SISTEMA NACIONAL DE CAPACITACION
DISEÑO DE LA ACTIVIDAD

Nombre

GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES

Código INAP IN36377/21 ***Estado*** Activo

Programa)Campos de Práctica ***Área***)TIC Aplicadas a la Gestión

Fundamentación

Propósito: Actualización o sensibilización

El uso creciente de Internet y de las Tecnologías de la Información y las Comunicaciones, comenzado a mediados de la década del 90’ con la apertura comercial de la red por parte del gobierno de los Estados Unidos, permitió optimizar y mejorar la gestión y administración de los organismos públicos y privados.
No obstante, esa evolución tecnológica trajo aparejados riesgos, delitos informáticos, que pueden comprometer la seguridad de las personas, los dispositivos -como computadoras, tablets, celulares, etc- y/o la información que contienen los mismos.
Por tal motivo, resulta fundamental capacitar a las distintas organizaciones en materia de ciberseguridad, para que adquieran conceptos y contenidos centrales que les permitan detectar, mitigar y gestionar los riesgos que puedan afectar la seguridad de la información, es decir, su confidencialidad, integridad y disponibilidad.
En ese marco, la Dirección Nacional de Ciberseguridad de la Secretaría de Innovación Pública propone el presente curso, que contiene un abordaje temático atravesado por la seguridad de la información, la gestión de incidentes informáticos y auditorías en ciberseguridad, con el propósito de introducir a las y los participantes, al mundo de los riesgos del ciberespacio y sus consecuencias, como también, a las herramientas y/o mecanismos para mitigar los mismos.

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 que los y las participantes adquieran al finalizar el curso:
- Una comprensión básica de los riesgos que acompañan el aprovechamiento de las tecnologías de la información y las comunicaciones.
- Nociones sobre el proceso de gestión de incidentes y el rol que les compete.
- El entendimiento de la función de auditoría y su valor para la mejora del ambiente de control en un entorno de uso masivo

y exhaustivo de Internet y las redes informáticas.

Perfil del participante

La actividad está dirigida a todos los trabajadores y trabajadoras de la Administración Pública Nacional que fueron designados como Puntos Focales de Ciberseguridad.

Objetivos

Que las y los participantes logren:
- Comprender que el uso de Internet trae aparejada la necesidad de adoptar medidas de seguridad para la protección personal y de los recursos que la organización nos asigna para llevar adelante las tareas.
- Reconocer los principales tipos de auditorías en materia de ciberseguridad para poder Interactuar con los equipos de auditoría informática, respondiendo adecuadamente a los requerimientos que formulen en materia de seguridad de la información.
- Comprender conceptos introductorios sobre gestión de incidentes, para poder participar en el proceso de gestión, de ser requerido.

Contenido

Módulo 1: Introducción a la seguridad de la información

- Seguridad de la Información: ¿por qué debería importarnos?
- Qué es la seguridad de la información.
- Propiedades: confidencialidad, integridad y disponibilidad.
- Concepto de amenaza, vulnerabilidad y riesgo.
- Componentes: procesos, personas y tecnología.
- El recurso humano: clave para proteger mejor la información.
- Gestión de la seguridad de la información en la organización.

Módulo 2: Gestión de incidentes informáticos

- Introducción a la gestión de incidentes
- Ciclo de vida en la gestión de incidentes
- Clasificación y priorización
- Cooperación y comunicación

Módulo 3: Auditorías de ciberseguridad

Conceptos fundamentales de las auditorías
- Tipos de auditoria:

De cumplimiento: auditorías que verifican el cumplimiento de un determinado estándar de seguridad.
Técnicas: auditorías o revisiones de seguridad técnica cuyo alcance está acotado a un sistema o sistemas informáticos objeto de la revisión.
Forense
Aplicaciones web
Control de acceso físico
Networking
- Normas y Framework de Ciberseguridad
- Gobernabilidad, Riesgo y Cumplimiento
- Gestión del riesgo

Estrategias metodológicas y recursos didácticos

Durante los encuentros sincrónicos, se realizarán exposiciones sobre los fundamentos teóricos de los temas incluidos en cada unidad temática. Se plantearán casos referidos a los mecanismos a adoptar en cuanto a la protección de la información y preguntas disparadoras que den lugar al debate, para que las y los participantes puedan dar cuenta de sus opiniones, reflexiones, análisis; sobre la gestión de la seguridad de la información en las organizaciones, y su relación con las tareas desarrolladas en sus puestos de trabajo.
Al finalizar la cursada, deberán realizar una actividad final, integradora de los contenidos centrales abordados a lo largo de los encuentros.

Descripción de la modalidad

Virtual sincrónica

Bibliografía

Módulo 1
Qué es la Seguridad Informática – Hugo Scolnik – Editorial Paidós, 2014.
ISO/IEC 27001:2013 – Tecnologías de la Información – Técnicas de Seguridad – Sistemas de Gestión de la Seguridad de la Información – Requisitos.
ISO/IEC 27002:2013 – Tecnologías de la Información – Técnicas de Seguridad – Código de buenas prácticas para la Gestión de la Seguridad de la Información.

Módulo 2
España. (2020). Esquema Nacional de Ciberseguridad. Gestión de ciberincidentes. Centro Criptológico Nacional.
Estados Unidos. (2012). NIST SP 800-61 - Computer Security Incident Handling Guide.
ISO/IEC. (2016). ISO/IEC 27035 - information security (cybersecurity) incident management.
LACNIC. (2012). Manual Básico de: Gestión de incidentes de seguridad informática. Uruguay.
López Lio, R. (2015). Ciberdefensa e infraestructuras críticas. CEFA Digital.

Módulo 3
ISO/IEC 17021 Requisitos para los organismos que realizan la auditoría y la certificación de sistemas de gestión.
ISO/IEC 27001 Es un estándar para la seguridad de la información aprobado y publicado como estándar internacional en octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission.
ISO 9001:2015 Elaborada por la Organización Internacional para la Estandarización, determina los requisitos para un Sistema de Gestión de la Calidad.

Evaluación de los aprendizajes

De proceso: Se realizará en forma continua a lo largo de la cursada. Se valorarán los intercambios realizados por las y los participantes en los espacios de debate.

De producto: Al finalizar el tercer encuentro y a modo de integración final, las y los participantes deberán resolver un cuestionario de respuestas múltiple choice.

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

Asistir a los tres encuentros virtuales sincrónicos que conforman el curso.
Realizar y aprobar el cuestionario de integración con el 70% de respuestas correctas.

Duración (Hs.)

6

Detalle sobre la duración

6 horas distribuidas en tres encuentros virtuales sincrónicos de dos horas de duración cada uno.

Lugar

Plataforma de videoconferencias CISCO Webex
Campus virtual INAP.

Perfil Instructor

Especialistas en Seguridad informática de la Dirección Nacional de Ciberseguridad.
María Patricia Prandini.
Rodrigo López Lío.

Guillermo Ranucci.

Origen de la demanda

Dirección Nacional de Ciberseguridad.

Secretaría de Innovación Pública.

Prestadores Docentes

CUIT/CUIL	APELLIDO Y NOMBRE
23135307564	PRANDINI,MARIA PATRICIA