SISTEMA NACIONAL DE CAPACITACION
DISEÑO DE LA ACTIVIDAD

Nombre

NUEVOS DESAFÍOS PARA LA SEGURIDAD INFORMÁTICA

Código INAP IN36011/21 ***Estado*** Activo

Programa)Actividades Transversales ***Área***)TIC Aplicadas a la Gestión

Fundamentación

Propósito: Actualización.
Las tecnologías de la información, la seguridad, la integridad de la información y los propios ciudadanos afrontan hoy un reto tan difícil como urgente: entender y adaptarse a los nuevos riesgos y desafíos que cada día se van generando junto con la dinámica tecnológica. Esta actividad se propone aportar herramientas para poder utilizar las tecnologías, minimizando los riesgos personales y los que pueden generarse en el ámbito laboral.
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 y saber qué hacer.

Contribución esperada

Se espera que los participantes comprendan los riesgos y los desafíos que involucra el uso de las TIC y que adquieran herramientas que les permitan aplicar saberes y hábitos responsables para enfrentar amenazas habituales y advertir acerca de la importancia del cuidado de la información de las organizaciones.
Se espera asimismo, que reconozcan las últimas amenazas que han surgido en internet, que comprendan su funcionamiento y sus posibles remediaciones.

Perfil del participante

Personal de la Administración pública nacional, con independencia de las tareas que realiza.

Requisitos: Los participantes deberán tener acceso a internet y una dirección de correo electrónico.

Objetivos

Se espera que, al finalizar el curso, los participantes sean capaces de:

- comprender conceptos vinculados a la seguridad de la información y a los nuevos desafíos que van surgiendo con el paso del tiempo y los avances tecnológicos;

- reflexionar sobre las implicancias de ciertas prácticas que pueden afectar la información tanto personal como de las organizaciones a las que pertenecen;

- experimentar prácticas responsables con ciertas herramientas informáticas de uso habitual.

- proteger la información laboral y

- promover el buen uso de las tecnologías en sus ámbitos de trabajo.

Contenido

Módulo I: Dispositivos Móviles y Computación en la Nube
Ventajas y riesgos de seguridad en el uso de dispositivos móviles.
Medidas de seguridad en dispositivos móviles
Conceptos básicos de la computación en la nube
Riesgos de seguridad.
Experiencias en el mundo.

Módulo II: Últimos Desafíos y Amenazas a la Seguridad
Ransomware.
Malware sin archivos.
Troyanos financieros.
Ataques a programas en la nube y proveedores.
Noticias falsas.

Estrategias metodológicas y recursos didácticos

Se trabajará con :
- revisión de las ideas y conocimientos previos.
- apropiación y uso de nuevos saberes.
- análisis y la revisión de las propias prácticas.

La estrategia incorpora diferentes técnicas y propuestas de actividades:
- foros de debate, intercambio y análisis;
- consignas en cada ocasión de apertura;
- seguimiento y devoluciones;
- devoluciones evaluativas generales y comentarios individuales;
- intercambios mediante foros, para responder dudas o realizar devoluciones particulares para cada participnate;

- ficha de contenidos y actividades;
- análisis y resolución de casos.

Recursos didácticos
- Selección de bibliografía.
- Videos disponibles en las unidades como material disparador para responder en los foros de debate.
- Internet: links a sitios y documentos de interés.
- Recursos de la plataforma educativa: foros de discusión, páginas webs sugeridas, anuncios del tutor, mensajería interna, propuesta de actividades, bases de datos, etc.

Descripción de la modalidad

Virtual tutorado.

Bibliografía

Diferentes sitios de organismos de nuestro país y del exterior que comparten material de concientización.
Sitios webs oficiales del Estado nacional
Sitios webs de diferentes organismos públicos.
Diferentes sitios webs con noticias y documentos vinculados a la temática.

Evaluación de los aprendizajes

Evaluación de proceso: se evaluarán las diferentes producciones parciales de los participantes, las que serán presentadas a través de diferentes recursos de la plataforma.

Evaluación de producto: A partir de dos situaciones dadas por el docente, los participantes deberán relacionar los conceptos fundamentales trabajados en el curso y recomendar, de acuerdo con las prácticas internacionales, qué estrategias aplicarían para preservar la seguridad y las infraestructuras críticas.

Criterios de evaluación:
- Análisis de la situación: 50%.
- Propuesta de solución: coherencia 25% y aplicabilidad 25%.

Instrumentos para la evaluación

Instrumentos para la evaluación de los aprendizajes
- Informes de la plataforma.
- Guía para la elaboración del trabajo práctico final integrador y grilla para su evaluación.

Instrumentos para la evaluación de la actividad
- Encuesta de satisfacción del participante, de resolución en línea.

Requisitos de Asistencia y aprobación

Entrega de las actividades de proceso y de producto en tiempo y forma, con ajuste a los criterios de evaluación formulados.

Duración (Hs.)

12

Detalle sobre la duración

12 horas distribuidas en 3 semanas.

Lugar

Campus virtual INAP

Perfil Instructor

Especialistas en la temática.

Origen de la demanda

Dirección Nacional de Ciberseguridad.

Prestadores Docentes

CUIT/CUIL	APELLIDO Y NOMBRE
27252515890	GALAN,MARIANA