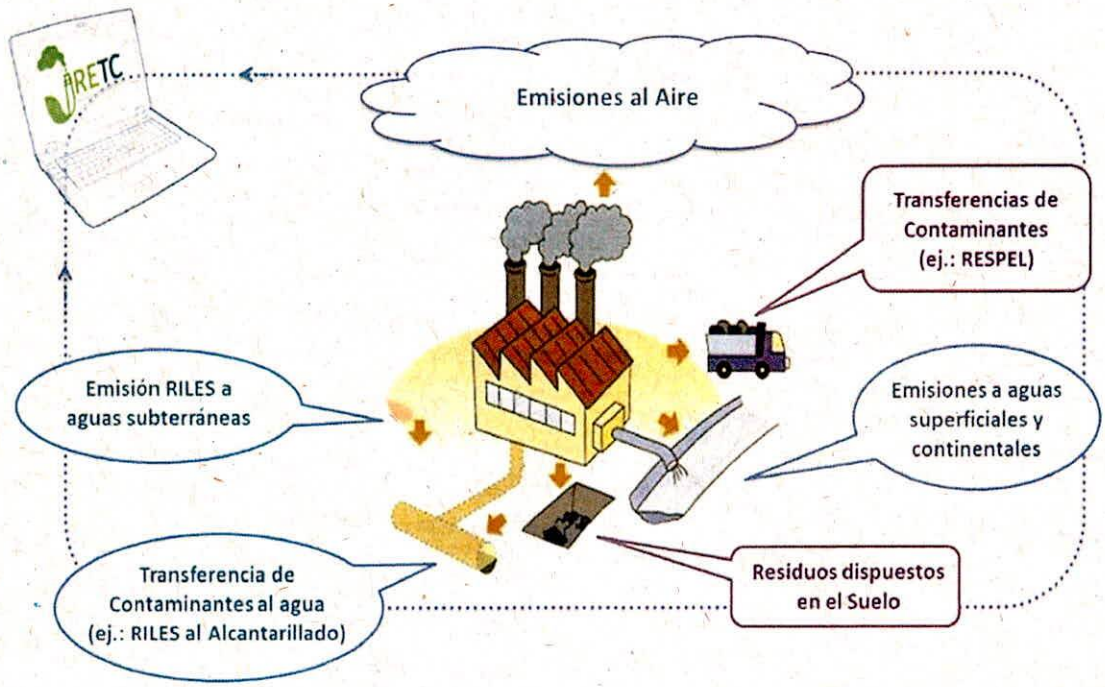
Reporte Único de Emisiones Atmosféricas, RUEA.

El módulo de Reporte Único de Emisiones Atmosféricas corresponde a la actualización del sistema de declaración F138. Su objetivo es realizar la cuantificación de emisiones mediante factores de emisión o con información precargada desde otros sistemas de reporte (tanto de la Superintendencia del Medio Ambiente, el Ministerio de Salud y del Ministerio del Medio Ambiente, tales como; Sistema de Centrales Termoeléctricas, SICTER; Sistema de Impuestos Verdes, SIV, y Formulario Electrónico - F138.

42 Acceden los representantes de la empresa autorizadas para subir información y usuarios institucionales.

43 Formulario único disponible en el portal electrónico del RETC y a través del cual se accederá a los sistemas de declaración de los órganos fiscalizadores, para dar cumplimiento a la obligación de reporte de los establecimientos emisores o generadores.

Imagen N° 3: Esquema general de emisiones, residuos y/o transferencias de contaminantes asociadas al ingreso a través del Sistema VU del RETC.



Fuente: Documentación proporcionada por el organismo mediante correo de 24 de marzo de 2021.

Los sujetos regulados deben ingresar al Sistema Ventanilla Única del RETC, y es el Encargado de Establecimiento quien solicita su creación, para posteriormente efectuar las distintas declaraciones o entrega de reportes, registrando en dicha solicitud, además, los datos básicos para la identificación de la dependencia. Una vez aprobado por la autoridad, éste solicita su incorporación a los distintos sistemas de declaración y reporte integrados con el Sistema Ventanilla Única del RETC.

Luego de la activación en los aplicativos de declaración y reporte, el Encargado de Establecimiento[43] puede gestionar a los usuarios delegados de los sistemas, para que estos puedan declarar en las plataformas sectoriales y dar cumplimiento a los elementos establecidos en la normativa asociada a cada sistema de declaración.

43 Encargado de Establecimiento: corresponde al cargo responsable en materias ambientales dentro del establecimiento, quien deberá informar las modificaciones del establecimiento en el Sistema VU RETC; tales como, actualización de razón social; cambio de titularidad, cese de funciones, administración de usuarios delegados, cambio de encargado del establecimiento y representante legal.

Imagen N° 4: Esquema general simplificado del funcionamiento del RETC.

Fuente: Documentación proporcionada por el organismo mediante correo electrónico de 24 de marzo de 2021.

La información de los sujetos regulados permite identificar y estandarizar a quienes deben cumplir con las regulaciones, luego dichos sujetos deben registrar sus declaraciones en los respectivos sistemas sectoriales.

Una vez que se efectúan los procesos de declaración, según lo indicado en el artículo 13, del decreto supremo N° 1, de 2013, del MMA, los Enlaces del RETC, deben ingresar la información del año anterior, a más tardar en mayo de cada año, para lo cual se facilitan distintos mecanismos que permitan la entrega de la información.

Indicado lo anterior, y en relación a la recepción de los datos 2019 -declaración 2020- de los diferentes sistemas asociados al Sistema VU RETC, estos se realizan mediante diferentes medios:

a) Cargas sectoriales en el Sistema Ventanilla Única del RETC: Es un repositorio de archivos disponibles para los enlaces del RETC en su sesión de usuarios, en el cual pueden cargar la información de emisiones y transferencias de contaminantes.

b) Bases de datos internas: En los sistemas administrados por el Departamento de Información Ambiental, se tiene acceso a las bases de datos de forma interna.

c) Recepción mediante webservice.

Una vez recibidos los datos, estos son revisados a través de un tratamiento denominado ETL, Extract -Transform – Load. Ahí se verifica que no existan omisiones o errores en la información, luego estos datos son adaptados y transformados con el fin de poder almacenarlos en el nodo central del RETC. Para concluir, se realiza un chequeo para verificar que toda la información fue cargada a la base de datos.

Finalmente, la información permite la generación de los reportes y la construcción de los indicadores del Informe Consolidado de Emisiones y Transferencias de Contaminantes.

Esta información queda en una Base de Datos del RETC, relativa al año de reporte, y es difundida a través del portal Web del RETC.

Imagen N° 5: Diagrama General del proceso de gestión de datos del RETC.

Fuente: Documentación proporcionada por el organismo mediante correo electrónico de 24 de marzo de 2021.

Durante el primer trimestre de 2020, entró en operación una nueva versión de la plataforma RETC, que incluye una serie de innovaciones tecnológicas y modernización de procesos, que implican un cambio en la forma de realizar las declaraciones de emisiones atmosféricas ante los organismos del Estado.

La principal innovación del Registro es que cuenta con un Sistema de Registro de Fuentes y Procesos donde por única vez el usuario deberá registrar las fuentes fijas de emisiones existentes en sus establecimientos y que están sujetas a diferentes normativas. Esto permitirá generar un catastro único, con información que la plataforma compartirá con los cuatro sistemas de declaración de emisiones atmosféricas que la normativa fija:

- El Formulario 138
- Sistema de Centrales Termoeléctricas SICTER (DS13)
- El Sistema de Impuestos Verdes
- El Sistema de Planes de Descontaminación Atmosférica

A partir de esta actualización, el Registro de Fuentes y Procesos opera como una puerta de entrada para los mencionados sistemas, centralizando la información en el nuevo Reporte Único de Emisiones Atmosféricas, RUEA.

La interoperabilidad entre el registro y los distintos sistemas sectoriales elimina la duplicidad de requerimientos por parte del Estado en esta materia, quedando solo acotado al reporte de las emisiones sujetas al cumplimiento normativo ante las distintas instituciones: los ministerios de Salud y Medio Ambiente y la Superintendencia del Medio Ambiente.

Imagen N° 6: Esquema de interoperabilidad entre el registro y los distintos sistemas sectoriales.

Fuente: Documentación proporcionada por el organismo mediante correo de 24 de marzo de 2021.

ANEXO N° 2: Detalle del Contrato del Sistema de Ventanilla Única.

SERVICIO CONTRATADO	Puesta en marcha del Sistema Ventanilla Única 2.0 y sus sistemas asociados
NOMBRE DEL PROVEEDOR	Blue Company S.A.
RUT DEL PROVEEDOR	96.981.410-2
IDENTIFICADOR MERCADO PÚBLICO	ID N° 608897-50-CM20
RESOLUCIÓN QUE ADJUDICA CONVENIO MARCO	Resolución N° 31, de 10 de septiembre de 2015
MONTO TOTAL DEL CONTRATO	UF 1.744,0000
MODALIDAD DE PAGO	4 pagos contra aprobación de informes (pagos 1 al 3, 30% cada uno; y pago 4 del 10%)
DURACIÓN DEL CONTRATO	8 meses
FECHA DE INICIO	26 de febrero de 2020
TIPO DE CAUCIÓN	Boleta de Garantía o Certificado de Fianza a la vista o Vale Vista u Otro
BENEFICIARIO DE LA GARANTÍA	Dirección de Compras y Contratación Pública
MONTO DE LA CAUCIÓN	$ 250.000
FECHA DE VENCIMIENTO DE LA BOLETA DE GARANTÍA	31-12-2021
TIPO DE MULTAS	El Adjudicatario podrá ser objeto de la aplicación de multas por atrasos o incumplimientos derivados de su responsabilidad
DEFINICIÓN DE LAS MULTAS	1.- Retraso en la primera respuesta de toma de conocimiento respecto a un requerimiento de servicios. 2.- Retraso de la respuesta efectiva al requerimiento informado. 3.- 20% del total del contrato por la no reparación de fallas del software original. 4.- Incumplimiento de hitos. 5.- 20% del último pago, en caso de que el software desarrollado no cumpla con el 100% de los requerimientos funcionales.

Fuente: Elaboración propia de acuerdo con la información descargada el 26 de abril de 2021 desde la plataforma electrónica de mercado público.

ANEXO N° 3: Detalle del Contrato del Sistema Reporte Único de Emisiones Atmosféricas, RUEA.

SERVICIO CONTRATADO	Actualización RUEA y Actualización del nodo de control RETC.
NOMBRE DEL PROVEEDOR	Tic Blue Limitada.
RUT DEL PROVEEDOR	76.317.379-8
IDENTIFICADOR MERCADO PÚBLICO	ID N° 608897-73 CM20
RESOLUCIÓN QUE ADJUDICA CONVENIO MARCO	Resolución N° 31, de 10 de septiembre de 2015
MONTO TOTAL DEL CONTRATO	UF 1.742,40
MODALIDAD DE PAGO	4 pagos contra aprobación de informes (pagos 1 al 3, 30% cada uno; y pago 4 del 10%)
DURACIÓN DEL CONTRATO	8 meses
FECHA DE INICIO	Fecha recepción Orden de Compra
TIPO DE CAUCIÓN	Boleta de Garantía o Certificado de Fianza a la vista o Vale Vista u Otro
BENEFICIARIO DE LA GARANTÍA	Dirección de Compras y Contratación Pública
MONTO DE LA CAUCIÓN	$ 250.000
FECHA DE VENCIMIENTO DE LA GARANTÍA	31-12-2021
TIPO DE MULTAS	El Adjudicatario podrá ser objeto de la aplicación de multas por atrasos o incumplimientos derivados de su responsabilidad
DEFINICIÓN DE LAS MULTAS	1.- Retraso en la primera respuesta de toma de conocimiento respecto a un requerimiento de servicios. 2.- Retraso de la respuesta efectiva al requerimiento informado. 3.- 20% del total del contrato por la no reparación de fallas del software original. 4.- Incumplimiento de hitos. 5.- 20% del último pago, en caso de que el software desarrollado no cumpla con el 100% de los requerimientos funcionales.

Fuente: Elaboración propia de acuerdo con la información descargada el 26 de abril de 2021 desde la plataforma electrónica de mercado público.

CONTRALORÍA GENERAL DE LA REPÚBLICA
DEPARTAMENTO DE AUDITORÍAS ESPECIALES
UNIDAD DE AUDITORÍA DE SISTEMAS

ANEXO N° 4: Estado de Observaciones de Informe Final N° 630, de 2021.

A) OBSERVACIONES QUE VAN A SEGUIMIENTO POR PARTE DE LA CONTRALORÍA GENERAL

Nº DE OBSERVACIÓN Y EL ACÁPITE	MATERIA DE LA OBSERVACIÓN	NIVEL DE COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN O VERIFICAR MEDIDAS ADOPTADAS	MEDIDA IMPLEMENTADA Y SU DOCUMENTACIÓN DE RESPALDO	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DEL SERVICIO
Capítulo I, Aspectos de control interno, acápite 1. Situaciones de riesgo no controlados por el servicio, numeral 1.1.	Falta de procedimientos de recuperación de desastres.	C: Observación Compleja.	La repartición deberá elaborar dicho instrumento e informar sobre su estado de avance en el plazo de 60 días hábiles contado desde la recepción del presente informe final.			
Capítulo I, Aspectos de control interno, acápite 1. Situaciones de riesgo no controlados por el servicio, numeral 1.2.	Ausencia de un procedimiento para el control de los cambios realizados en los sistemas informáticos en operación en el RETC.	C: Observación Compleja.	La entidad tendrá que confeccionar la documentación técnica del citado sistema, comunicando su estado de avance en el término de 60 días hábiles a contar de la recepción del presente informe final.			
Capítulo I, Aspectos de control interno, numeral 3.	Falta de procedimientos para la validación de la integridad de la información recepcionada por el RETC.	C: Observación Compleja.	Corresponde que la SMA desarrolle y remita el procedimiento formalizado que incorpore las etapas y actividades de control que permitan la validación de la integridad de la información del aludido sistema, , en el término de 60 días hábiles a contar de la recepción del presente informe final.			

CONTRALORÍA GENERAL DE LA REPÚBLICA
DEPARTAMENTO DE AUDITORÍAS ESPECIALES
UNIDAD DE AUDITORÍA DE SISTEMAS

Nº DE OBSERVACIÓN Y EL ACÁPITE	MATERIA DE LA OBSERVACIÓN	NIVEL DE COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN O VERIFICAR MEDIDAS ADOPTADAS	MEDIDA IMPLEMENTADA Y SU DOCUMENTACIÓN DE RESPALDO	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DEL SERVICIO
Capítulo II, Examen de la Materia Auditada, numeral 4.	Inexistencia de evidencia que dé cuenta de la realización de las reuniones del Comité de Seguridad de la Información.	C: Observación Compleja.	La repartición deberá remitir el documento que contiene la calendarización de las respectivas reuniones, debidamente formalizado en el plazo de 60 días hábiles á contar de la recepción del presente informe final.			
Capítulo II, Examen de la Materia Auditada, numeral 5.	Inexistencia de procedimientos que garanticen la continuidad operacional.	C: Observación Compleja.	Corresponde que la repartición remita la mejora de los procedimientos actuales y el control en el monitoreo; especialmente en lo referido al respaldo y restauración de información, en el término de 60 días hábiles, a contar desde la recepción del presente informe final.			
Capítulo II, Examen de la Materia Auditada, numeral 6.	Ausencia de monitoreo de la actividad de la red..	C: Observación Compleja.	La institución fiscalizada deberá remitir el documento sancionado que contenga la calendarización de las fechas de recopilación de los reportes, evidencias y registros periódicos, contemplado en el Compromiso de Desempeño Colectivo, en el plazo de 60 días hábiles contado desde la recepción del presente informe final.			

CONTRALORÍA GENERAL DE LA REPÚBLICA
DEPARTAMENTO DE AUDITORÍAS ESPECIALES
UNIDAD DE AUDITORÍA DE SISTEMAS

Nº DE OBSERVACIÓN Y EL ACÁPITE	MATERIA DE LA OBSERVACIÓN	NIVEL DE COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN O VERIFICAR MEDIDAS ADOPTADAS	MEDIDA IMPLEMENTADA Y SU DOCUMENTACIÓN DE RESPALDO	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DEL SERVICIO
Capítulo II, Examen de la Materia Auditada, numeral 7.	Falta de un procedimiento de configuración de los sistemas.	C: Observación Compleja.	La entidad deberá complementar su Política de Seguridad para las Operaciones, de manera de incorporar las omisiones advertidas por esta Entidad de Control, suministrando un informe de avance en el plazo de 60 días hábiles contado desde la recepción del presente informe final.			
Capítulo II, Examen de la Materia Auditada, numeral 8.	Inexistencia de procedimientos para la autorización, registro, modificación, revocación y revisión periódica de los permisos de acceso de los usuarios.	C: Observación Compleja.	Corresponde que el Departamento de TI, desarrolle un protocolo institucional que administre el alta, baja y los perfiles de usuario y elabore un procedimiento formal de revisión de derechos de acceso, remitiendo la documentación que acredite el estado de avance de lo dispuesto, en el plazo de 60 días hábiles contado desde la recepción del presente informe final.			

CONTRALORÍA GENERAL DE LA REPÚBLICA
DEPARTAMENTO DE AUDITORÍAS ESPECIALES
UNIDAD DE AUDITORÍA DE SISTEMAS

Nº DE OBSERVACIÓN Y EL ACÁPITE	MATERIA DE LA OBSERVACIÓN	NIVEL DE COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN O VERIFICAR MEDIDAS ADOPTADAS	MEDIDA IMPLEMENTADA Y SU DOCUMENTACIÓN DE RESPALDO	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DEL SERVICIO
Capítulo II, Examen de la Materia Auditada, numeral 9.	Inexistencia de un procedimiento sobre el cambio de contraseña después del primer inicio de sesión.	C: Observación Compleja.	La entidad deberá revisar el procedimiento de verificación de inicio de sesión seguro (Código:SSI.PR.09.04.02), de modo de optimizar los criterios y reglas de complejidad y la incorporación de estos en los actuales desarrollos de la institución, incluyendo tanto los de Ventanilla Única, como los futuros desarrollos interno y externos, remitiendo la documentación en el término de 60 días hábiles a contar de la recepción del presente informe final.			
Capítulo II, Examen de la Materia Auditada, numeral 10.	Ausencia de políticas de uso, almacenamiento, acceso y distribución de mensajes electrónicos.	C: Observación Compleja.	Corresponde que la entidad elabore un procedimiento formal de la política de correos de la Institución y lo remita en el plazo de 60 días hábiles a contar de la recepción del presente informe final.			

CONTRALORÍA GENERAL DE LA REPÚBLICA
DEPARTAMENTO DE AUDITORÍAS ESPECIALES
UNIDAD DE AUDITORÍA DE SISTEMAS

Nº DE OBSERVACIÓN Y EL ACÁPITE	MATERIA DE LA OBSERVACIÓN	NIVEL DE COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN O VERIFICAR MEDIDAS ADOPTADAS	MEDIDA IMPLEMENTADA Y SU DOCUMENTACIÓN DE RESPALDO	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DEL SERVICIO
Capítulo II, Examen de la Materia Auditada, numeral 14.	Falta del protocolo de ingreso a las salas de servidores.	C: Observación Compleja.	La institución fiscalizada deberá implementar un registro formal para la gestión de acceso, y bitácoras de ingreso a los espacios restringidos, para su continuo monitoreo, informando documentadamente en el plazo de 60 días hábiles contado desde la recepción del presente informe final.			
Capítulo II, Examen de la Materia Auditada, numeral 15.	Ausencia de registros de ingreso al datacenter.	C: Observación Compleja.				
Capítulo II, Examen de la Materia Auditada, numeral 16.	Residuos peligrosos en dependencias institucionales.	C: Observación Compleja.	Corresponde que la entidad gestione el retiro de las baterías en desuso desde las dependencias del datacenter y su traslado a una entidad certificada que cumpla con la normativa vigente en el plazo de 60 días hábiles contado desde la recepción del presente informe final.			

CONTRALORÍA GENERAL DE LA REPÚBLICA
DEPARTAMENTO DE AUDITORÍAS ESPECIALES
UNIDAD DE AUDITORÍA DE SISTEMAS

Nº DE OBSERVACIÓN Y EL ACÁPITE	MATERIA DE LA OBSERVACIÓN	NIVEL DE COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN O VERIFICAR MEDIDAS ADOPTADAS	MEDIDA IMPLEMENTADA Y SU DOCUMENTACIÓN DE RESPALDO	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DEL SERVICIO
Capítulo II, Examen de la Materia Auditada, numerales 11 y 12.	Falta de registro de ejecución y recuperación de respaldos.	C: Observación Compleja.	La repartición deberá confeccionar un ejercicio de restauración para la verificación de los respaldos de los servidores AVAMAR, así como la calendarización para el año 2022 de los trabajos de respaldo, verificación y restauración del sistema de RETC y remitir los resultados en el término de 60 días hábiles a contar de la recepción del presente informe final.			
	Falta de registros de pruebas de respaldo y recuperación de la información.	C: Observación Compleja.				
Capítulo II, Examen de la Materia Auditada, numeral 13.	Falta de implementación de un sitio externo de almacenamiento que cumpla al menos con las mismas características de seguridad que el sitio principal.	C: Observación Compleja.	La entidad deberá desarrollar una solución para dar respuesta a los sistemas críticos priorizados por la institución, así como el análisis de factibilidad y recursos para la disposición de un sitio secundario, informando sobre el estado de avance de ello, remitiendo dicho antecedente en el término de 60 días hábiles a contar de la recepción del presente informe final.			