



REGLAMENTO N° 2 DE 2026

Miércoles, 08 de abril de 2026

REGLAMENTO DE CUENTAS DE CORREO ELECTRÓNICO INSTITUCIONAL DE LA MUNICIPALIDAD DE VILLA ALEGRE.

VISTO Y CONSIDERANDO:

1. Decreto 100, que Fija el Texto Refundido, Coordinado y Sistematizado de la Constitución Política de la República de Chile.
2. DFL 1-19.653, que Fija el Texto Refundido, Coordinado y Sistematizado de la Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado.
3. DFL 1, que Fija el Texto Refundido, Coordinado y Sistematizado de la Ley N° 18.695, Orgánica Constitucional de Municipalidades.
4. Ley 19.880, que Establece Bases de los Procedimientos Administrativos que rigen los Actos de los Órganos de la Administración del Estado.
5. Ley 21.180, sobre Transformación Digital del Estado.
6. Ley 19.628, sobre Protección de la Vida Privada.
7. Ley N° 21.663, Marco de Ciberseguridad.
8. Decreto 10 que establece norma técnica de documentos y expedientes electrónicos para la gestión de procedimientos administrativos.
9. Decreto Alcaldicio N° 970, de 17 de mayo de 2019, que Aprueba Reglamento de Organización y Funcionamiento Interno de la Municipalidad de Villa Alegre.
10. Correo electrónico de fecha 11 de febrero de 2026, por medio del cual la Coordinadora de Transformación Digital remitió el borrador del reglamento, invitando a las unidades competentes a participar mediante su revisión y formulación de observaciones.
11. Decreto Alcaldicio N° 2572 del 06 de diciembre de 2024, a través del cual se efectúa nombramiento del Sr. Alcalde de la comuna de Villa Alegre don ARTURO PALMA VILCHES.
12. Que, resulta necesario contar con un reglamento que regule los procedimientos internos de gestión de las cuentas institucionales y herramientas de colaboración digital de la Municipalidad de Villa Alegre, en su calidad de activos de información, de manera coherente con el proceso de transformación digital del Estado, a fin de normar objetivamente la forma de obtención y eliminación de cuentas institucionales, así como el debido respaldo y conservación de la información asociada durante ciertos plazos mínimos, junto con los procedimientos para acceder a ella, respetando las normas técnicas de seguridad de la información y ciberseguridad.
13. Por tanto, con base en la interpretación armónica del visto y considerando expuesto.

RESUELVO:

APRUÉBASE el presente Reglamento de Cuentas de Correo Electrónico Institucional de la Municipalidad de Villa Alegre.



TÍTULO I DISPOSICIONES GENERALES

Artículo 1. Objeto del reglamento.

El presente reglamento tiene por objeto regular los procedimientos internos relativos a la asignación, uso, administración, respaldo, conservación, acceso excepcional y eliminación de las cuentas institucionales y herramientas de colaboración digital de la Municipalidad, de conformidad con las normas sobre seguridad de la información y ciberseguridad.

Artículo 2. Cuentas institucionales.

Las cuentas institucionales consisten en un nombre de usuario y una contraseña que pueden usarse para acceder a distintos productos, incluyendo una casilla de correo electrónico institucional y herramientas de colaboración digital como el almacenamiento en la nube, ofimática en línea, videoconferencias, gestión de calendario, entre otras herramientas tecnológicas que, siendo propiedad de la Municipalidad, son proporcionadas por esta a sus empleados(as) como apoyo al desarrollo de las labores administrativas.

Artículo 3. Ámbito de aplicación.

El presente reglamento deberá aplicarse a la gestión de cuentas institucionales de las unidades municipales de la Municipalidad de Villa Alegre. La gestión de cuentas y correos institucionales del Departamento de Salud Municipal se regirá por sus propios procedimientos. Sin embargo, aquellos deberán respetar las normas de seguridad de la información, tanto de aplicabilidad general como de carácter interno, procurando realizar los respaldos necesarios en resguardo de las obligaciones legales de la municipalidad y de la continuidad operativa del servicio, todo ello con pleno respeto y protección de los datos e información personal que pudieren verse involucrados.

Artículo 4. Administración de las cuentas institucionales.

La administración de las cuentas institucionales de la Municipalidad de Villa Alegre se encontrará bajo dirección del o la Coordinador(a) de Transformación Digital (TD), que tendrá a su cargo la asignación de tales cuentas, su suspensión o eliminación, el respaldo de la información contenida en ellas, y la gestión de solicitudes de acceso a tales respaldos.

TÍTULO II PROCEDIMIENTOS DE GESTIÓN DE CUENTAS INSTITUCIONALES PÁRRAFO 1 ASIGNACIÓN, SUSPENSIÓN Y ELIMINACIÓN DE CUENTAS

Artículo 5. Procedimiento de asignación de una cuenta institucional.

Para efectos de la creación de un usuario de cuenta institucional y su asignación a un(a) funcionario(a) o servidor(a) municipal que lo requiera para el desempeño de su labor administrativa, se deberá seguir el siguiente procedimiento:



- a) La jefatura directa solicitará la asignación de una cuenta institucional al o la subalterno(a) que lo requiera, mediante un correo electrónico dirigido al o la Coordinador(a) de TD, donde deberán expresarse las funciones concretas que debe cumplir dicho(a) empleado(a) y que justifican la necesidad de una cuenta institucional.
- b) Recibida una solicitud, el o la Coordinador(a) de TD verificará el cumplimiento del requisito de justificación y, de ser procedente, ordenará la asignación de la cuenta institucional.
- c) En la creación del nombre de usuario de una cuenta institucional, deberá observarse el siguiente patrón: Primera letra del nombre, más el primer apellido de la persona respectiva, seguido del dominio @villalegre.cl. Por ejemplo, para una funcionaria llamada Rosa Pérez, el nombre de usuario sería "rperez@villalegre.cl".
En el evento de que se encuentre ocupada la dirección resultante luego de aplicar dicha nomenclatura, el o la encargado(a) de crear las direcciones de correo electrónico deberá utilizar otras combinaciones provenientes de los nombres y apellidos del o la empleado(a) respectivo(a), procurando que el resultado no sea irrisorio o denigrante.
- d) Creada la cuenta institucional, el o la funcionario(a) de TD respectivo deberá comunicar dicha circunstancia por correo electrónico dirigido a la jefatura que haya solicitado la gestión, señalando:
 - Nombre de usuario (dirección de correo electrónico) y credenciales de acceso.
 - Nombre del o la funcionario(a) o servidor(a) a quien se asignan.
 - Instrucciones para modificar la clave por primera vez y para recuperación de la cuenta en caso de olvido o pérdida.

Artículo 6. Disponibilidad de cuentas institucionales.

La Municipalidad dispondrá de cuentas institucionales para sus funcionarios(as) y servidores(as) municipales en la medida de lo posible según disponibilidad presupuestaria; debiendo priorizarse su asignación a quienes efectivamente requieran esta herramienta para la ejecución correcta, eficiente y eficaz de sus funciones administrativas.

El o la administrador(a) de las cuentas institucionales, deberá realizar revisiones periódicas para determinar la existencia de cuentas institucionales en desuso, a fin de proceder a su reutilización en funciones donde efectivamente se requieran.

En el evento de que existan dos o más solicitudes de asignación de una cuenta institucional, sin que exista stock suficiente para cubrirlas todas, y siempre que no sea posible la contratación de un mayor número de cuentas, el o la Coordinador(a) de TD deberá ponderar la situación, considerando la justificación entregada en cada solicitud y su alineamiento con los fines y funciones de la municipalidad y de la unidad respectiva. Con base en aquello, ordenará la asignación de la o las cuentas disponibles de la manera que resulte más conveniente para dar continuidad y eficacia al servicio.

Artículo 7. Suspensión de una cuenta institucional.



La suspensión de una cuenta se verificará en aquellos casos en que un correo electrónico institucional se encuentre en desuso, porque el o la empleado(a) municipal ha sido suspendido(a) de su cargo en el contexto de un procedimiento disciplinario, porque se encuentra haciendo uso de una licencia médica cuya duración exceda de 2 meses, o por cualquier otro motivo que implique la inactividad de la cuenta por un período superior al mismo plazo.

Cuando se produzca una suspensión en el contexto de un procedimiento disciplinario, la jefatura directa del o la funcionario(a) suspendido(a) deberá dar aviso inmediato o más tardar dentro de 2 días, al o la Coordinador(a) de TD, mediante correo electrónico, del hecho de haberse configurado la hipótesis antedicha, para que proceda a realizarse la suspensión de la cuenta institucional, previo respaldo de su contenido.

Esta suspensión se extenderá por todo el tiempo que persista la causal de inactividad temporal del o la funcionario(a) o servidor(a) municipal.

Artículo 8. Eliminación de una cuenta institucional.

Una cuenta institucional deberá ser eliminada cuando se produzca la desvinculación del o la funcionario(a) o servidor(a) municipal al que se encontraba asignada; cuando por una modificación de funciones se elimine la necesidad de utilización de una cuenta institucional para efectos del eficaz y eficiente cumplimiento de su labor administrativa, o por cualquier otra causa, la cuenta deje de ser utilizada definitivamente.

Para estos efectos, la jefatura directa tendrá el deber de informar al o la Coordinador(a) de TD, dentro del plazo máximo de 2 días desde que se produzca la desvinculación o el cambio de funciones, solicitando dar de baja la respectiva cuenta institucional.

PÁRRAFO 2

RESPALDO, CONSERVACIÓN Y ACCESO A INFORMACIÓN DE CUENTAS INSTITUCIONALES

Artículo 9. Naturaleza y relevancia de las cuentas institucionales.

Las cuentas institucionales de correo electrónico y las herramientas digitales asociadas a ellas constituyen bienes de propiedad de la Municipalidad de Villa Alegre y forman parte de sus activos de información.

El contenido generado, recibido o almacenado a través de dichas cuentas constituye información relevante para la gestión municipal, el control interno y externo, la transparencia, la continuidad operativa y, eventualmente, para la sustanciación de procedimientos administrativos, disciplinarios, judiciales u otros de similar naturaleza; motivo por el cual debe ser respaldada y conservada.

Artículo 10. Respaldo de las cuentas institucionales.

La Municipalidad deberá asegurar el respaldo adecuado, íntegro y oportuno de la información contenida en las cuentas institucionales, incluyendo, a lo menos:



- a) Los mensajes de correo electrónico enviados y recibidos;
- b) Los archivos adjuntos a dichos mensajes; y
- c) Los documentos, archivos y demás contenidos producidos y/o almacenados en las herramientas digitales asociadas a la cuenta institucional.

El respaldo deberá efectuarse de forma previa a la suspensión o eliminación de una cuenta institucional, cualquiera sea la causa que la motive, incluyendo el término de funciones del o la funcionario(a) o servidor(a) municipal.

La administración y ejecución de los respaldos corresponderá a la unidad que se encuentre designada para la Coordinación de Transformación Digital, y deberá realizarse por quien tenga a su cargo la gestión técnica de las cuentas institucionales.

La información respaldada deberá almacenarse exclusivamente en infraestructura, sistemas o soportes de propiedad o control institucional, quedando expresamente prohibido su almacenamiento en dispositivos, cuentas o servicios de carácter personal de funcionarios(as) o terceros.

Artículo 11. Conservación de la información respaldada.

La información respaldada de las cuentas institucionales deberá conservarse por un plazo mínimo de cinco años, contado desde la fecha de suspensión o eliminación de la cuenta respectiva. Para estos efectos, la información deberá constar en formatos que aseguren su preservación digital a mediano plazo, de manera que sea legible y utilizable durante el tiempo reglamentario.

Durante dicho período, el o la encargado(a) de la gestión técnica de los respaldos deberá emplear el debido cuidado y diligencia para garantizar la integridad, disponibilidad, confidencialidad y preservación de la información, evitando su pérdida, alteración, destrucción o acceso no autorizado.

Para estos efectos, deberán observarse, a lo menos, las siguientes medidas mínimas:

- a) Mantener registros actualizados de la realización de copias de seguridad, indicando al menos: Fecha de su realización, cuenta institucional y nombre del usuario(a) a que corresponde, motivo del respaldo (suspensión o eliminación de la cuenta), soporte de almacenamiento y nombre del responsable.
- b) Mantener medidas específicas de recuperación frente a incidentes de seguridad u otros eventos que comprometan la disponibilidad de la información, llevando un registro específico de la realización de tales procedimientos de restauración, que indique, al menos: la fecha del incidente y de la recuperación, las cuentas afectadas, la causa de la pérdida o deterioro (tipo de incidente), el procedimiento utilizado, la estimación de la cantidad de información perdida o el período temporal comprendido, y la identificación del responsable del procedimiento de recuperación.
- c) Almacenar las copias de seguridad en ubicaciones seguras, manteniendo, en lo posible, copias en línea y fuera de línea, de manera que se reduzca el



riesgo de pérdida de información ante fallas técnicas, desastres, incidentes de seguridad u otros eventos similares.

- d) Realizar pruebas periódicas de restauración, a fin de verificar la confiabilidad de los respaldos y la capacidad efectiva de recuperación de la información, sin comprometer los datos originales.
- e) Implementar medidas de protección adicionales, tales como cifrado u otras, cuando la naturaleza de la información respaldada así lo requiera, especialmente si contiene datos personales o sensibles.

Artículo 12. Resguardo de datos personales y acceso restringido.

El almacenamiento y conservación del contenido de las cuentas institucionales deberá realizarse resguardando adecuadamente los datos personales y/o sensibles que pudieren estar contenidos en tales archivos, de conformidad con la Constitución y las leyes vigentes, especialmente la Ley N° 19.628 y sus modificaciones.

El acceso a la información respaldada quedará restringido, para efectos de su conservación y administración, exclusivamente a la unidad que tenga a su cargo la Transformación Digital, sin perjuicio de las excepciones reguladas en los artículos siguientes.

Los(as) usuarios(as) de las cuentas institucionales deberán procurar abstenerse de enviar o almacenar información propia del ámbito de su vida privada, datos personales y datos sensibles a través de esta vía; a fin de mantener los respaldos de información institucional libres de todo contenido ajeno a la función pública, y permitir con ello una mayor eficiencia en la entrega de información solicitada a través de los mecanismos de la Ley 20.285, que exige resguardar la información personal.

Artículo 13. Entrega excepcional de información respaldada.

Excepcionalmente, el o la Coordinador(a) de TD podrá autorizar la entrega total o parcial de la información asociada a una cuenta institucional, activa o eliminada, cuando exista una orden administrativa o judicial expresa que así lo disponga, y dicha información resulte necesaria para una investigación, fiscalización o procedimiento destinado a determinar la responsabilidad de un(a) funcionario(a), servidor(a) o autoridad municipal.

También podrá ordenarse la entrega de la información contenida en cuentas institucionales cuando sea requerido mediante una solicitud de acceso a la información pública de la Ley de Transparencia, pero deberán censurarse previamente todos los datos personales o sensibles pertenecientes a personas naturales.

Cuando la entrega de información se realice en virtud de una orden administrativa o judicial, esta se efectuará sin censura de los datos personales que pudiere contener; sin perjuicio de la observancia de la normativa general o especial sobre protección de tales datos, por parte del o la receptor(a) de información.



Las comunicaciones, documentos y archivos de cualquier tipo obtenidos a través de los procedimientos regulados en el presente reglamento, podrán ser utilizados válidamente como medios de prueba en procedimientos disciplinarios, judiciales o de cualquier otra índole, conforme a la legislación aplicable.

Artículo 14. Procedimiento para el acceso interno a información de cuentas institucionales.

En el marco de los procedimientos disciplinarios internos de la Municipalidad, el o la fiscal o investigador podrá solicitar acceso a información contenida en una cuenta institucional, especialmente a los correos electrónicos, cuando ello resulte necesario para el éxito de la investigación.

Para tal efecto, deberá presentar una solicitud mediante correo electrónico dirigido al o la Coordinador(a) de TD, donde deberá acompañar la resolución del respectivo procedimiento disciplinario mediante la cual se ordena la entrega de la información contenida en una cuenta determinada, individualizando claramente al funcionario(a) o servidor(a) respecto de quien se requiere, y el período de tiempo que comprende la solicitud.

Verificado el cumplimiento de los requisitos, el o la Coordinador(a) de TD dispondrá la entrega de la información solicitada dentro del plazo de tres días hábiles, o del plazo menor que establezca la resolución respectiva.

Artículo 15. Procedimiento para el acceso externo a información de cuentas institucionales.

La información asociada a cuentas institucionales podrá ser requerida por organismos o autoridades externas a la Municipalidad en el marco de investigaciones, fiscalizaciones o procedimientos de su competencia, tales como investigaciones policiales instruidas por el Ministerio Público, fiscalizaciones de la Contraloría General de la República o procedimientos judiciales.

Recibida una solicitud de este tipo, será derivada a la unidad de Transformación Digital, donde el o la Coordinador(a) de TD deberá verificar:

- a) Que la solicitud se funde en una orden judicial o administrativa expresa, emitida por autoridad competente;
- b) Que la orden se presente por un medio que permita razonablemente constatar su origen y autenticidad formal. Por ejemplo, verificación de la firma electrónica avanzada, o documento en papel con firmas y timbres; y
- c) Que el o la funcionario(a) externo que la presenta acredite su identidad y pertenencia al organismo emisor de la orden.

Cumplidos dichos requisitos, el o la Coordinador(a) de TD deberá dejar registro y copia digitalizada de la orden recibida y dispondrá la entrega de la información solicitada dentro del plazo de tres días hábiles, o dentro del plazo menor que expresamente señale la orden respectiva.



La entrega de la información deberá limitarse estrictamente al alcance y período indicado en la orden.

Artículo 16. Registro de entrega de información contenida en cuentas institucionales.

El o la Coordinador(a) de TD deberá llevar un registro de entrega de información contenida en cuentas institucionales, donde deberá dejar constancia de los siguientes elementos:

- a) Fecha de la solicitud de acceso y fecha de la entrega efectiva de la información.
- b) Identificación de la cuenta institucional: Dirección de correo electrónico, nombre y cargo del usuario(a) de la cuenta.
- c) Período temporal: Período de tiempo al que corresponde la información entregada.
- d) Causa de la entrega: Señalar si fue por requerimiento interno, externo, o por una solicitud de acceso a la información de la Ley de Transparencia.
- e) Responsable de la entrega.

PÁRRAFO 3 USO DE LAS CUENTAS INSTITUCIONALES

Artículo 17. Responsabilidad del usuario(a).

Todo(a) usuario(a) de una cuenta institucional será responsable del uso adecuado de la misma, de la confidencialidad de sus credenciales de acceso y de las acciones realizadas bajo su identidad digital, debiendo dar cumplimiento estricto a este reglamento y a las demás normas internas sobre seguridad de la información.

Artículo 18. Dispositivos de acceso a cuentas institucionales.

El acceso a las cuentas institucionales y a la información municipal deberá realizarse, preferentemente, desde dispositivos tecnológicos proporcionados por la Municipalidad.

Excepcionalmente, y cuando razones de servicio así lo justifiquen, dicho acceso podrá efectuarse desde dispositivos personales del o la usuario(a). En estos casos, deberá adoptar las medidas razonables de cuidado necesarias para resguardar la confidencialidad, integridad y disponibilidad de la información institucional a la que acceda, siendo responsable del uso que realice de su cuenta institucional desde tales dispositivos.

Artículo 19. Uso de las cuentas institucionales.

Las cuentas institucionales solo podrán ser utilizadas para el apoyo de las labores propias de los(as) funcionarios(as) y que se encuentren directamente relacionadas con los fines de la Municipalidad.

Los correos electrónicos institucionales serán el medio de comunicación oficial entre los y las funcionarios(as) y servidores(as) municipales, con otros órganos públicos



o privados, y con la comunidad en general; sin perjuicio del uso de los respectivos anexos telefónicos, de la procedencia de envío o recepción mediante la plataforma de comunicaciones oficiales del Estado -DocDigital- y de las notificaciones que corresponda practicar en procedimientos administrativos.

Toda comunicación por correo electrónico deberá indicar un asunto explicativo de su contenido; y cuando se trate de materias urgentes o sujetas a plazo, dicha circunstancia deberá explicitarse en el mismo, a fin de facilitar su identificación.

Los(as) funcionarios(as) y servidores(as) municipales deberán revisar diariamente su casilla de correo electrónico institucional durante su jornada laboral, o si no la tienen, entre las 08:00 y las 17:30 horas, dando respuesta oportuna y respetuosa a las comunicaciones recibidas. Si se tratare de cuestiones urgentes o de plazo, deberá responderse dentro del mismo día hábil, o a más tardar el día siguiente, si se envió fuera del horario ya indicado.

Artículo 20. Uso de las herramientas de colaboración digital.

Las herramientas de colaboración digital asociadas a una cuenta institucional -como Google Drive, Meet, Calendario, Formularios, Documentos, Hojas de cálculo, entre otros- deberán ser utilizadas como medio oficial para el trabajo colaborativo y coordinado entre las unidades y funcionarios(as), privilegiando la edición en tiempo real, cada vez que ello sea conveniente para la eficiencia de la tarea en cuestión.

En consecuencia, deberá evitarse la práctica de enviar archivos descargables mediante correo electrónico o de imprimir tales documentos para su entrega presencial, salvo que sea estrictamente necesario.

La nube de almacenamiento -Google drive- solo podrá ser utilizada para guardar archivos relacionados con las funciones que, dentro de la Municipalidad, corresponda desarrollar al o la titular de la cuenta.

Artículo 21. Conductas prohibidas

Se prohíbe a todo(a) usuario(a) utilizar las cuentas institucionales para fines ilícitos, contrarios al orden público, a los fines de la Municipalidad o a la probidad administrativa. En particular, se prohíben las siguientes conductas:

- a) Uso indebido de recursos institucionales: Utilizar las cuentas para fines personales, comerciales o de lucro; enviar cadenas, spam o comunicaciones ajenas a la función municipal; registrarse en servicios personales; o almacenar contenidos recreativos o archivos de gran tamaño que no sean necesarios para el trabajo.

Entiéndase comprendida dentro de esta prohibición el uso de correo electrónico para mantener conversaciones de carácter personal, transmitir información sensible ajena a la labor administrativa; el uso de la nube de almacenamiento para cargar fotografías, videos, documentos, u otros archivos del ámbito de la vida privada del o la titular de la cuenta; o cualquier otra conducta que sea ajena al desarrollo de labores institucionales.



- b) Difusión o almacenamiento de contenido inapropiado: Enviar, recibir o almacenar contenidos ofensivos, discriminatorios, hostigadores, pornográficos, político-partidistas, o cualquier otro incompatible con la función pública.
- c) Infracciones a la seguridad de la información: Compartir credenciales de acceso; habilitar reenvíos automáticos a cuentas personales; intentar acceder sin autorización a sistemas o datos; o divulgar información interna, confidencial o reservada sin autorización, almacenar información institucional en dispositivos personales sin observar las condiciones mínimas de seguridad.
- d) Infracciones legales y de propiedad intelectual: Utilizar las cuentas para cometer delitos o ilícitos civiles; vulnerar derechos de autor u otros derechos de propiedad intelectual; o suplantar identidades o alterar la información del remitente.

Se entenderán igualmente prohibidas cualesquiera otras conductas análogas que comprometan la seguridad de la información o el correcto funcionamiento del servicio.

Artículo 22. Gestión de incidentes de seguridad de la información.

Todo(a) usuario(a) que detecte o sospeche un uso indebido, acceso no autorizado, pérdida de confidencialidad o compromiso de su cuenta institucional, deberá informar inmediatamente y por la vía más expedita al o la Coordinador(a) de TD, a fin de adoptar las medidas de contención, análisis y recuperación que correspondan.

ANÓTESE, PUBLÍQUESE Y ARCHÍVESE

CLAUDIA BERRÍOS NILO

ARTURO PALMA VILCHES

SECRETARIA MUNICIPAL

ALCALDE

Distribución:

- Todas las Direcciones Municipales.
- Servicios Traspasados.
- Oficina de Personal y Remuneraciones.
- Secretaría Municipal.
- Oficina de Partes.



ANEXO 1: EJEMPLO REGISTRO DE COPIAS DE SEGURIDAD DE CUENTAS INSTITUCIONALES

REGISTRO DE COPIAS DE SEGURIDAD DE CUENTAS INSTITUCIONALES						
FECHA DEL RESPALDO	CUENTA INSTITUCIONAL	NOMBRE DEL/LA USUARIO/A	CARO DEL/LA USUARIO/A	MOTIVO DEL RESPALDO	SOPORTE DE ALMACENAMIENTO	RESPONSABLE DEL RESPALDO
05-03-2026	ejemplo@villalegre.cl	NOMBRE APELLIDO APELLIDO	JEFE/A DE FINANZAS	Término de la prestación de servicios	Drive de cuenta de respaldo	Desarrollador TD

ANEXO 2: EJEMPLO REGISTRO DE PROCEDIMIENTOS DE RECUPERACIÓN DE INFORMACIÓN

REGISTRO DE PROCEDIMIENTOS DE RECUPERACIÓN DE INFORMACIÓN							
FECHA DEL INCIDENTE	FECHA DE RESTAURACIÓN	TIPO DE INCIDENTE	CUENTA INSTITUCIONAL	PERÍODO O INFORMACIÓN AFECTADA	PROCEDIMIENTO DE RECUPERACIÓN	RESPONSABLE	RESULTADO
03-01-2026	04-01-2026	Eliminación accidental de correos por <i>phishing</i> .	ejemplo@villalegre.cl	15-12-2025 AL 31-12-2025	Respaldo institucional	DESARROLLADOR TD	Recuperación parcial (indicar qué se perdió)



ANEXO 3: EJEMPLO REGISTRO DE ENTREGA DE INFORMACIÓN DE RESPALDOS DE CUENTAS INSTITUCIONALES

REGISTRO DE ENTREGA DE INFORMACIÓN DE RESPALDOS DE CUENTAS INSTITUCIONALES					
FECHA SOLICITUI	FECHA ENTREGA	CUENTA INSTITUCION	PERÍODO TEMPORAL ENTREGADO	CAUSA DE LA ENTREGA	RESPONSABLE DE LA ENTREGA
04-01-2026	05-01-2026	ejemplo@villalegre.cl	01-01-2023 - 31-12-2025	Procedimiento disciplinario DAE N°X	COORDINADORA TD