SISTEMA NACIONAL DE CAPACITACION
DISEÑO DE LA ACTIVIDAD

Nombre

INTRODUCCIÓN A LA PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

Código INAP IN29217/18 ***Estado*** Activo

Programa -Formación Continua ***Área*** + Tecnologías de Información y Comunic.

Fundamentación

El presente curso se enmarca en la estrategia de capacitación del MINISTERIO DE MODERNIZACIÓN, en colaboración con el Instituto Nacional de la Administración Pública y el Proyecto de Modernización del Estado.

Uno de los objetivos, a nivel nacional es establecer prioridades y planes estratégicos para liderar el abordaje de la ciberseguridad en el Sector Público Nacional como también la promoción de la toma de conciencia de los integrantes de las organizaciones del Estado y del público en general en relación con los riesgos que acarrea el uso de medios y herramientas tanto en el ámbito laboral como en la vida diaria, así como del rol compartido entre el sector público y el privado para el resguardo de la infraestructura crítica.

La protección de las infraestructuras críticas es una problemática que data de la antigüedad, cuando todo pueblo, tribu o comunidad se preocupaba por proteger aquello que le resulta de vital importancia para su supervivencia. Por ejemplo, el abastecimiento de agua, el alimento, la energía, etc.. Recién hacia fines del siglo XX se comenzó a nombrar explícitamente a las infraestructuras críticas.

Las amenazas a las infraestructuras críticas datan también de antaño y responden a diversos motivos, 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 las mismas han surgido nuevos tipos de ataques: el ciberdelito, 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.

Con el paso del tiempo esta tendencia se va a ir marcando cada vez más, ya que los avances tecnológicos tanto para bien como para mal, no van a detenerse. Por ello, seguiremos disfrutando de mejoras a nuestra calidad de vida por la evolución de las infraestructuras críticas, pero también veremos cómo se ampliarán y profundizarán las técnicas y los medios

utilizados para el atentado a las mismas.

Contribución esperada

Se espera que los miembros de los organismos conozcan a qué llamamos infraestructuras críticas, la importancia que poseen para la vida cotidiana, los riesgos a los cuales se exponen y las maneras en las cuales es necesario protegerlas y garantizar así la calidad de vida de las personas.
Adicionalmente, muchos de los organismos forman parte de las infraestructuras crítica, por lo que deben tomar cartas en el asunto a la hora de protegerlas, y el conocimiento de las mismas así como de sus riesgos resulta vital a la hora de emprender acciones tendientes a su salvaguarda.

Perfil del participante

•Agentes de entidades y jurisdicciones definidas en el artículo 8º de la Ley Nº 24.156 a cargo de tareas administrativas, no se requieren conocimientos previos en seguridad informática.
• Personal de Organismos Interjurisdiccionales.
• Personal de Organismos Civiles
• Personal del Sector privado
No se requieren conocimientos previos en seguridad de la información.

Objetivos

Se espera que al finalizar el curso los participantes sean capaces de:
• Identificar las infraestructuras críticas de una nación, familiarizándose con los conceptos y la importancia de las mismas.
• Conocer la evolución de los ataques a las infraestructuras críticas.
• Comprender los riesgos a los cuales se exponen las infraestructuras críticas de nuestro país.
• Conocer el panorama internacional de las acciones llevadas a cabo para la protección de las infraestructuras críticas.
• Contar con una noción de las acciones que pueden llevarse adelante para proteger las infraestructuras críticas.

Contenido

Módulo 1:
• Antecedentes
• ¿Cuáles son las infraestructuras críticas?
• ¿Cómo pueden verse afectadas?
• Ciberseguridad
• Casos reales del pasado
• Distribución de ataques y de sectores objetivos.

Módulo 2:
• Situación en el mundo
o América
o Europa
o Asia
• Comparativa de puntos principales.

Módulo 3:
• Mejores prácticas para la protección de infraestructuras críticas
o Líneas de trabajo
o Medidas de seguridad
o Legislación vigente
- USA
- Europa
- España
- Argentina

Estrategias metodológicas y recursos didácticos

Como todo curso a distancia mediado por tecnologías, una de las cuestiones principales a tener en cuenta respecto de la metodología es establecer una mediación apropiada entre quienes asumen el desafío de facilitar el aprendizaje y quienes tienen la intención de aprender. Para ello se ha diseñado un dispositivo didáctico constituido por prácticas, estrategias y procesos que se desarrollan e implementan para lograr los objetivos determinados.

Las mediaciones, en este caso, se concretan a través de los materiales de estudio diseñados específicamente para el aprendizaje a distancia-, el entorno virtual de enseñanza y aprendizaje y la intervención didáctica del tutor. Este último asume diversos roles. Los tutores cumplen un papel fundamental como organizadores y facilitadores de la participación de los cursantes. Esta función implica tres roles complementarios en su tarea como dinamizador (Mason, 1991):

a) Rol organizativo: implica organizar y establecer una agenda estimativa (lecturas, actividades, fechas, reglas de procedimiento, normas); además supone actuar como impulsor de la participación del grupo: pidiendo contribuciones regularmente, proponiendo actividades en las que se deba dar una respuesta, iniciando la interacción, variando el tipo de participación, no monopolizando la participación.

b) Rol social: crear un ambiente agradable de aprendizaje, interactuando constantemente con los participantes y haciendo un seguimiento positivo de las actividades que realicen y pidiendo que expresen sus opiniones cuando lo necesiten.

c) Rol intelectual: como facilitador de aprendizaje orienta centrando las discusiones en los puntos cruciales, haciendo preguntas, y respondiendo a las consultas de los participantes, despejando obstáculos que puedan presentarse en el aprendizaje, ofreciendo ejemplos, animando también a los participantes a elaborar y ampliar sus comentarios y aportes.

Teniendo en cuenta que se trata de una capacitación a distancia, en la modalidad e-learning, los participantes cuentan con los siguientes recursos para llevar adelante su estudio.

• Material de estudio:
Material que presenta situaciones cotidianas a modo de casos, en los que la seguridad de la información tanto personal como de las organizaciones donde trabajamos puede verse amenazada. El material permite analizar el caso presentado a través de interrogantes y permite introducir algunos conceptos fundamentales y reflexionar sobre consecuencias de algunas prácticas habituales. A su vez, de este análisis se derivan una serie de recomendaciones que promueven un uso seguro de la información.
o Material en PDF: al final de cada caso se ofrecen una serie de textos en formato PDF para ampliar y revisar los aspectos teóricos relacionados con cada situación.

• Otros recursos: El entorno virtual, además del material de estudio, ofrece distintos recursos, herramientas y espacios de interacción para favorecer el estudio a distancia:
o El Foro de los Participantes que permite promover el intercambio asincrónico de opiniones sobre las temáticas del curso entre los inscriptos de todo el país.
o El Espacio del tutor, en el cual un tutor publicará las respuestas a las consultas referidas a los temas del curso. Este es un espacio de uso exclusivo del tutor. El tutor es un especialista en los contenidos del curso al que el participante podrá recurrir cada vez que lo necesite. La frecuencia con la que atenderá y responderá las consultas será comunicada a los participantes, en su primer mensaje. Asimismo, en el foro el docente publicara noticias de actualidad relacionadas con las unidades a los fines de que los alumnos puedan contrastar la teoría con la realidad, volcar sus comentarios o dudas. De igual manera, el docente los alentara a que compartir notas, videos o material vinculado.

• Lecturas: para consultar otros textos de lectura complementaria al material del curso.
o Sitios Web relacionados: son accesos a las páginas de Internet que ofrecen contenidos relacionados con las temáticas del curso.
o Glosario: con los términos o expresiones que adquieren significado específico en el curso.
o Videos relacionados que ilustran situaciones de la vida cotidiana vinculadas con la seguridad de la información.
- Documentos o papers de actualidad que el docente recomiende.

• Además, desde la página principal del Programa (https://procae.sgp.gov.ar) puede accederse a una Mesa de Ayuda, para solicitar asistencia ante cualquier problema con la plataforma o acceso al curso

Descripción de la modalidad

Virtual.

Bibliografía

- S2 Grupo - Infraestructuras Criticas

- NIST-Framework for Reducing Cyber Risks to Critical Infrastructure

- NIST-Critical Infrastructure Protection

- 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
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

- National Cyber Security Strategies – CANADA
http://www.publicsafety.gc.ca/prg/ns/cybr-scrty/_fl/ccss-scc-eng.pdf

- CNPIC – ESPAÑA
http://www.cnpic-es.es/

- Estrategia del ciberespacio- USA
http://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

- Protección de infraestructuras críticas
http://j.mp/u5Rd2a

- Alemania
http://www.bmi.bund.de/cae/servlet/contentblob/598732/publicationFile/34423/kritis_englisch.pdf

http://msmunir.batan.go.id/iaea2008/Reference_material/NatlStd/GER_National_Plan_for_Information_Infrastructure_Protection.pdf.

Evaluación de los aprendizajes

La evaluación de los aprendizajes se realizará mediante las siguientes herramientas:

• Actividades de intercambio en foros del entorno virtual: Se presentan consignas que permiten realizar el seguimiento del proceso de los participantes en el curso, su compromiso con el trabajo de reflexión y de colaboración que pretende promover. El seguimiento es posible a través de las intervenciones, aportes y opiniones que elaboren y envíen los participantes.

• Autoevaluaciones en línea (unidad 1 y 3), de respuesta automática. Apuntan a corroborar el trabajo de lectura y análisis de los contenidos, el dominio y comprensión de los aspectos conceptuales del curso. Se califican con nota numérica, escala de 1 a 10 en la que 10 es el puntaje más alto.

• Trabajo practico (Unidad 2): Algunas unidades son evaluadas mediante un trabajo practico en el cual se establece una consigna a desarrollar vinculadas a la unidad en curso.

•Trabajo final Integrador: se plantea una consigna final integradora de todo el curso para que los alumnos realicen un trabajo práctico de desarrollo el cual será evaluado por los docentes.

Requisitos para la aprobación

• Registrar al menos tres participaciones en los foros, una por cada unidad temática.
• Completar las dos autoevaluaciones (Unidad 1 y 3) con un mínimo de 7 puntos.
• Completar el trabajo práctico de la unidad restante (Unidad 2) con una calificación de “aprobado”.
• Completar el Trabajo final integrador de todo el curso con una calificación de “aprobado.”

Instrumentos para la evaluación

• Informes de la plataforma.
• Ejercicios de autoevaluación en el Entorno Virtual.
• Trabajo practico
• Trabajo practico final integrador.
• Participación en los foros.

Requisitos de Asistencia y aprobación

Para los participantes el proceso de aprendizaje implica:

• Estudiar los contenidos del curso.
• Profundizar los contenidos a través de la consulta de la bibliografía recomendada.
• Realizar las actividades propuestas en el foro.

• Interactuar con el tutor y el resto de los participantes.
• Navegar por sitios Web relacionados con el curso.

La acreditación del curso estará dada por las siguientes instancias:
• Estudio de la totalidad de los contenidos que conforman la propuesta.
• Participación en las actividades que plantee el tutor en el entorno virtual.
• Obtención de un 70% de efectividad en las actividades de autoevaluación (calificación automática por parte de la función específica de la plataforma).

Duración (Hs.)

45

Detalle sobre la duración

4 semanas.

Lugar

Campus virtual INAP.

Perfil Instructor

Especialistas en la temática especifica del curso y en la modalidad a distancia, en particular en e-learning.

Origen de la demanda

MINISTERIO DE MODERNIZACIÓN.

Prestadores Docentes

CUIT/CUIL	APELLIDO Y NOMBRE
27252515890	GALAN,MARIANA