Supervisar y gobernar

Autor
Agesic

Fecha de creación
08/02/2020

Tipo de publicación
Lineamiento

Resumen

Conocé de qué manera podés llevar a cabo el trabajo de ciberseguridad en tu organización.

Introducción

- *Gestión de Ciberseguridad*. Supervisá el programa de Ciberseguridad de un sistema o una red de información, incluida la gestión de las implicaciones de Seguridad de la Información dentro de la organización, programa específico u otra área de responsabilidad, para incluir estrategias, personal, infraestructura, requisitos, cumplimiento de políticas, planificación de emergencias, conciencia de seguridad y otros recursos.
- *Liderazgo cibernético ejecutivo*. Supervisá, gestioná y dirigí el trabajo y las tareas que realizan trabajos de operaciones cibernéticas.
- *Asesoría legal y abogacía*. Brindá asesoramiento y recomendaciones legalmente sólidas al liderazgo y al personal sobre una variedad de temas dentro del dominio de materias relevantes. Abogá por cambios legales y de políticas y presentá un caso en nombre del cliente a través de una amplia gama de productos de trabajo escritos y orales, incluidos resúmenes y procedimientos legales.
- *Programa de gestión y adquisición*. Aplicá el conocimiento de datos, información, procesos, interacciones organizacionales, habilidades y experiencia analítica, así como sistemas, redes y capacidades de intercambio de información para administrar programas de adquisición. Ejecutá funciones que rigen los programas de adquisición de hardware, software y sistemas de información y otras políticas de administración de programas. Brindá soporte directo para adquisiciones que usan Tecnologías de la Información (TI), incluidos los sistemas de seguridad nacional, aplicando leyes y políticas relacionadas con TI. Asimismo, brinda orientación relacionada con TI durante todo el ciclo de vida de adquisición.
- *Planificación estratégica y política*. Desarrollá políticas y planes y aboga por cambios en las políticas que apoyen iniciativas de ciberespacio organizacionales o cambios y mejoras requeridos.
- *Entrenamiento, educación y conciencia.* Realizá la capacitación del personal dentro del dominio de la materia relevante.

Marco de Ciberseguridad

El documento está basado en el Marco de Ciberseguridad definido por el Instituto Nacional de Estándares y Tecnología (NIST-CSF) para la mejora de la Ciberseguridad en infraestructuras críticas y contextualizadas a las organizaciones que requieren:

- Gestionar los riesgos inherentes a la Seguridad de la Información y al uso de la infraestructura tecnológica que le da soporte.
- Adoptar políticas que mejoren el nivel de Ciberseguridad existente.
- Incorporar medidas para lograr centros de datos seguros.
- Cumplir con la normativa vigente en materia de Seguridad de la Información, en particular, la aplicable a la Administración Central.

Ver Marco de Ciberseguridad.

Seguro te conectás: materiales didácticos

Seguro te Conectás es una campaña de difusión orientada a sensibilizar a los usuarios de internet y dispositivos digitales.

Su objetivo es dar a conocer y aumentar la comprensión de las amenazas informáticas, propiciando un vínculo responsable entre las personas e internet.

La campaña te permitirá informarte acerca de lo que puede afectar tu seguridad en el mundo digital y de qué manera protegerte

- Videos
- Afiches
- Folletos
- Presentación
- Juegos

Más información: Seguro te conectás

Si tenés consultas, podés escribir al correo: seguroteconectas@agesic.gub.uy