Subd. de Gestión y Desarrollo de Personas
Depto. Planificación y Gestión de la Dotación

RESOLUCIÓN EXENTA N° 1756

PUNTA ARENAS, 01 de abril de 2025

VISTOS : Resolución N°36/19.12.2024 de la Contraloría General de la República, que fija las normas sobre exención del trámite de toma de razón; D.S. N° 140/2004 Reglamento Orgánico de los Servicios de Salud; D.F.L. N° 01 de 2005 que fija Texto Refundido, Coordinado y Sistematizado del Decreto Ley 2763/79 y Leyes 18.933 y 18.469; Resolución Exenta N° 123/06.01.2025, que Establece la nueva Estructura Orgánica de la Dirección del Servicio de Salud Magallanes; Resolución Exenta N° 124/06.01.2024 que complementa Resolución Exenta N° 123/06.01.2025 que establece la nueva Estructura Orgánica de la Dirección del Servicio de Salud Magallanes, con descripción de sus funcionalidades de sus respectivas Subdirecciones, Departamentos, Unidades y Asesorías respectivas; y en uso de las facultades que me confiere el Decreto Exento N° 22 del 10 de abril de 2023 del Ministerio de Salud que establece orden de subrogancia de la Dirección del Servicio de Salud Magallanes; y

CONSIDERANDO:

1) Que, a través de Memorándum N° 03 del 25 de febrero de 2025 del Jefe del Departamento de Tecnología de la Información y la comunicación (TIC), emite a la Subdirectora (S) de la Subdirección de Gestión de Personas del Servicio de Salud Magallanes, la aprobación y actualización de la "Política de Seguridad de Recursos Humanos" documento revisado y ajustado con el propósito de reforzar los lineamientos en materia de seguridad y gestión del personal dentro de nuestra organización.

2) Que, en mérito de lo expuesto, dicto la siguiente:

R E S O L U C I Ó N :

1. **APRUÉBESE**, a contar de la fecha de la presente resolución, **"POLÍTICA DE SEGURIDAD DE RECURSOS HUMANOS"** del Departamento de Tecnología de la Información y la Comunicación (TIC) perteneciente a la Dirección del Servicio de Salud Magallanes.

2. **DÉJESE PRESENTE,** que esta actualización tiene como objetivo garantizar la protección de la información y los recursos institucionales mediante la correcta gestión de los procesos de selección, contratación, permanencia y desvinculación del personal, promoviendo el cumplimiento de las normativas vigentes y buenas prácticas en materia d seguridad.

Política de Seguridad de Recursos Humanos

Preparado por:	Daniel Barría Águila		
Revisado por	Jefe Departamento TIC del Servicio de Salud Magallanes		
Revisado por			
Aprobado por:	Ricardo Ignacio Toledo Barría	**Fecha de Aprobación:**	24-0-2025
		Fecha de Publicación:	
		Vigente desde:	
		Vigente Hasta:	Nueva Revisión

Control de versiones

Versión	Fecha de Vigencia	Aprobado por	Fecha publicación	Firma	Comentario
2.0	10-07-2018	Pablo Cona Romero	11-10-2018		Revisión Crítica de la 1era versión.
2.1	24-02-2025	Ricardo Toledo Barría			

(*) La presente versión substituye completamente a todas las precedentes, de manera que éste sea el único documento válido de entre todos los de la serie.

Cualquier pregunta o comentario sobre esta Política de Seguridad de Información dirigirla al Departamento TIC.

Índice

INTRODUCCIÓN

La gestión de la seguridad de la información, al igual que la mayoría de los ámbitos de la gestión en la DSSM, depende principalmente de las personas que componen la Organización. La información sólo tiene sentido cuando es utilizada por las personas y son estas, **quienes**, en último término, deben gestionar adecuadamente este importante recurso. Por tanto, no se puede proteger adecuadamente la información sin una correcta gestión de los Recursos Humanos. Pero sin duda, una de las áreas que más importancia tiene en la seguridad de la información es el departamento encargado de gestionar los Recursos Humanos.

Aspectos como la formación de los empleados, la captación y selección de nuevos miembros, la gestión de empleados que abandonan la Organización o la implementación de la normativa interna, son fundamentales en el tema que nos ocupa.

SEGURIDAD DE RECURSOS HUMANOS

[illegible]

[illegible]

Los funcionarios de la DSSM, tanto contrata, planta como personal a honorarios, tienen la responsabilidad de clasificar la información que le ha sido asignada, de acuerdo al esquema de clasificación definido según la Política de Clasificación y Manejo de la Información.

Cada propietario de la información debe autorizar la divulgación de información, considerando los controles adecuados.

[illegible]

Las principales responsabilidades del Comité de Seguridad de la Información son:

- Unificación de los criterios de clasificación de la información en la organización.
- Gestionar unidades en código de confidencialidad (quién puede generar información confidencial).
- Detectar comportamientos que se salgan de la norma sin tener que esperar a los ciclos de auditorías o inspecciones.
- Interlocutor natural con Auditoría Interna y Control Interno – Riesgo Operacional.
- Elaborar, junto con Cumplimiento Normativo, el código de conducta de sistemas de información de la DSSM.

Roles y responsabilidades Departamento de Tecnología de la información y la comunicación

- Actuar en forma coordinada con el Departamento de RRHH para la oportuna creación, modificación y eliminación de Cuentas de Usuario asociadas al personal y, asimismo, velar por el adecuado registro de la información asociada dichas cuentas.
- Establecer mecanismos de información para permitir a los usuarios supervisar la actividad normal de su cuenta, así como alertarlos oportunamente sobre actividades inusuales.

Roles y responsabilidades de Departamentos/Encargados

- Solicitar formalmente al Departamento de Tecnologías de información, cada vez que sea necesario, realizar algún cambio en el perfil de privilegios de acceso para una Cuenta de Usuario de su dependencia.
- Revisar y confirmar periódicamente los derechos de acceso. Se debe llevar a cabo la comparación periódica entre los recursos y los registros de las cuentas para reducir el riesgo de errores, fraudes, alteración no autorizada o accidental.

Roles y responsabilidades encargado de seguridad de la información

- Autorizar la asignación de privilegios de administración a cuentas que no pertenecen al grupo de administradores.
- Autorizar la asignación de Código-Usuario y Contraseñas para personal externo a la institución cuando corresponda.

- Actuar en forma coordinada con el Departamento de Tecnologías de Información comunicación, para notificar de las altas, bajas y traslados de miembros del personal de la DSSM, de modo tal que se puedan mantener actualizadas las correspondientes cuentas de usuario.
- Este departamento deberá ser la Fuente oficial que certifique los datos de identidad de todo el personal de la institución, así como la información relativa a su área de trabajo, cargo, oficina y anexo telefónico asignado.

SEGURIDAD DE RECURSOS HUMANOS EN EL TRABAJO

La seguridad de los recursos humanos dentro de la organización, debe considerar como recurso humano al personal interno, temporal o partes externas en el aseguramiento de las responsabilidades que son asignadas a cada uno, asociadas con sus respectivos roles, para reducir el riesgo de robo, fraude o uso inadecuado de las instalaciones.

Todo el recurso humano que hace parte de la Organización debe estar consciente de las amenazas y vulnerabilidades relacionadas con la seguridad de la información y sus responsabilidades y deberes en el apoyo que deben brindar a la política de seguridad de la organización establecida para la reducción del riesgo de error humano.

A.7 SEGURIDAD ANTES DE LA CONTRATACIÓN DEL EMPLEO

Objetivo:

Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean idóneos para los roles para los cuales son considerados; y reducir el riesgo de robo, fraude y mal uso de los medios. Las responsabilidades de seguridad deben ser tratadas antes del empleo en descripciones de trabajo adecuadas y en los términos y condiciones del empleo.

Reclutamiento

A cada nuevo empleado, la DSSM le asigna una serie de tareas y responsabilidades, y proporciona los medios materiales y la información necesaria para que pueda llevarlas a cabo. Debe existir un procedimiento de reclutamiento que tenga en cuenta los siguientes aspectos relativos a la seguridad:

Definición del puesto: Para cada nueva vacante se debe definir la criticidad del puesto a cubrir según su responsabilidad y la información que maneja. Algunos puestos críticos pueden ser directivos, personal de seguridad, personal de contabilidad, etc.

Investigación de antecedentes:

Se deben realizar en conjunto con el área de Recursos Humanos de la DSSM una valoración del proceso de verificación de antecedentes legales, comportamientos éticos y otros antecedentes de relevancia esto se debe aplicar al personal candidato ya sea de planta, contrata o personal honorario que ingrese a la Dirección Servicio Salud Magallanes, teniendo en cuenta el tipo y clasificación de la información a la que tendría acceso en sus respectivos cargos y responsabilidades.

Se debe tener en cuenta que no todos los procesos de contratación en la organización deben ser manejados de igual forma, cada rol y sus responsabilidades debe tener un manejo diferente con relación a la verificación de antecedentes, procedencia, formación, conocimientos, etc.

Contrato: El contrato laboral debe incluir los correspondientes acuerdos de confidencialidad, propiedad intelectual y protección de datos.

Comienzo: Durante los primeros días de trabajo, es recomendable que el empleado:

- Asista a unas sesiones de formación donde se le introduzca en la normativa interna y de seguridad de la Dirección Servicio Salud Magallanes. De este modo todo empleado conoce sus obligaciones de seguridad tales como la protección de sus claves de acceso, uso adecuado del email e internet, clasificación de la información, etc.
- Reciba un manual de normativa interna y firme un compromiso de cumplimiento del mismo. Este trámite establece formalmente las normas internas y garantiza que el empleado conoce la normativa existente.

Accesos: Los accesos a la información y sistemas informáticos deben ser solicitados siempre por el responsable directo del empleado al departamento TIC. Dichos accesos deben ser siempre justificables por la labor que se va a realizar, y en caso de ser privilegiados, el Departamento de Seguridad debe aprobar su concesión.

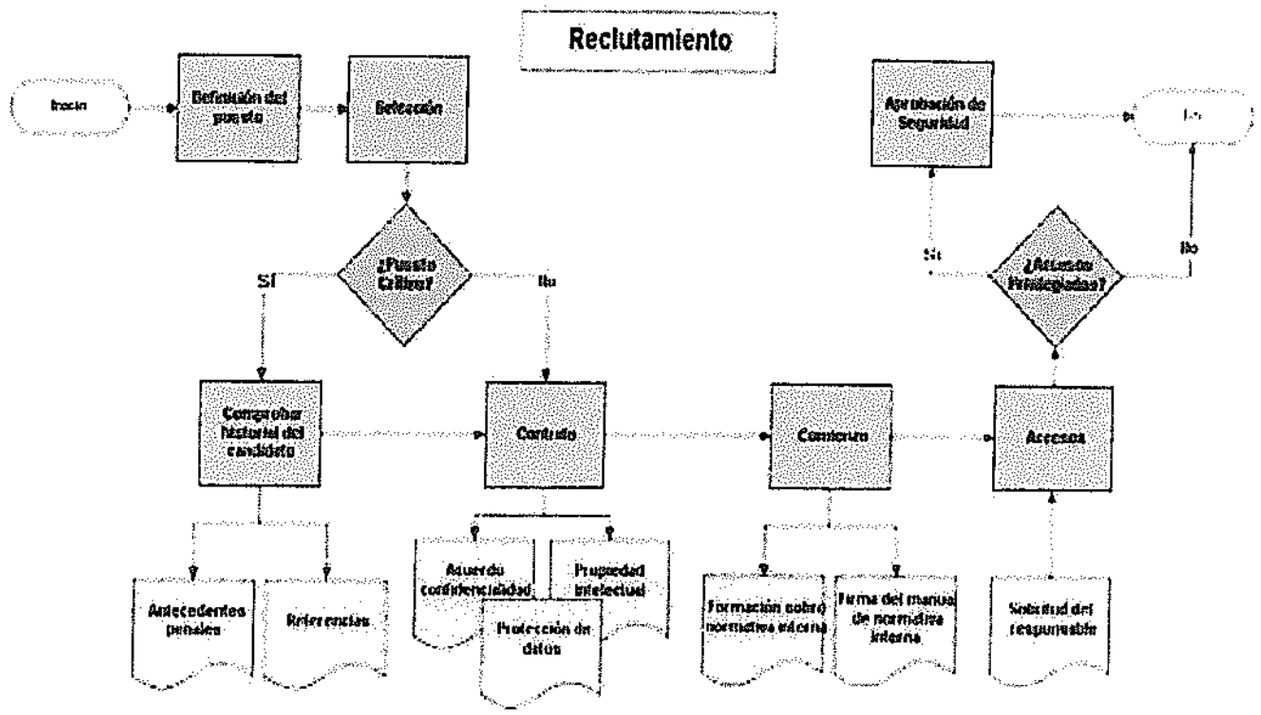

Fig. 1 Reclutamiento de personal

8. SEGURIDAD DURANTE LA CONTRATACIÓN

Objetivo: Asegurar que los usuarios empleados de la DSSM, de planta, contrata o personal honorario y terceras personas estén al tanto de las amenazas e inquietudes de la seguridad de la información, sus responsabilidades y obligaciones, y estén equipadas para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir el riesgo de error humano.

Se deben asegurar en la contratación del personal de la DSSM, acuerdos de confidencialidad de la información que se manejarán durante el tiempo que labore dentro de la organización y una vez finalizado el contrato.

Debe quedar documentado en acuerdos de confidencialidad, materiales de concientización, contratos de empleo entre el empleado y la organización la responsabilidad de los trabajadores relacionada con la protección de la información manejada por la DSSM.

Anualmente se debe considerar la posibilidad de revisar en conjunto con los empleados los términos, acuerdos y condiciones expuestas en los contratos laborales, para garantizar el compromiso que adquirieron con relación a la seguridad de la información con la organización.

Responsabilidades de la Jefatura: Debe requerir a los usuarios empleados, contratistas y terceras personas que apliquen la seguridad en concordancia con políticas y procedimientos bien establecidos por la DSSM.

Conocimiento, educación y capacitación en seguridad de la información
Todos los empleados de la DSSM y, cuando sea relevante, y terceras personas deben recibir una adecuada capacitación en seguridad y actualizaciones regulares sobre las políticas y procedimientos organizacionales conforme sea relevante para su función laboral.

6. SEGURIDAD EN LA FINALIZACIÓN O CAMBIO DE EMPLEO

Objetivo: Asegurar que los usuarios empleados de la DSSM, de planta, contrata o personal honorario y terceras personas salgan de la organización o cambien de empleo de una manera ordenada. Se deben establecer las responsabilidades para asegurar que la salida de la organización del usuario empleado, contratista o tercera persona sea manejada y se complete la devolución de todo el equipo y se eliminen todos los derechos de acceso.

Cuando los empleados finalizan sus contratos laborales con la organización o se retiran de ésta, se deben tener en cuenta varias actividades que se deben realizar para garantizar la gestión apropiada de activos de la organización que tenía a su cargo.

Devolución de los activos

Al finalizar un contrato de empleo por parte de la DSSM, a raíz del cual se utilizan diversos equipos, software o información en formato electrónico o papel, el usuario debe devolver todos esos activos de información al Jefe departamento de Informática y Jefe departamento de finanzas según corresponda.

Retiro de los derechos de acceso

Los derechos de acceso de todos los usuarios empleados de la DSSM, de planta, contrata o personal honorario y terceras personas a la información y los medios de procesamiento de información deben ser retirados a la terminación de su empleo, contrato o acuerdo, o deben ser reajustados de acuerdo al cambio.

Proceso disciplinario: Los empleados de la DSSM que han cometido un incumplimiento de la seguridad de la información deberán ser parte de un proceso disciplinario cargo del Comité de Seguridad de la Información

Subd. de Gestión y Desarrollo de Personas
Depto. Planificación y Gestión de la Dotación

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE.

SERVICIO DE SALUD MAGALLANES
DIRECTOR
XII REGIÓN

RICARDO CONTRERAS FAÚNDEZ
DIRECTOR (S)
SERVICIO DE SALUD MAGALLANES

V°B° SDGDP

RCF/FRG/FQM/voo
Nº 1048

DISTRIBUCIÓN:
-Dirección del Servicio de Salud Magallanes.
-Subdirección Gestión y Desarrollo de las Personas.
-Depto. Planificación y Gestión de la Dotación.
-TIC
-Interesado/a
-Oficina de Partes.