SISTEMA NACIONAL DE CAPACITACION
DISEÑO DE LA ACTIVIDAD

Nombre

INTRODUCCIÓN A LA GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

Código INAP IN38565/22 ***Estado*** Activo

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

Fundamentación

Sub tema: Gestión administrativa, de la información y los datos
Propósito: Sensibilización/Actualización

Esta actividad se enmarca en el Programa INAP Futuro por su contribución al desarrollo de capacidades digitales.

El creciente y continuo uso de las Tecnologías de Información y las Comunicaciones (TIC) en la gestión pública han permitido optimizar y mejorar los procesos de los organismos, pero a su vez, dicha evolución trae riesgos que pueden afectar de forma directa las operaciones, sistemas e información. Por esto resulta pertinente capacitar a los funcionarios públicos con las nociones técnicas y administrativas básicas que permitan mitigar los riesgos de seguridad informática, por medio de una correcta gestión de los incidentes detectados. Es clave que ante un problema de seguridad que afecte a los sistemas se cuente con las herramientas que permitan a los funcionarios entender cuestiones tales como la severidad del incidente, hacer una categorización crítica del problema, entender sobre las acciones concretas que debe llevar a cabo, y poder brindar un seguimiento adecuado que mejore la prevención, protección, resiliencia y seguridad de los sistemas.

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

Contribución esperada

Se espera elevar la eficiencia en el manejo operativo de los incidentes de seguridad informática de los organismos, mejorar la resiliencia de los sistemas ante eventuales ataques y dotar a los funcionarios técnicos de conocimientos que ayuden a garantizar la correcta gestión de los problemas.

Perfil del participante

Personal de la Administración Pública Nacional

Objetivos

Que los participantes logren:

- Identificar los incidentes de seguridad informática
- Evaluar incidentes de seguridad informática por medio de una correcta calificación, tratado, resolución y comprensión del mismo.
- Valorar los procedimientos que contribuyan a la prevención, protección y resiliencia de los sistemas informáticos a su cargo.
- Integrar herramientas y buenas prácticas que impacten en la mejora de los procesos y procedimientos correspondientes a la administración de los sistemas informáticos
- Reflexionar sobre los riesgos y responsabilidades que conlleva la administración de los sistemas informáticos.

Contenido

Unidad I: Incidentes de seguridad informática
- Seguridad, seguridad de la información y seguridad informática
La seguridad de la información, la triada CID, vulnerabilidad, amenaza, incidentes, relación entre vulnerabilidad, amenaza e incidente, incidente informático versus incidente de seguridad informática, riesgos en seguridad informática
Unidad II: Gestión del incidente
- Desarrollo de capacidades del Estado en un nuevo contexto, Taxonomía CERT, Taxonomía CSIRT, criticidad de un incidente, el ciclo de vida de la gestión y respuesta a un incidente de seguridad, estados de un incidente, protocolo de semáforos.
Unidad III: Estándares y buenas prácticas en seguridad de la información
- ¿Qué es un estándar?, ¿Qué es una buena práctica?, Estándares de seguridad de la información, Beneficios de implementar estándares de seguridad en los organismos públicos, requisitos mínimos de seguridad de la información para organismos del sector público Nacional, autenticación; autorización, y control de acceso, gestión de incidentes de seguridad, aspectos, de seguridad para la continuidad de la gestión, adhesiones de diversos organismos a los requisitos mínimos.
Unidad IV: ¿Qué hacer ante un incidente?
- Recomendaciones para prevenir un incidente, recomendaciones generales, métodos de recolección de información

Estrategias metodológicas y recursos didácticos

La estructura del curso comprenderá tanto cuestiones de explicación narrativa, como diversos ejemplos prácticos que pueden presentarse como situaciones habituales de cualquier entorno de trabajo, en las áreas específicas de los diversos temas abordados. Además, se trabajará con datos e información verídica, que ayuden a la reflexión y entendimiento de la gestión de incidentes, prevención y protección de los sistemas, abordados a través de casos reales donde los participantes puedan sacar conclusiones propias e informarse para la creación o mejora de los procesos involucrados.

Actividades introductorias
Presentación del curso y guía del participante

Actividades de desarrollo
Con estas actividades se espera
- Reconocer y entender las diferencias de un incidente de seguridad informática
- Dotar a los participantes de métodos, buenas prácticas e información que garantice la correcta gestión de los incidentes de seguridad informático
- Impulsar al interés de los participantes por crear, mejorar y/o actualizar los procedimientos que brindan resiliencia, prevención y protección de los sistemas
- Crear conceptos que logren estimular a los participantes sobre la reflexión de la importancia del desarrollo y mejora los temas abordados, en el ámbito de sus competencias, Estas actividades serán cuestionarios de autocomprobación y los participantes cuentan con intentos ilimitados.

Actividades de integración
Con este cuestionario final se espera afianzar los conocimientos adquiridos de todos los temas abordados. Para resolverlo los participantes cuentan con 3 intentos.

Descripción de la modalidad

Virtual Autogestionado

Bibliografía

Norma ISO 27001 / Gestión de incidentes informáticos.

ITIL (Information Technology Infraestructure Library) v3 / Gestión de incidentes de la información.

LACNIC - Manual básico de Gestión de Incidentes de Seguridad Informática para América Latina y Caribe Proyecto AMPARO. (Cap.2 Modelos organizacionales de centros de respuesta de incidentes).

Evaluación de los aprendizajes

Evaluación del proceso: cuestionarios auto administrados al finalizar cada una de las unidades.

Evaluación del producto: cuestionario de autocomprobación de lectura

Instrumentos para la evaluación

Cuestionario de respuestas de selección múltiple, verdadero y falso.

Requisitos de Asistencia y aprobación

Aprobar la totalidad de los cuestionarios con al menos un 60% de respuestas correctas.

Duración (Hs.)

7

Detalle sobre la duración

7 horas disponible en plataforma durante dos semanas.

Lugar

Campus virtual INAP

Perfil Instructor

Bolino Patricio Emilio

Licenciado en Informática con experiencia en el área de la Ciberseguridad

Origen de la demanda

INAP- Dirección Nacional de Ciberseguridad de la Secretaría de Innovación Pública.

Prestadores Docentes

CUIT/CUIL	APELLIDO Y NOMBRE
	ACTIVIDAD,AUTOADMINISTRADA