

**REF: LLÁMESE A CONCURSO PÚBLICO PARA
PROVEER EL CARGO DE JEFE(A) DE
DEPARTAMENTO DE CIBERSEGURIDAD.**

VISTOS:

El DL N°3.538 de 1980, que crea la Comisión para el Mercado Financiero; el DFL N°1 de 2018, del Ministerio de Hacienda, que establece Estatuto de Personal de Carácter Especial de la Comisión para el Mercado Financiero modificado por el DFL N° 1 de 2020, del Ministerio de Hacienda, para su aplicación al personal traspasado desde la Superintendencia de Bancos e Instituciones Financieras; la Ley N°19.880, sobre Bases de Procedimientos Administrativos que Rigen los Actos de la Administración del Estado; la Ley N°18.575 Orgánica Constitucional de Bases Generales de la Administración del Estado; la Ley N° 21.796 de Presupuestos del Sector Público correspondiente al año 2026; la Resolución Exenta N° 6 de 2019, de la Contraloría General de la República; la Resolución Exenta N°3097 del 1 de junio de 2019, que ejecuta acuerdo celebrado en sesión ordinaria N° 132 del 23 de mayo de 2019, del Consejo de la Comisión para el Mercado Financiero, que aprueba la política de gestión de personas de la CMF; la Resolución Exenta N° 3213 de 2024 de la Comisión para el Mercado Financiero que delega facultad para firmar actos, oficios y resoluciones y deja sin efecto resolución que indica.

CONSIDERANDO:

1. Que, el artículo 6 del DFL N° 1 de 2018, del Ministerio de Hacienda, que Establece el Estatuto de Personal de Carácter Especial de la Comisión para el Mercado Financiero modificado por el DFL N° 1 de 2020, del Ministerio de Hacienda, para su aplicación al personal traspasado desde la Superintendencia de Bancos e Instituciones Financieras dispone que el concurso público será un proceso técnico y objetivo que se utilizará para seleccionar al personal que ingresará a la Comisión sea en calidad de planta o a contrata con duración indefinida.
2. Que, el artículo antes mencionado dispone que en el concurso público se deberán respetar los principios de transparencia, imparcialidad, no discriminación, igualdad de condiciones de los/las postulantes y calidad técnica.
3. Que, la Comisión para el Mercado Financiero requiere realizar un concurso público para proveer el cargo de Jefe(a) de Departamento de Ciberseguridad, perteneciente a la Dirección General de Tecnologías de la Información, Profesional Grado 09.

RESUELVO:

1. **LLÁMESE** a concurso público para proveer el Jefe(a) de Departamento de Ciberseguridad, Profesional Grado 09, de acuerdo con las siguientes bases:



**BASES CONCURSO
DE LA COMISIÓN PARA EL MERCADO FINANCIERO**

I. ANTECEDENTES DEL SERVICIO

La Comisión para el Mercado Financiero (CMF) es un servicio público descentralizado, de carácter técnico, dotado de personalidad jurídica y patrimonio propio, que se relaciona con el Presidente de la República a través del Ministerio de Hacienda.

A la Comisión para el Mercado Financiero le corresponde la fiscalización de entidades de los mercados de valores, seguros y bancos, además de otras entidades establecidas por ley.

II. VACANTES PARA PROVEER

CÓDIGO CARGO	ESTAMENTO	GRADO	Nº VACANTES	CARGO	CALIDAD JURÍDICA
JDC26	PROFESIONAL	09	1	JEFE(A) DE DEPARTAMENTO DE CIBERSEGURIDAD	CONTRATA INDEFINIDA

III. ANTECEDENTES DEL CARGO

3.1. Objetivo del cargo: El cargo tiene como objetivo liderar el equipo de Ciberseguridad, administrar, gestionar y mejorar las reglas de detección y alerta de los equipos de seguridad y ciberseguridad que se encuentran funcionando en la plataforma tecnológica institucional con la finalidad de garantizar la protección contra amenazas cibernéticas, además de proponer y establecer controles y procedimientos que permitan el cumplimiento de los niveles de seguridad y ciberseguridad establecidos en la institución.

3.2. Funciones del cargo: Entre sus principales responsabilidades se encuentran:

- Liderar el equipo de ciberseguridad, definiendo en conjunto con el jefe de la División de Infraestructura Tecnológica y Conectividad, los roles y funciones de sus integrantes para que se cumplan los objetivos del Departamento.
- Liderar los proyectos de ciberseguridad que se lleven a cabo en la institución, apoyándose en los otros equipos internos de la Dirección General de Tecnologías de la Información y del área de Gestión de Riesgos.
- Gestionar las actividades de mitigación requeridas frente a alertas de seguridad, tanto a nivel interno de TI como con empresas que presten apoyo a TI en el ámbito de ciberseguridad.
- Participar activamente en la construcción y actualización del plan de recuperación tecnológica (DRP), liderar los equipos y procesos de respuesta ante incidentes cibernéticos y contención de alarmas y alertas cibernéticas.
- Elaborar, gestionar y mejorar los planes y proyectos de Ciberseguridad, alineados con la estrategia y metas institucionales.
- Mantener, actualizar y proponer procedimientos de Seguridad y Ciberseguridad alineados con la Política de Seguridad vigente de la institución.
- Participar activamente en los procesos y proyectos de tecnología que se desarrollen en la División de Infraestructura Tecnológica y Conectividad.
- Desarrollar las demás actividades institucionales que se le encomienden, en el ámbito de sus competencias.

3.3. Competencias del cargo:

- Planificación y Control de Trabajo
- Negociación e Influencia
- Gestión de Recursos
- Actitud Innovadora
- Visión Estratégica
- Gestión del Conocimiento Organizacional
- Desarrollo del Equipo de Trabajo
- Gestión del Clima Laboral y Conflictos



Para validar ir a <http://www.svs.cl/institucional/validar/validar.php>
FOLIO: RES-10538-26-37198-B SGD: 2026090614645

3.4 Conocimientos para el cargo:

- Arquitectura y operación de seguridad perimetral: firewalls de nueva generación (Fortinet, Palo Alto o Check Point), WAF, VPN, ZTNA, segmentación de red, IDS/IPS y balanceadores de carga.
- Plataformas de detección y respuesta: EDR/XDR, sandboxing y análisis de malware.
- SIEM y detección: diseño, ajuste y mejora continua de reglas de correlación y casos de uso.
- Gestión de vulnerabilidades: escaneo, priorización por riesgo, coordinación de remediación y pruebas de penetración (planificación, alcance y seguimiento de hallazgos).
- Hardening y administración segura de sistemas operativos Windows y Linux, servidores web y de aplicaciones (Apache, JBoss, IIS) y bases de datos relacionales; criptografía aplicada y gestión de certificados (PKI).
- Seguridad de redes y enlaces de comunicaciones: protocolos, VLAN, enrutamiento, DNS/DHCP, monitoreo de tráfico.
- Gestión de riesgos de ciberseguridad.
- Inglés técnico nivel intermedio

3.5. Nivel de Remuneración ofrecido: La renta corresponde a **Profesional Grado 09** equivalente a una remuneración bruta de **\$5.028.834.-**

IV. REQUISITOS DE POSTULACION

4.1. Requisitos generales.

Para ingresar a la Comisión en calidad de funcionario/a, será necesario cumplir con los siguientes requisitos:

- a) Ser ciudadano/a;¹
- b) Haber cumplido con la ley de reclutamiento y movilización, cuando fuere procedente;
- c) Tener salud compatible con el desempeño del cargo, lo que deberá certificarse por el Servicio de Salud correspondiente o por las entidades de salud que determine la Presidenta de La Comisión, a proposición de la Dirección General de Personas;
- d) Licencia de Educación Media o equivalente;
- e) No haber cesado en un cargo público como consecuencia de haber obtenido una calificación deficiente, o por medida disciplinaria, salvo que hayan transcurrido más de cinco años desde la fecha de expiración de funciones;
- f) No estar inhabilitado/a para el ejercicio de funciones o cargos públicos, ni hallarse condenado/a por delito que tenga asignada pena de crimen o simple delito;
- g) Cumplir con los requisitos específicos que la ley exige para determinados cargos.

La acreditación de los requisitos anteriores deberá efectuarse al momento de la postulación (completando formato de Declaración Jurada disponible en la página Web de la CMF). En el caso de lo dispuesto en la letra c), sólo debe acreditarlo el/la postulante seleccionado/a, previo al inicio de sus funciones.

4.2. Formación profesional requerida.

Título profesional de Ingeniero(a) Civil en Computación o Informática, Ingeniero(a) en Computación o Informática, Ingeniero(a) de Ejecución en Computación o Informática, Ingeniero(a) en Redes o Ingeniero(a) en Ciberseguridad.

4.3. Estudios de especialización.

- Requerido Magíster, postítulo o diplomado en Ciberseguridad, Seguridad de la Información, Gestión de Riesgos Tecnológicos o Gestión de Proyectos.
- Deseable certificación técnica en al menos una de las siguientes temáticas: ISO/IEC 27001 Lead Implementer o Lead Auditor, Continuidad Operacional (ISO 22301), Gestión

¹ Excepcionalmente, cuando para el desempeño de labores profesionales, fiscalizadoras o técnicas se requieran conocimientos científicos o de carácter especial, la Presidenta de la Comisión podrá designar a personal que no cumpla con este requisito. El acto que disponga la designación deberá ser fundado, especificándose claramente la especialidad que se requiere para el empleo.



de incidentes (GCIH o equivalente), Fortinet NSE 4 o superior, Splunk Core Certified, CEH, OSCP, CompTIA Security+ / CySA+ o Microsoft SC-200 / SC-300.

4.4. Experiencia profesional requerida.

- Experiencia profesional comprobable de al menos 4 años en Ciberseguridad, liderando equipos, proyectos o servicios de ciberseguridad.
Para este efecto será considerada como válida la experiencia desarrollada en todos los siguientes aspectos:
 - Operación de plataformas de seguridad perimetral, Endpoint, SIEM y gestión de identidades en entornos productivos;
 - Gestión y respuesta a incidentes de ciberseguridad, incluyendo contención, erradicación, análisis post-incidente y reporte a autoridades;
 - Implementación o mantención de marcos y normativas: ISO/IEC 27001 o NIST CSF 2.0 o COBIT y Ley 21.663 (Ley Marco de Ciberseguridad) y normativa de la ANCI;
 - Construcción y pruebas de planes de recuperación tecnológica (DRP) y continuidad operacional (BCP); y,
 - Experiencia comprobable en la administración y gestión de contratos de servicios con proveedores.
- Deseable experiencia de al menos 3 años en el sector financiero, regulador o en organismos públicos.

V. ETAPAS Y CRITERIOS DE EVALUACIÓN

La metodología de selección consistirá en evaluación de fases sucesivas e independientes, en las que los/las postulantes con la puntuación requerida de una etapa pasarán a la siguiente, en el orden que se indica:

1. **Evaluación de antecedentes curriculares** (Formación, especialización y experiencia profesional requerida).
2. **Evaluación de conocimientos técnicos y/o habilidades.**
3. **Evaluación de competencias laborales para el cargo.**
4. **Entrevista de apreciación global.**
5. **Selección final.**

Las fechas establecidas para realizar la evaluación de conocimientos técnicos y/o habilidades, competencias laborales para el cargo y entrevista de apreciación global, serán informadas vía correo electrónico, al señalado por cada postulante en su currículum vitae.

ETAPA 1. Evaluación de antecedentes curriculares.

Se asignarán puntajes en función de los requisitos establecidos en el perfil del cargo, de acuerdo con el siguiente detalle:



FACTOR FORMACIÓN, ESPECIALIZACIÓN Y EXPERIENCIA PROFESIONAL				
Subfactor	Categoría de evaluación	Ptje.	Ptje Máx.	Ptje Min.
1. Título profesional requerido.	Título profesional de Ingeniero(a) Civil en Computación o Informática, Ingeniero(a) en Computación o Informática, Ingeniero(a) de Ejecución en Computación o Informática, Ingeniero(a) en Redes o Ingeniero(a) en Ciberseguridad.	9	30	24
	Otros títulos profesionales.	0		
2. Estudios de especialización requeridos. *	Magíster en Ciberseguridad, Seguridad de la Información, Gestión de Riesgos Tecnológicos o Gestión de Proyectos	7		
	Postítulo o Diplomado en Ciberseguridad, Seguridad de la Información, Gestión de Riesgos Tecnológicos o Gestión de Proyectos.	5		
	No acredita estudios indicados.	0		
3. Estudios de especialización deseables. *	Certificación técnica en al menos una de las siguientes temáticas: ISO/IEC 27001 Lead Implementer o Lead Auditor, Continuidad Operacional (ISO 22301), Gestión de incidentes (GCIH o equivalente), Fortinet NSE 4 o superior, Splunk Core Certified, CEH, OSCP, CompTIA Security+ / CySA+ o Microsoft SC-200 / SC-300.	2		
	No acredita certificaciones indicadas.	0		
4. Experiencia profesional requerida. **	Al menos 4 años en Ciberseguridad, liderando equipos, proyectos o servicios de seguridad y conforme a indicado en el punto 4.4 de estas bases.	10		
	No cumple con los años o el tipo de experiencia indicada.	0		
5. Experiencia profesional deseable. **	Al menos 3 años en el sector financiero, regulador o en organismos públicos.	2		
	No cumple con los años o el tipo de experiencia indicada.	0		

* Se puntuará la especialización más alta presentada por el/la postulante; no se sumarán. De igual forma, se puntuará únicamente una certificación presentada por el/la postulante; no se sumarán certificaciones.

** Para evaluar la experiencia profesional, en el curriculum vitae que se adjunte a la postulación, se deben detallar de forma explícita las funciones desarrolladas.

Avanzarán a la siguiente etapa aquellos/as postulantes que obtengan el puntaje mínimo esperado.

ETAPA 2: Evaluación de conocimientos técnicos y/o habilidades.

En esta etapa se evaluarán los conocimientos técnicos y/o habilidades para el desempeño del cargo mediante una evaluación técnica y/o evaluación de habilidades, quedando clasificados/as en alguna de las siguientes categorías, con los puntajes que se indican a continuación:

FACTOR CONOCIMIENTOS TÉCNICOS Y/O HABILIDADES ASOCIADAS AL PERFIL			
Categoría de evaluación		Ptje.	Ptje. Máx. Ptje. Mín.
Muy satisfactorio (posee conocimientos y/o habilidades por sobre lo esperado).		20	20 10
Satisfactorio (posee conocimientos y/o habilidades conforme a lo requerido).		10	20 10
No satisfactorio (posee conocimientos y habilidades en un nivel menor a lo requerido).		0	

La evaluación de los conocimientos técnicos y/o habilidades, se realizará mediante alguna de las siguientes metodologías: prueba de desarrollo, prueba de selección múltiple, ensayo, resolución de casos, entrevista técnica, entre otros. En el evento de aplicarse más de una prueba, ello se hará de manera secuencial y solamente avanzarán a la siguiente prueba aquellos/as postulantes que obtengan el puntaje mínimo esperado en la prueba anterior.

La evaluación será realizada por una Consultora o profesional especializado.

Avanzarán a la siguiente Etapa aquellos/as postulantes que hayan obtenido el puntaje mínimo requerido, de acuerdo con la metodología utilizada para evaluar los conocimientos técnicos y/o habilidades.

Se informará el estado de la postulación al finalizar la etapa.

ETAPA 3: Evaluación de Competencias Laborales para el Cargo.

Se evaluarán las competencias definidas para el cargo, a través de una evaluación psicolaboral consistente en la aplicación de algunas de las siguientes metodologías: entrevista por competencias, test psicolaboral, dinámicas grupales, entre otras.

Los/las postulantes quedarán clasificados/as en alguna de las siguientes categorías, con los puntajes que se indican a continuación:

FACTOR COMPETENCIAS LABORALES PARA EL CARGO			
Categoría de evaluación	Ptje.	Ptje. Máx.	Ptje. Mín.
Recomendable de acuerdo con el perfil de Competencias definido para el cargo.	20	20	10
Recomendable con observaciones de acuerdo con el perfil de Competencias definido para el cargo.	10		
No Recomendable de acuerdo con el perfil de Competencias definido para el cargo.	0		

La evaluación será realizada por una Consultora o profesional especializado.

Avanzarán a la siguiente etapa aquellos/as postulantes que obtengan el puntaje mínimo esperado.

Se informará el estado de la postulación al finalizar la etapa.

ETAPA 4: Entrevista de Apreciación Global.

En esta etapa se evaluarán aspectos motivacionales y el nivel de adecuación de el/la postulante al perfil del cargo, a través de una entrevista de apreciación global realizada por el Comité de Selección, pudiendo éste designar a dos o más de sus integrantes para realizarla.

Se asignarán los puntajes de acuerdo con la categoría de evaluación obtenida por cada postulante, los que se indican en la siguiente tabla:

FACTOR ENTREVISTA DE APRECIACIÓN GLOBAL			
Categoría de Evaluación	Ptje.	Ptje Máx.	Ptje. Mín.
Se adecúa completamente a los aspectos motivacionales, relacionales y de socialización para el cargo.	30	30	20
Se adecúa a los aspectos motivacionales, relacionales y de socialización para el cargo.	20		
Se adecúa con observaciones a los aspectos motivacionales, relacionales y de socialización para el cargo.	10		
No se adecúa a los aspectos motivacionales, relacionales y de socialización para el cargo.	0		

ETAPA 5: Selección Final.

Luego de realizadas las Entrevistas de Apreciación Global, el Comité de Selección confeccionará una lista ordenada, en forma descendente, de acuerdo con el puntaje total obtenido por cada postulante, el que corresponderá a la sumatoria de los puntajes obtenidos en cada una de las etapas. Será considerado/a postulante idóneo/a aquel/lla que, cumpliendo los puntajes mínimos exigidos en cada etapa, obtenga un puntaje total de, a lo menos, **64 puntos**.



Posteriormente, el Comité propondrá a la Presidenta los nombres de los/las candidatos/as que hubieren obtenido los mejores puntajes. En caso de producirse empate entre dos o más postulantes con igual puntaje total, se resolverá de acuerdo con los siguientes criterios:

1. Puntaje Etapa de Entrevista de Apreciación Global.
2. Puntaje Entrevista de Apreciación Global.
3. Puntaje Etapa Conocimientos Técnicos y/o Habilidades.
4. Puntaje Etapa Competencias Laborales para el cargo.
5. Puntaje Etapa Formación, especialización y Experiencia profesional requerida.

La Presidenta de la Comisión para el Mercado Financiero seleccionará a una de las personas propuestas, de la nómina entregada por el Comité de Selección, o declarará desierto o parcialmente desierto, cuando ninguno/a de los/las postulantes alcance el puntaje mínimo definido para el respectivo concurso.

VI. CALENDARIZACIÓN CONCURSO PÚBLICO.

ACTIVIDAD / ETAPA	FECHA
Fecha de inicio de postulación	24 de Septiembre de 2026
Postulación y recepción de antecedentes.	10 días hábiles desde la Publicación del Concurso Público (24 de septiembre al 07 de octubre de 2026).
Análisis de Admisibilidad y Evaluación de Antecedentes Curriculares.	8 días hábiles a partir del día siguiente al cierre de las postulaciones (08 al 20 de octubre de 2026).
Conocimientos Técnicos y/o Habilidades.	8 días hábiles (21 al 30 de octubre de 2026).
Evaluación de competencias laborales para el cargo.	8 días hábiles (02 al 11 de noviembre de 2026).
Entrevista de Apreciación Global.	5 días hábiles (12 al 18 de noviembre de 2026).
Selección Final.	3 días hábiles (19 al 23 de noviembre de 2026).

Sin perjuicio de lo anterior, por razones relacionadas con el óptimo desarrollo del proceso, la División de Selección y Desarrollo de Carrera de la Dirección General de Personas de la CMF podrá modificar los plazos contenidos en la calendarización.

El avance de las etapas del proceso será comunicado a través de la página web de la CMF, en el apartado TRABAJA EN CMF.

VII. PROCESO DE POSTULACIÓN Y RECEPCIÓN DE ANTECEDENTES

La postulación deberá realizarse a través de la página web de la Comisión para el Mercado Financiero <http://www.cmfchile.cl> en el apartado TRABAJA EN CMF. En dicho apartado será redirigido a la plataforma **trabajando.com**.

En la postulación que realice en la plataforma trabajando.com deberá adjuntar en la sección “Anexos al CV”, sólo los siguientes documentos:

1. Cédula de Identidad vigente por ambos lados.
2. Certificado de Título, de acuerdo con las exigencias del cargo.
3. Declaración jurada con un año de antigüedad como máximo (en página web de la CMF, en sección Trabaja en CMF, podrá descargar el formato de Declaración Jurada Simple que deberá completar y adjuntar en formato PDF con la firma respectiva).
4. Certificado de Magister, Postítulo, Diplomado o Certificación relacionado con el cargo a proveer.
5. Currículum Vitae actualizado.

Las postulaciones serán recibidas hasta las 23:59 horas del día **07 de octubre de 2026**.

Sólo serán consideradas admisibles las postulaciones que presenten todos los antecedentes solicitados y que sean realizadas dentro de los plazos indicados.

Los/las postulantes son responsables de la completitud y veracidad de la información que presentan al momento de postular.



El correo electrónico seleccion@cmfchile.cl sólo estará disponible para recibir consultas referentes al proceso de postulación y el estado de avance del concurso.

Los/las postulantes que presenten alguna discapacidad que les produzca impedimento o dificultad en la aplicación de los instrumentos de selección que se administrarán, deberán informarlo en su postulación para adoptar las medidas pertinentes, de manera de garantizar la igualdad de condiciones a todos los/las postulantes que se presenten en este concurso.

La División de Selección y Desarrollo de Carrera de la Dirección General de Personas, estará a cargo de reunir todas las postulaciones y verificar el cumplimiento de los requisitos del cargo y de los antecedentes curriculares de los/las postulantes, determinando que quienes cumplan con ellos y se ajusten a los requerimientos efectuados, pasarán a la etapa siguiente del concurso.

VIII. COMUNICACIÓN DE RESULTADOS DE LA POSTULACIÓN.

Toda comunicación referida al desarrollo del concurso público será remitida a la casilla de correo electrónico que registren los/las postulantes, al momento de realizar la postulación en la plataforma **trabajando.com**.

Para conocer el avance de los concursos públicos, se deberá revisar la página web de la CMF, www.cmfchile.cl en el apartado TRABAJA EN CMF, específicamente en la sección “Estado de Concursos Públicos y Procesos de Selección Vigentes”.

Una vez finalizado el concurso público se notificará, en primer lugar, a el/la candidato/a seleccionado/a a través de correo electrónico o telefónicamente; a los/las candidatos/as no seleccionados/as se les notificará a través de correo electrónico, una vez finalizado el proceso.

En virtud de la entrada en vigencia de la ley N°21.389 (que crea el Registro Nacional de Deudores de Pensiones de Alimentos) y en el caso de ser contratada/o y/o nombrada/o, la institución consultará si el/la postulante seleccionado/a posee alguna obligación pendiente en el Registro Nacional de Deudores de Pensiones de Alimentos, a efecto de proceder con las retenciones y pagos que correspondan. La persona que figure en el registro deberá autorizar como condición habilitante para su contratación/nombramiento, que la institución proceda a hacer las retenciones y pagos directamente al alimentario.

El concurso público podrá declararse desierto cuando ninguno/a de los/las postulantes alcance el puntaje mínimo definido para el respectivo concurso, lo que también se informará en la página web de la CMF.

ANÓTESE, NOTIFÍQUESE Y ARCHÍVESE.



Para validar ir a <http://www.svs.cl/institucional/validar/validar.php>
FOLIO: RES-10538-26-37198-B SGD: 2026090614645



Juan Francisco Cantillana Paredes
Director General de Personas
Por Orden del Presidente de la
Comisión para el Mercado Financiero



Para validar ir a <http://www.svs.cl/institucional/validar/validar.php>
FOLIO: RES-10538-26-37198-B SGD: 2026090614645