SISTEMA NACIONAL DE CAPACITACION
DISEÑO DE LA ACTIVIDAD

Nombre

BUENAS PRÁCTICAS DE CIBERSEGURIDAD

Código INAP IN38819/23 ***Estado*** Activo

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

Fundamentación

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

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.

Hoy en día, Internet y las Tecnologías de la Información y las Comunicaciones son herramientas fundamentales para el funcionamiento de cualquier organización, incluyendo las instituciones gubernamentales, ante lo cual, para evitar riesgos en la información que gestionan, deben utilizarse de forma adecuada.

Para ello se debe considerar a la información como un activo más, es decir, como otros bienes y servicios requeridos para cumplir con los objetivos de la organización.
La información puede presentarse en diversos formatos y soportes, como papel, archivos, registros, pen drive, discos duros, etc. Y, sin importar cuáles sean estos, debe estar protegida desde su creación, durante su ciclo de vida y hasta su destrucción, desuso o archivo definitivo.

En este sentido, es indispensable pensar que la información puede ser objeto de peligros, amenazas y usos indebidos e ilícitos, por lo tanto, se deben extremar las medidas de seguridad para preservarla.

Por tal motivo, se vislumbra como necesario y urgente que el personal de la Administración Pública Nacional, recurso central en las organizaciones, se capacite en materia de ciberseguridad, para la toma de conciencia, desarrollo de habilidades y construcción de conocimientos en seguridad de la información. Así, se espera que logren hacer un uso responsable de la información y de los recursos usados en su gestión para prevenir riesgos.

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 este espacio formativo le permita a las/os participantes construir conocimientos básicos, centrales, respecto a la seguridad de la información para así, generar en el ámbito laboral buenas prácticas de ciberseguridad vinculadas con la protección de la información que producen, gestionan y almacenan.

Perfil del participante

Agentes de la Administración Pública Nacional sin conocimientos en ciberseguridad

Objetivos

Que los participantes logren:
- Comprender los conceptos teóricos centrales sobre seguridad de la información.
- Identificar los riesgos y las amenazas que pueden afectar a la seguridad de la información en el ciberespacio.
- Adoptar medidas de protección para reducir y mitigar el impacto de posibles daños en los activos de información del Estado.
- Aplicar medidas de protección al compartir información personal en Internet.

Contenido

Módulo 1: Seguridad en Internet
Mundo real: espacio físico+espacio virtual (medidas de seguridad)
La importancia de la identidad digital
Qué es la privacidad
Suplantación de identidad en redes sociales

Módulo 2: Seguridad de la información
Qué es la Seguridad de la información
Amenazas más comunes a las que está expuesta la información
Consejos para determinar salvaguardas
Ejemplos de seguridad de la información según el sector

Módulo 3: Seguridad contra hackers
Qué es software malicioso
La ingeniería social
La importancia de la actualizaciones de seguridad
Consejos para realizar copias de seguridad

Módulo 4: Seguridad en el puesto de trabajo

Contraseñas seguras
Medidas de protección para el trabajo remoto
Uso seguro del correo electrónico
La importancia de los controles de acceso

Estrategias metodológicas y recursos didácticos

El curso fue elaborado para dictarse en cuatro encuentros que se realizarán una vez por semana, mediante la modalidad virtual sincrónica. En cada uno de ellos, se expondrán los contenidos temáticos de cada unidad con el apoyo de presentaciones de Power Point, videos o gráficos. A su vez, los participantes podrán complementar los contenidos trabajados con material de lectura que tendrán a disposición en el aula virtual.
En los encuentros, las y los asistentes compartirán sus saberes, ideas preliminares y experiencias que servirán de anclaje para la construcción de los nuevos conocimientos; intervendrán en espacios de debates propuestos por la docente con el objetivo de analizar las temáticas tratadas.
A modo de integración analizarán situaciones frecuentes y revisarán sus propias prácticas para detectar riesgos y evaluar las medidas de protección necesarias a aplicar.

Descripción de la modalidad

Virtual sincrónico

Bibliografía

-Oficina de seguridad del internauta. En Internet, cuida tu privacidad.
(https://www.osi.es/es/tu-informacion-personal)

-Willistowerswats. Medidas para proteger la identidad digital de los trabajadores.
(https://willistowerswatsonupdate.es/ciberseguridad/proteger-identidad-digital/)

-Web escuela. Los principios de persuasión de Cialdini.
(https://webescuela.com/principios-persuasion-cialdini/#:~:text=Seg%C3%BAn%20los%20principios%20de%20la,Tendemos%20a%20dar%20cuando%20recibimos).

-Plazi. Datos de la ingeniería social. (https://platzi.com/clases/2238-ingenieria-social/37058-datos-de-la-ingenieria-social/)

-Viewnext. Técnicas de ingeniería social.
(https://www.viewnext.com/tecnicas-de-ingenieria-social/)

-Academia Eset. Navegación segura.
(https://www.academiaeset.com/default/store/158600-navegacion-segura)

-Oficina de seguridad del internauta. Suplantación de identidad y secuestro de cuentas. (https://www.osi.es/es/actualidad/blog/2021/02/05/suplantacion-de-identidad-y-secuestro-de-cuentas-como-actuar)

-Instituto Nacional de Ciberseguridad de España. Protección de la información. (https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-de-la-informacion.pdf)

Evaluación de los aprendizajes

Evaluación de proceso: tendrá lugar durante los encuentros pautados y se realizará a partir de las intervenciones que realicen las y los participantes en los espacios de intercambio y debate propuestos.
Evaluación de producto: consistirá en analizar situaciones presentadas en los encuentros y la aplicación de medidas de protección necesarias.

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

Asistir al 80% de los encuentros sincrónicos.
Participar en los espacios de intercambio propuestos.
Realizar y aprobar las actividades promovidas.

Duración (Hs.)

10

Detalle sobre la duración

Cuatro encuentros virtuales sincrónicos de dos horas y media de duración cada uno.

Lugar

Plataforma Cisco Webex
Campus virtual de INAP

Perfil Instructor

Especialista en la materia

Origen de la demanda

INAP - Dirección Nacional de Ciberseguridad.

Prestadores Docentes

CUIT/CUIL	APELLIDO Y NOMBRE
27228591950	GARNICA,NANCY EVA