

SISTEMA NACIONAL DE CAPACITACION DISEÑO DE LA ACTIVIDAD

Nombre

INTRODUCCIÓN A LA PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

Código INAP IN37828/22 **Estado** Activo

Programa)Actividades Transversales **Área** Sistemas, procesos y tecnologías

Fundamentación

Subtema: Gestión administrativa, de la información y los datos: conceptos, prácticas y normativas vinculados con la gestión documental y los procesos de la Administración Pública. Incluye el análisis, la comprensión y el uso de las herramientas y procedimientos para la gestión de los datos e información digitales, y conceptos, nociones, prácticas y aplicaciones vinculadas al hardware y software, redes y seguridad informática. También abarca el tratamiento de la Inteligencia Artificial (IA), la gestión de grandes volúmenes de datos (big data), el trámite administrativo digital, y la automatización de procesos.

Propósito: Actualización / Sensibilización

Las amenazas y la consecuente protección de las infraestructuras críticas es una problemática que data de la Antigüedad, y responden a diversas causas, tanto accidentales como intencionales. Podemos hablar de catástrofes hasta atentados o guerras, por ejemplo. Pero en los últimos años se ha agregado a la lista un componente que aumenta considerablemente el riesgo sobre la seguridad de las infraestructuras críticas: las redes de computadoras. Debido al uso de éstas, han surgido nuevos tipos de ataques, por ejemplo, las ciberguerras, el ciberterrorismo, etc.

Esto sucede debido a que hace ya varios años y hasta el día de hoy, las infraestructuras críticas se apoyan fuertemente en la tecnología para su funcionamiento, lo cual permite grandes avances y mejora ampliamente la calidad de vida de las personas, pero por otro lado las expone a nuevas amenazas, como ya se dijo, las “ciber” amenazas.

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 reflexionar (saberes relacionados a la capacidad de volver el pensamiento sobre objetos, situaciones, hechos, creencias, etc).

Contribución esperada

Se espera que los participantes provenientes de los distintos organismos logren adoptar una visión integral de la ciberseguridad y reconocer las infraestructuras críticas, pudiendo aplicar y gestionar lo aprendido en pos de una protección eficaz de la información de sus organizaciones.

Perfil del participante

Servidores públicos de la APN

Objetivos

Que los participantes logren:

Identificar las infraestructuras críticas de una nación, familiarizándose con los conceptos y la importancia de las mismas.

Comprender nociones básicas de la ciberseguridad y casos a nivel mundial.

Reflexionar sobre los riesgos a los cuales se exponen las infraestructuras críticas de nuestro país.

Aplicar y gestionar acciones que pueden llevarse adelante para proteger las infraestructuras críticas.

Conocer el panorama legislativo nacional y una aproximación al internacional.

Contenido

Módulo 1: Aspectos introductorios

¿Cuáles son las infraestructuras críticas?

¿Cómo pueden verse afectadas?

Distintos tipos de riesgos

Casos reales del pasado

Distribución de ataques y de sectores objetivos – gráficos estadísticos

Módulo 2: Situación en el mundo

América

Europa

Asia

Módulo 3: Mejores prácticas para la protección de infraestructuras críticas

Líneas de trabajo

Medidas de seguridad

Legislación vigente en Argentina y en el mundo

Estrategias metodológicas y recursos didácticos

El curso se basa en teoría, redactada exclusivamente por la docente en formatos descargables para permitirnos conocer el significado, la historia de las Infraestructuras Críticas y su importancia, tanto a nivel local como internacional. Cada unidad cuenta con cuestionarios autoadministrados, con sus respectivos feedbacks, para fijar conceptos.

Descripción de la modalidad

Virtual autogestionado

Bibliografía

S2 Grupo - Infraestructuras Críticas –

NIST-Framework for Reducing Cyber Risks to Critical Infrastructure –

NIST-Critical Infrastructure Protection –

Sitio web de INCIBE – ESPAÑA –

National Cyber Security Strategies – ENISA

<http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper> -

National Cyber Security Strategies – UK

Evaluación de los aprendizajes

De proceso: Cuestionarios auto administrados al finalizar cada una de las unidades temáticas.

De producto: Cuestionario de selección múltiple, integrador de los contenidos trabajados.

Instrumentos para la evaluación

Instrumentos para la evaluación de los aprendizajes: Informes de la plataforma

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

Requisitos de Asistencia y aprobación

Realizar y aprobar los cuestionarios autoadministrados con el 60% de respuestas correctas.

Duración (Hs.)

10

Detalle sobre la duración

10 horas distribuidas en 2 semanas de trabajo en plataforma.

Lugar

Campus virtual INAP

Perfil Instructor

Especialistas en la temática.

Origen de la demanda

INAP - DIRECCIÓN NACIONAL DE CIBERSEGURIDAD

Prestadores Docentes

CUIT/CUIL	APELLIDO Y NOMBRE
	ACTIVIDAD,AUTOADMINISTRADA