SISTEMA NACIONAL DE CAPACITACION
DISEÑO DE LA ACTIVIDAD

Nombre

SEGURIDAD DE LA INFORMACIÓN: CONCEPTOS FUNDAMENTALES

Código INAP IN28570/18 **Estado** Activo

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

Fundamentación

La información es uno de los activos de mayor importancia para las organizaciones, entre las El presente curso se enmarca en la estrategia de capacitación diseñada SUBSECRETARÍA DE TECNOLOGÍAS Y CIBERSEGURIDAD dependiente del MINISTERIO DE MODERNIZACIÓN, en colaboración con el Instituto Nacional de la Administración Pública y el Proyecto de Modernización del Estado.

Uno de los principales objetivo de la subsecretaria es establecer prioridades y planes estratégicos para liderar el abordaje de la ciberseguridad en el Sector Público Nacional Asimismo, la subsecretaria tiene entre sus objetivos primordiales la promoción de la toma de conciencia de los integrantes de las organizaciones de gobierno y del público en general en relación con los riesgos que acarrea el uso de medios digitales en el Sector Público Nacional, así como del rol compartido entre el sector público y el privado para el resguardo de la infraestructura crítica.

Debido a que la información tiene un gran valor para los Organismos, es susceptible a pérdidas, alteraciones o divulgación no autorizada. Para evitar que esto ocurra, y conlleve efectos adversos al Organismo, es necesario gestionar la seguridad de dicha información. La seguridad de la información es una disciplina que busca garantizar su confidencialidad, integridad y disponibilidad mediante la implementación de controles. Las personas, como se dijo, son uno de los componentes que gestionan la información. Hay una frase que dice que la seguridad es una cadena que se rompe por el eslabón más delgado, las personas. Esto se debe a que, por más controles técnicos que se implementen para proteger la información, si las personas que la gestionan no se comportan adecuadamente en el tratamiento de la información, la misma se encontrará expuesta a incidentes que atentan contra su seguridad.
Es por ello que resulta vital la concientización continua de las personas sobre los riesgos a los cuales se expone la información de su Organismo, así como las formas de protegerla. En general se enfoca a modificar la conducta de las personas para que el manejo que hacen de la información en el ejercicio de sus funciones sea más seguro.

Contribución esperada

Se espera que este curso brinde competencias y herramientas a los empleados de los Organismos acerca de la importancia de proteger la información que manejan de los diversos riesgos de seguridad a los cuales se expone. Asimismo fomente la implementación de “buenos prácticas” a llevar a cabo diariamente con relación a sus

estaciones de trabajo, información recibida, información remitida, etc.
De esta forma se busca elevar el nivel de seguridad de la información de los Organismos previniendo incidentes que puedan ocasionar la divulgación, corrupción o pérdida de información y de equipamiento informática.

Perfil del participante

Empleados de organismos de la APN. No se requieren conocimientos previos en seguridad de la información.

Objetivos

Se espera que al finalizar el curso los participantes sean capaces de:
Comprender conceptos elementales vinculados a la seguridad de la información.
Conocer y comprender los riesgos existentes en la gestión de la información, tanto utilizando herramientas tecnológicas como manuales, los cuales pueden comprometer su confidencialidad, integridad y/o disponibilidad.
Incorporar buenas conductas en la actividad laboral, que permitan proteger la información que se gestiona.

Contenido

El contenido del curso se estructura a partir de situaciones habituales que pueden generar incidentes para la seguridad de la información como por ejemplo, el uso de contraseñas y la solicitud de datos confidenciales (phishing). A partir del análisis de los casos, se desarrollan los siguientes temas:

Módulo 1: Conceptos básicos
Fundamentos de la seguridad de la información.
Riesgos para la seguridad de la información.
Estrategias de ataque: Ingeniería social, ingeniería de datos y ataques a contraseñas.
Políticas de seguridad de la información.

Módulo 2: Contraseñas. Riesgos y recomendaciones
Control de acceso lógico a los sistemas de información.
Características de una contraseña segura.
Recomendaciones para la elección de contraseñas.
Recomendaciones para el uso de contraseñas.
Buenas prácticas: Escritorios y pantallas limpios.

Módulo 3: Uso responsable del correo electrónico
Correo electrónico: conceptos fundamentales.
Dominios de Internet.
Redes sociales.
Mensajes no solicitados: Spam.
Phishing.

Recomendaciones para evitar ser víctima de phishing.

Estrategias metodológicas y recursos didácticos

Con el fin de alcanzar los objetivos de aprendizaje propuestos, las estrategias metodológicas se centran en actividades de distinto tipo y nivel de complejidad que los participantes deben completar a lo largo del curso.
Las actividades introductorias se orientan a que los participantes se familiaricen con los diferentes recursos y herramientas del entorno virtual de modo que se sientan más afianzados en las cuestiones operativas. Se desarrollan en espacios de intercambio en el entorno virtual.
Las actividades de desarrollo se corresponden con cada unidad de contenidos y están organizadas en secuencias. Son de distinto tipo: autoevaluaciones, elaboración de trabajo práctico individual a partir de la lectura comprensiva de los materiales del curso y reflexiones sobre distintas cuestiones relacionadas con la aplicación de los contenidos en el propio entorno laboral.
Se prevé la participación en foros y espacios de interacción entre cada participante y el tutor y entre los participantes entre sí, con el objetivo de promover la construcción colectiva de conocimientos.
La actividad final permite integrar los aprendizajes a partir de una consigna de trabajo, que requiere el reconocimiento de aspectos de la seguridad de la información que se relacionan directamente con las tareas a cargo. Se trata de una elaboración personal que pueda ser aprovechada en el ámbito laboral.
En todas estas actividades los participantes ponen en práctica los conceptos y metodologías desarrolladas en el curso.
Teniendo en cuenta que se trata de una capacitación a distancia, los participantes y tutores cuentan con un entorno virtual especialmente diseñado para la capacitación.
Las actividades serán coordinadas, supervisadas y evaluadas por el tutor.
El tutor utilizará los recursos disponibles en la plataforma para generar espacios de intercambio, debates y otras formas de actividad entre los participantes, que permitan conocer las opiniones, dificultades y dudas, y trabajar en torno de ellas.
El tutor es un especialista en los contenidos del curso al que los participantes podrán recurrir cada vez que lo necesiten.
El entorno cuenta con los siguientes espacios y recursos:
- Materiales de estudio elaborados especialmente para el curso: contenidos en formato PDF, con el desarrollo integral de los temas de cada unidad.
- Lecturas y bibliografía recomendada.
- Espacios de participación e interacción: un espacio para el tutor, desde el cual se coordina la actividad del grupo, indica actividades, resuelve dudas y consultas, publica información relevante y orienta a los participantes en el proceso de capacitación virtual; un foro para las presentaciones personales y foros para la participación y consultas de los participantes.
- Mesa de ayuda: para solicitar asistencia ante cualquier problema técnico vinculado con el uso o acceso a la plataforma.
- Acceso a sitios webs relacionados: son accesos a las páginas de Internet que ofrecen contenidos relacionados con las temáticas del curso.
-Los participantes podrán acceder a la plataforma cuando lo requieran en función de sus necesidades (sin un compromiso de horario específico) y orientados por el cronograma de estudio previsto.

Descripción de la modalidad

Virtual

Bibliografía

ICIC. (2014). Guía práctica sobre el uso de contraseñas.
ICIC. 82014). Recomendaciones para el uso seguro del correo electrónico en los organismos de la APN.
Artículos de divulgación general.
Noticias y casos de la vida real.
ICIC. (2014). Recomendaciones para evitar ser víctima del “phishing”
Sitios especializados: www.internetsano.gob.ar

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 se pretende promover. El seguimiento es posible a través de las intervenciones, aportes y opiniones que elaboren y envíen los participantes.

Autoevaluaciones en línea, 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.

Autoevaluación final integradora en línea de respuesta automática. Se integran todos los conceptos volcados en el curso.

Trabajo final: Se plantea una consigna final para que los alumnos realicen un trabajo práctico de desarrollo el cual será evaluado por los docentes.

Instrumentos para la evaluación

Informes de la plataforma.
Consignas para desarrollar.
Ejercicios de autoevaluación en el entorno virtual para cada unidad.
Ejercicio de autoevaluación integrador de todo el proceso.
Trabajo práctico final.
Encuesta virtual.

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 webs relacionados con el curso.

Para la aprobación del curso será necesario obtener una calificación de, al menos, el 70% en las actividades de autoevaluación -ponderación en forma automática por parte de la función específica de la plataforma- y cumplir con todas las actividades propuestas por el docente, incl

Duración (Hs.)

45

Detalle sobre la duración

Cuatro semanas.

Lugar

Campus virtual INAP.

Perfil Instructor

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

Origen de la demanda

Oferta INAP

Prestadores Docentes

CUIT/CUIL	APELLIDO Y NOMBRE
27252515890	GALAN,MARIANA