FONDO NACIONAL DE RECURSOS
Medicina Altamente Especializada

Llamado a Responsable de Seguridad de la Información

El Fondo Nacional de Recursos (FNR) llama a interesados/as a postularse para ocupar el puesto de Responsable de Seguridad de la Información (RSI) en modalidad de contrato de servicios profesionales.

Objetivo del puesto

- Asesorar y participar en la formulación y cumplimiento de objetivos respecto a la Seguridad del Fondo Nacional de Recursos, teniendo como principales responsabilidades la de implementar, mantener y gestionar el Sistema de Gestión de Seguridad de la Información de acuerdo al Marco de AGESIC, y las relativas al rol según las recomendaciones de dicho órgano, y las políticas de estructura de la Seguridad de la Información aprobadas por la organización.
- El Responsable de Seguridad de la Información será responsable de establecer y mantener el programa de seguridad de la información de la empresa, alineado con los objetivos de negocio y en cumplimiento con las regulaciones aplicables. El FNR busca incorporar una visión estratégica de la seguridad y traducirla en un plan de ciberseguridad coherente, gestionando riesgos y promoviendo una cultura de seguridad en toda la organización

Formación

- Nivel terciario en tecnología de la información.
- Especialidad en seguridad de la información / ciberseguridad (por ejemplo: certificaciones CISSP, CISM, OSCP, entre otros).

Experiencia

- Mínimo de 2 años de experiencia en roles de liderazgo en ciberseguridad, preferiblemente en Instituciones de Salud o Instituciones Públicas o Paraestatales.
- Experiencia demostrable en la implementación de Sistemas de Gestión de Seguridad de la Información, de marcos de seguridad como el de AGESIC, NIST MCU, ISO 27001, COBIT o CIS Controls, o similares.
- Experiencia en la gestión de equipos de seguridad y en la interacción con la alta dirección.
- Investigaciones y/o proyectos relacionados a temas de seguridad de la información en general.
- Experiencia en respuesta a incidentes de ciberseguridad.

Requisitos a valorar

Se valorará tener:

- Amplios conocimientos en ciberseguridad.

- Conocimientos en seguridad de sistemas, redes y aplicaciones.
- Conocimientos en monitoreo de Seguridad.
- Conocimientos en desarrollo de soluciones de seguridad o afines.
- Conocimientos en procesos de Gestión de Incidentes.
- Auditorías de seguridad de la información.
- Gestión de riesgos de ciberseguridad.

Competencias personales

- Proactividad, iniciativa, y autonomía
- Orientación a resultados.
- Organización y planificación.
- Buen relacionamiento interpersonal y trabajo en equipo.
- Capacidad para trabajar bajo presión.
- Excelentes habilidades de liderazgo, comunicación y negociación.
- Capacidad para pensar estratégicamente y resolver problemas de manera creativa.
- Profundo conocimiento de tecnologías de seguridad y amenazas cibernéticas.
- Habilidad para gestionar presupuestos y recursos eficazmente.

Tareas

Liderazgo y Estrategia

- Desarrollar, implementar y supervisar la estrategia de ciberseguridad de la empresa, basándose en marcos de referencia como el Marco de Ciberseguridad de Uruguay, ISO 27000, NIST, HIPAA.
- Establecer la gobernanza de la seguridad de la información, definiendo políticas, estándares y procedimientos.
- Asesorar a la alta dirección y a la Comisión Honoraria Administradora sobre los riesgos de seguridad y el estado del programa de ciberseguridad.

Gestión de Riesgos

- Identificar, evaluar y mitigar los riesgos de seguridad de la información.
- Gestionar el proceso de evaluación de riesgos y asegurar la implementación de controles adecuados.
- Desarrollar y mantener un plan de respuesta a incidentes de seguridad robusto.

Conformidad y Cumplimiento

- Asegurar que la organización cumpla con las leyes, regulaciones y estándares de la industria aplicables (ej., MCU, HIPAA, ISO 27001).

- Coordinar auditorías internas y externas de seguridad.

Gestión de Operaciones de Seguridad

- Supervisar los equipos de seguridad de la información, incluyendo la gestión de amenazas, vulnerabilidades, monitoreo y respuesta a incidentes.
- Evaluar y seleccionar tecnologías de seguridad para proteger los activos de la empresa.

Cultura y Capacitación

- Promover una cultura de seguridad en toda la organización a través de programas de concientización y capacitación.
- Comunicar de manera efectiva los riesgos y las políticas de seguridad a todos los niveles de la empresa.

Descripción de Actividades

Las actividades del rol son las sugeridas por el órgano rector en la materia y las establecidas por las políticas y órganos internos, de las cuales se destacan principalmente:

- Desarrollar e implementar planes para la mejora de la seguridad de la información, en el Fondo Nacional de Recursos; tomando como referencia el Marco de ciberseguridad desarrollado por AGESIC, así como las buenas prácticas pertinentes basadas en estándares internacionales aplicables a cada materia.
- Velar por la vigencia de las políticas de seguridad de la información, mediante la revisión periódica y la actualización de las mismas de acuerdo a las definiciones del Fondo Nacional de Recursos.
- Verificar la alineación de la seguridad de la información con los objetivos estratégicos del Organismo.
- Recomendar, implementar, mantener y documentar el Sistema de Gestión de Seguridad de la Información.
- Gestionar la realización de revisiones independientes de seguridad de la información para asegurar la adecuación del sistema de gestión de seguridad de la información y su cumplimiento con la normativa vigente y el marco de ciberseguridad.
- Asegurar que la implementación de los controles de seguridad de la información esté coordinada en toda la organización y revisar en forma periódica los documentos y controles del Sistema de Gestión de Seguridad de la Información.
- Verificar la falta o superposición de controles en seguridad de la información.

- Desarrollar métricas y métodos que permitan monitorear las actividades de seguridad de la información, y verificar la eficiencia y eficacia de los controles.
- Trabajar en forma colaborativa con todas las áreas del Fondo Nacional de Recursos, promoviendo la implementación de buenas prácticas, asesorando e identificando oportunidades de mejora en materia de seguridad.
- Promover y participar de manera activa en la gestión de riesgos de seguridad de la información.
- Identificar cambios significativos en las amenazas y la exposición de la información y de las instalaciones de procesamiento de la información a las amenazas.
- Validar las definiciones de seguridad definidas por el área de TI y/o proveedores, específicas y relacionadas a aplicaciones y sistemas.
- Identificar y dar un orden a los controles de seguridad de la información para habilitar el acceso a un proveedor a los activos de información.
- Definir procedimientos y responsabilidades de gestión para la protección de los sistemas ante software malicioso.
- Asegurar el mantenimiento de los comprobantes de propiedad intelectual adquirida (ej. licencias, discos, manuales, etc.) y la utilización únicamente de software autorizado y bajo licencia y eliminar cualquier violación en este sentido.
- Coordinar con los "propietarios" de los procesos y activos de información, la alineación con la seguridad de la información definida.
- Velar por una adecuada implementación para la gestión de incidentes en el Fondo Nacional de Recursos, así como coordinar la gestión de incidentes de seguridad de la información, oficiar de punto de contacto con las autoridades en la materia y reportar al CERTuy los incidentes de seguridad informática detectados o sospechados siendo responsable, asimismo, de la definición del proceso de Gestión de Incidentes de Seguridad de la Información y de la coordinación de este proceso.
- Evaluar la información recibida de los seguimientos y revisiones de los incidentes de seguridad de la información y las acciones recomendadas en respuesta a los mismos.
- Definir y gestionar el plan de contingencia y recuperación ante desastres siendo responsable, asimismo, de la definición de los diferentes equipos de contingencia y de la coordinación de éstos.
- Promover instancias de concientización y actualización en cuanto a políticas y procedimientos organizacionales relevantes en materia de Seguridad de la información para el mejor cumplimiento de las funciones para todo el personal.
- Promover la difusión, concientización, educación y la formación en seguridad de la información.
- Elaborar el Plan Anual de Capacitación en Materia de Seguridad.
- Mantener contactos con autoridades relevantes vinculadas directa o

indirectamente con la seguridad de la información, así como con grupos de interés y foros especializados en seguridad.
- Promover el cumplimiento con la normativa y legislación vigente en relación con aspectos de seguridad de la información.

Condiciones

- Contrato de arrendamiento de servicios con una dedicación de al menos 30 horas semanales.
- Remuneración: acorde al cargo, la formación de grado y a la experiencia del candidato/a.
- Período de prueba: 90 días iniciales.
- Las actividades se realizarán bajo la supervisión de la Dirección General y en coordinación con el Comité de Seguridad de la Información.

Otras consideraciones especiales

La persona seleccionada deberá, como requisito indispensable para la firma de contrato, presentar una declaración jurada de conflicto de intereses y firmar un acuerdo de confidencialidad (NDA) respecto a toda la información a la que acceda en virtud de su Rol.

Sólo se considerará la formación o experiencia debidamente acreditada por documentación probatoria (certificados, diplomas, notas emitidas por las organizaciones donde haya trabajado, etc.).

Selección. Se realizará en base a criterios exclusivos del FNR.
Contempla lo dispuesto por el Art. 4º de la Ley Nº 19.122 de 21/8/2013 y el Art. 49 de la Ley Nº 18.651 de 19/2/2010.

- Recepción de CVs y carta de motivación hasta el 30 de noviembre de 2025
- Evaluación de postulaciones
- Entrevistas a los preseleccionados
- Psicotécnico a los preseleccionados

Se recibirán postulaciones hasta el **5 de diciembre de 2025**, únicamente por sitio web del FNR: http://www.fnr.gub.uy - Llamados