# *SISTEMA NACIONAL DE CAPACITACION*
# *DISEÑO DE LA ACTIVIDAD*

## ***Nombre***

INTRODUCCIÓN A LA GESTIÓN DE RIESGOS DE SEGURIDAD INFORMÁTICA

***Código INAP*** IN38817/23 ***Estado*** Activo

***Programa*** )Campos de Práctica ***Área*** Sistemas, procesos y tecnologías

## ***Fundamentación***

Tema: Gestión administrativa, de la información y los datos
Propósito: Desarrollo / fortalecimiento de capacidades

La presente actividad se enmarca en el Programa INAP Futuro, con el propósito de fortalecer las capacidades digitales vinculadas a la seguridad en entornos digitales.

La gestión de riesgos de seguridad informática consiste en detectar y valorar cómo éstos pueden afectar a una organización para luego definir qué medidas tomar para enfrentarlos. Se trata de una labor fundamental y central para la protección de los activos de información y, sobre todo, la continuidad de las operaciones de una organización, ya sea pública o privada. De modo que tener un plan de riesgos permitirá que los objetivos propuestos puedan ser alcanzados de la mejor manera posible, haciendo resiliente a la organización.

Por tal motivo, capacitar a los empleados del Sector Público Nacional en esta temática permitirá que analicen impactos de diferentes factores que pueden afectar su labor cotidiana, los servicios que brindan, como la operatividad, la seguridad de la información que gestionan y el rendimiento de sus dispositivos. Asimismo podrán aplicar recursos, acciones y medidas de seguridad para minimizar, controlar y supervisar cualquier impacto negativo que pudiera afectarlos, con foco en aquellos datos y sistemas considerados críticos.

A partir de lo mencionado y en línea con la Propuesta Formativa del INAP, en la presente actividad prevalecen los siguientes tipos de saberes: Saber (saberes objetivados sobre la realidad organizados en sistemas de conceptos y teorías) - Saber hacer (saberes de acción vinculados con la capacidad de intervenir) - Saber qué hacer (saberes de situación relacionados con la capacidad de tomar decisiones en situaciones y contextos específicos).

## ***Contribución esperada***

Se espera que los participantes aprendan los aspectos fundamentales de la gestión de riesgos de seguridad informática para definir estrategias a implementar, medidas de seguridad que permitan mitigar, prevenir o reducir daños y consecuencias en los activos de información del organismo en el que se desempeñan.

## ***Perfil del participante***

Perfiles que se desempeñen en áreas de TI, Seguridad o Auditoría Informática en los organismos públicos, que deban identificar, gestionar, adoptar, monitorear y evaluar medidas para mitigar los riesgos asociados al uso de sistemas, infraestructura y servicios informáticos ya sea propio o de terceros que brindan servicios al Estado.

## ***Objetivos***

Que los participantes logren:
- Comprender y dimensionar el alcance y el impacto potencial de los riesgos a los que se expone el organismo cuando gestiona, implementa y/o adquiere servicios o sistemas informáticos para llevar adelante sus competencias.
- Gestionar los riesgos identificados de acuerdo a las pautas establecidas por las autoridades del organismo.
- Comunicar en forma precisa y comprensible los aspectos que deben considerarse para determinar la postura a adoptar frente a cada tipo de riesgo.
- Conocer distintas metodologías de evaluación de riesgo para aplicarlas en sus organismos.

## ***Contenido***

MÓDULO 1: Qué es el riesgo
Definición – Tipo de riesgo en una organización – Riesgo de ciberseguridad - Características – Vinculación con los conceptos de vulnerabilidad, amenaza y controles/medidas de seguridad.

MÓDULO 2: El proceso de gestión de riesgos de Seguridad de la Información.
Principales metodologías y estándares internacionales.

MÓDULO 3: Normas nacionales aplicados a la gestión de riesgo de ciberseguridad.
Normativas aplicables a organismos públicos (Decisión Administrativa N° 641/2021, Resolución SIGEN N° 87/2022).

## ***Estrategias metodológicas y recursos didácticos***

Se trabajará con modalidad virtual virtual sincrónica a partir de estrategias metodológicas que faciliten:
- la revisión de las ideas, conocimientos previos.
- la apropiación y uso de nuevos saberes,
- el análisis y la revisión de las propias prácticas.

La propuesta de trabajo promueve las siguientes actividades:
- Puesta en común de ideas, saberes y experiencias previas.
-Espacios de participación para que las y los participantes intercambien respecto a las temáticas abordadas, compartan sus opiniones, ideas, realicen consultas.
- Análisis y resolución de casos a partir de los contenidos desarrollados.

Por su parte, la/s tutoras acompañaran y realizarán el seguimiento de los aprendizajes del grupo, brindarán devoluciones evaluativas generales, realizarán comentarios de retroalimentación individuales.

## Descripción de la modalidad

Virtual sincrónica

## Bibliografía

La presente bibliografía tiene carácter optativo.

Normas Nacionales

Decisión Administrativa N° 641/2021
Resolución SIGEN N° 87/2022

Internet: links a sitios y documentos de interés.
Situaciones de riesgo moral e incentivos desalineados en ciberseguridad – Rev. Chilena de Derecho tecnológico. Vol.11 no.1 Santiago jun. 2022 Disponible en:
https://www.scielo.cl/scielo.php?pid=S0719-25842022000100103&script=sci_arttext&tlng=pt
Modelo de Evaluación de Madurez para la Gestión de la Seguridad de la Información Integrada en los Procesos de Negocio – Cap. 1 y 5 - Trabajo Final de Maestría de Marcia Maggiore – Maestría en Seguridad Informática (UBA) – 2014. Disponible en:
http://bibliotecadigital.econ.uba.ar/download/tpos/1502-0550_MaggioreML.pdf
Vulnerabilidades, amenazas y riesgo en “texto claro” – Patricia Prandini y Marcela Pallero – Revista Magazcitum – 2013 - Disponible en https://www.magazcitum.com.mx/index.php/archivos/2193

## Evaluación de los aprendizajes

Evaluación de proceso:
Se evaluarán las diferentes producciones parciales de los participantes mediante preguntas multiple choice al término de algunos de los encuentros.

Evaluación de producto
A partir de situaciones y casos planteados, los participantes deberán relacionar los conceptos fundamentales trabajados y recomendar -de acuerdo a lo aprendido en el curso y sus propias realidades- las estrategias y metodologías que se seguirán para realizar una adecuada evaluación de riesgos.

## Instrumentos para la evaluación

Instrumento para la evaluación de los aprendizajes: Informes de la plataforma. Matriz para el seguimiento y evaluación de las actividades.

Instrumentos para la evaluación de la actividad: Encuesta de satisfacción INAP.

## Requisitos de Asistencia y aprobación

Requisitos de asistencia y aprobación

Asistir al menos a cinco (5) de los seis (6) encuentros virtuales sincrónicos

Realizar y aprobar las actividades intermedias con 60%.

Realizar y aprobar la evaluación final con 60%.

## Duración (Hs.)

12

## Detalle sobre la duración

12 horas totales, divididas en seis encuentros virtuales sincrónicos semanales de dos horas cada uno

## Lugar

Plataforma Cisco Webex

Campus virtual de INAP

## Perfil Instructor

Experta en la materia

## Origen de la demanda

INAP - Dirección Nacional de Ciberseguridad

## Prestadores Docentes

| CUIT/CUIL | APELLIDO Y NOMBRE |
|---|---|
| 27126661709 | MOLINARI,LÍA HEBE |
| 23135307564 | PRANDINI,MARIA PATRICIA |