

## ANEXO N°2

### COMPETENCIAS MÍNIMAS DE LA CONTRAPARTE TÉCNICA ANTE ESTA SCJ

#### Competencias mínimas para el rol:

- Desarrollar y comunicar políticas, estándares y pautas de seguridad de la información corporativa. Contribuir al desarrollo de estrategias organizacionales que abordan los requisitos de control de la información. Identificar y monitorear las tendencias ambientales y del mercado y evaluar proactivamente el impacto en las estrategias, beneficios y riesgos comerciales. Liderar la provisión de asesoramiento y orientación autorizados sobre los requisitos para los controles de seguridad en colaboración con expertos en otras funciones, como soporte legal y técnico. Asegurar, que los principios arquitectónicos se apliquen durante el diseño para reducir el riesgo e impulsar la adopción y el cumplimiento de políticas, estándares y pautas.
- Proporcionar asesoramiento y orientación sobre estrategias de seguridad para gestionar los riesgos identificados y garantizar la adopción y el cumplimiento de los estándares. Obtener y actuar sobre la información de vulnerabilidad y realizar evaluaciones de riesgos de seguridad, análisis de impacto empresarial y acreditación en sistemas de información complejos. Investigar las principales brechas de seguridad y recomendar las mejoras de control adecuadas.
- Explicar el propósito y brindar asesoramiento y orientación sobre la aplicación y operación de controles elementales de seguridad físicos, procedimentales y técnicos. Realizar evaluaciones de riesgos de seguridad, vulnerabilidades y análisis de impacto empresarial para sistemas de información de complejidad media. Investigar presuntos ataques y gestionar incidentes de seguridad. Utilizar análisis forense cuando sea apropiado.
- Comunicar los riesgos y problemas de seguridad de la información a los gerentes comerciales y otros. Aplicar y mantener controles de seguridad específicos según lo requiera la política de la organización y las evaluaciones de riesgos locales. Investigar presuntos ataques. Responder a las brechas de seguridad de acuerdo con la política de seguridad y registrar los incidentes y las acciones tomadas.
- Competencias sobre gobierno de la seguridad de la información
- Competencias sobre gestión de riesgos de seguridad de la información
- Competencias sobre gestión de un programa de seguridad de la información
- Competencias sobre gestión de incidentes de seguridad de la información
- Conocimientos sobre marcos legales atinentes a seguridad de la información y ciberseguridad
- Conocimiento sobre marcos normativos nacionales e internacionales sobre ciberseguridad

Estos aspectos se verificarán con alguna o todas estas posibilidades.

- Deseable certificación CISM o equivalente
- Deseable certificación CISSP o equivalente
- Deseable certificación Implementador ISO27001 o equivalente
- Deseable Diplomados en Gestión de Seguridad de la Información
- Deseable Magister o Doctorado en Seguridad de la información
- Necesaria experiencia laboral verificable en seguridad de la información
- Carrera deseables: Ingeniería en Informática, Ingeniería Electricista, Abogado con experiencia en ciberseguridad y datos o Electrónica, Ingenierías en Ciberseguridad o afín.