SISTEMA NACIONAL DE CAPACITACION
DISEÑO DE LA ACTIVIDAD

Nombre

ABORDAJE INTEGRAL DE CIBERSEGURIDAD

Código INAP IN41143/24 ***Estado*** Activo

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

Fundamentación

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

Hablar de ciberseguridad implica describir un conjunto de políticas, estrategias y acciones orientadas a elevar los niveles de seguridad de las personas frente a incidentes y delitos que tengan como medio o fin un dispositivo informático, es decir, a un aparato capaz de procesar en forma automática datos e información.
La ciberseguridad está atravesada por dos ejes centrales: los incidentes de seguridad y los delitos informáticos. Los primeros pueden afectar la confidencialidad, integridad y disponibilidad de la información, que está almacenada en dispositivos informáticos como computadoras, tablets, smartphones, cámaras fotográficas, filmadoras digitales, smart TVs y consolas de videojuegos, entre otros.
El área que se ocupa de mitigar estos incidentes es la seguridad informática, y la que aborda y trata los delitos informáticos se conoce como cibercrimen.
Por su parte, la Organización de las Naciones Unidas (ONU), afirma que la seguridad humana exige respuestas centradas en las personas, adaptadas a cada contexto, orientadas a la prevención y que refuercen la protección y el empoderamiento de todas las personas y todas las comunidades.
Siguiendo la misma línea de pensamiento que la ONU, se puede decir que la ciberseguridad es un concepto amplio que va más allá de la seguridad informática de la información, almacenada en dispositivos, softwares y hardwares. Centra su eje principal en la seguridad de las personas y en tratar de prevenir actos disvaliosos, que afecten sus derechos, y puedan atentar contra la libertad, la integridad física y la propiedades de las mismas. Estos eventos de impacto negativo obedecen -en algunos casos- a fallas y actitudes irresponsables o malintencionadas, pero también ocurren por falta de conocimientos.
Teniendo en cuenta que, en las últimas décadas, las tecnologías de la información redefinieron la forma de vinculación entre los organismos que las componen y la ciudadanía, y que la mayoría de la población mundial se presenta como un usuario intensivo de Internet, saber conceptos de ciberseguridad se considera muy importante para la sociedad de la información, en la que vivimos hoy. En este sentido, debido a que la realidad actual plantea un fuerte desafío para el personal que se desempeña en organizaciones de todo tipo, donde pueden surgir vulnerabilidades o incidentes informáticos, la Dirección Nacional de Ciberseguridad desarrolló la presente capacitación, con el objetivo de habilitar un

espacio de actualización en materia de ciberseguridad, es decir, en la seguridad de la información, los delitos informáticos y la seguridad de las personas. Este espacio de formación, propone brindar herramientas que le permita al personal proteger la información laboral y personal, conocer los delitos informáticos más actuales y sus leyes, conocer y proteger los datos personales, y detectar en la web acciones violentas.

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 qué hacer (saberes de situación relacionados con la capacidad de tomar decisiones en situaciones y contextos específicos) – Saber reflexionar (saberes relacionados a la capacidad de volver el pensamiento sobre objetos, situaciones, hechos, creencias, etc).

Contribución esperada

Se espera al finalizar la capacitación, que los participantes cuenten con los conocimientos centrales en materia de Ciberseguridad que les permitan identificar y prevenir vulnerabilidades e incidentes informáticos, para así, disminuir los riesgos en la gestión de la información al interior de las organizaciones públicas.

Perfil del participante

Personal de la Administración Pública Nacional

Objetivos

Que los participantes logren:
Comprender conceptos básicos de ciberseguridad.
Adquirir una visión actualizada de la legislación vigente de los delitos informáticos y de las normas actuales en materia de ciberseguridad del Sector Público Nacional.
Conocer las funciones de la Dirección Nacional de Ciberseguridad y del CERT.
Distinguir acciones y conductas violentas en entornos digitales
Prevenir los principales delitos informáticos que se cometen contra los niños y adolescentes en entornos virtuales.
Comprender nociones introductorias de la investigación criminal de los delitos informáticos.
Identificar la importancia de la protección de los datos personales.
Prevenir vulnerabilidades e incidentes informáticos.

Contenido

Unidad 1: Derecho en materia de ciberseguridad
Presentación y funciones de la Dirección Nacional de Ciberseguridad.
Comité de Ciberseguridad.
Programa Nacional de Infraestructuras Críticas.
Funciones del CERT.
Convención de Budapest sobre cibercrimen.

Ley de Delitos Informáticos N° 26.388.
Artículo 131 del Código Penal argentino: grooming.

Unidad 2: Seguridad informática
Seguridad de la Información: ¿por qué debería importarnos?
Qué es la seguridad de la información.
Propiedades: confidencialidad, integridad y disponibilidad.
Perspectivas: seguridad física y lógica.
Concepto de amenaza, vulnerabilidad y riesgo.
El recurso humano: una clave para proteger mejor la información.
Gestión de la seguridad de la información

Unidad 3: Protección de datos
Finalidad y objetivos de los datos personales
El derecho a la intimidad en la Constitución Nacional
El valor de la privacidad y los datos personales en la economía del conocimiento.
La legislación argentina- obligaciones y responsabilidades en la gestión de bases de datos
Responsabilidad del Estado y el sector privado.
Argentina en el contexto internacional de la protección de datos
Homologación con la UE.
Tráfico transfronterizo de datos.
Debates pendientes hacia una actualización de la norma vigente.

Unidad 4: Violencia en entornos digitales
- Características de la violencia digital
Concepto de violencia digital
Escenarios donde se manifiesta esa violencia
El impacto de las TICs en la violencia
- Tipos de violencia en línea:
Cibercontrol
Difusión no consentida de imágenes
Doxxing
La suplantación y el robo de la identidad
Daños a la imagen y a la reputación
Vigilancia y monitoreo
Ciberhostigamiento o ciberacecho

Ciberacoso
Ciberbullying
Extorsión y Amenazas
Violencia física mediante las TICs
Abuso y explotación por medio de las TICs

Unidad 5: Delitos contra la integridad sexual de niños y adolescentes en intornos digitales
Abuso sexual contra niños y adolescentes. Pedofilia y Pederastía.
Indicadores de abuso sexual e indicadores asociados a las nuevas tecnologías.
Nueva modalidad de acoso y abuso: grooming.
Sexting, Sextorsión y Porno-venganza.
Proyecto de Ley sobre publicación no consentida de material íntimo.
Material de abuso/explotación sexual contra niños y adolescentes (pornografía infantil).
La importancia de la denuncia.
Ley Mica Ortega y su aplicación. Prevención y sensibilización.

Unidad 6: Informática forense
Investigación Criminal de los delitos informáticos
Informática Forense.
Evidencia Digital.
Principios Forenses.
Protocolos y Guías de Buenas Prácticas en el tratamiento de la evidencia digital nacionales e internacionales.

Estrategias metodológicas y recursos didácticos

El curso se estructurará alrededor de seis clases (una clase por semana), que se impartirán bajo la modalidad virtual sincrónica. En cada encuentro, se se realizarán exposiciones de los contenidos correspondientes a cada unidad temática, a partir de diferentes recursos utilizados por las docentes, como videos, gráficos y/o presentaciones de Power Point. Los participantes contarán con materiales de lectura en el aula virtual que complementarán las exposiciones realizadas por las docentes.
Durante el desarrollo del curso, los participantes intervendrán en los debates propiciados por las docentes en cada encuentro, con el objetivo de contextualizar, analizar y valorar las temáticas tratadas en sus propios espacios laborales; y lograr establecer relaciones significativas entre las mismas y las tareas que desarrollan en sus puestos de trabajo. A modo de integración, realizarán actividades con el fin de analizar e integrar los conceptos centrales trabajados.

Descripción de la modalidad

Virtual sincrónica

Bibliografía

Seguridad Informática

Qué es la Seguridad Informática – Hugo Scolnik; Editorial Paidós, 2014
Factor Humano: el talón de Aquiles de la Seguridad I: la percepción del valor de la información – Sara Bursztein; Disponible en: https://www.magazcitum.com.mx/?p=2735#.YAsqNBbQ82w – 2014

Delitos contra la integridad sexual de niños y adolescentes

Código Penal, delitos contra la integridad sexual; Vicisitudes del proceso de sexuación: importancia médico-legal; Juan Carlos Romi.
El trauma de la irrupción de la sexualidad adulta en el universo infantil.” Eva Giberti. Síntesis del trabajo leído el día 29 de Junio de 2007 en el Congreso Internacional de Estrés Postraumático. Editado en su totalidad en la Revista especializada en Estrés Postraumático.
Vínculos adolescentes atravesados por la virtualidad.” Cristina Blanco y Norma Brea. Revista Actualidad Psicológica, junio 2019.
La construcción de la subjetividad adolescente en la era digital; Mag. Silvia A. Lastra, Lic. Graciela Saladino y Lic. Elena Weintraub
Algunas reflexiones sobre la pedofilia y el abuso sexual de menores; Juan Carlos Romi y Lorenzo García Sanmartino
Ley 26.904
Grooming.” Material de Faro Digital; Contra la pedofilia en Internet; Gustavo Sain
Ley 27.590 (sancionada en noviembre de 2020) “Ley \"Mica Ortega\" Programa Nacional de prevención y concientización del grooming o ciberacoso contra niños y adolescentes.

Informática forense

Di Iorio, A.H. et a; El rastro digital del Delito. Aspectos técnicos, legales y estratégicos de la informática forense en el proceso penal; - 1a ed. - Mar del Plata. Universidad FASTA, 2017. Disponible en: https://info-lab.org.ar/descargas/libros-y-guias
Brenna, Bauzá Reylli; Justicia y Registros Públicos. La tecnología al servicio de la justicia y la seguridad jurídica;. 1a ed. - Buenos Aires. La Ley Thomson Reuters, 2020.
Scientific Working Group on Digital Evidence (SWGDE): «Best Practices for Mobile Device Evidence Collection and Preservation, Handling, and Acquisition» Version: 1.1, July 2019. Disponible en: https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20Mobile%20Device%20Evidence%20Collection%20and%20Preservation,%20Handling,%20and%20Acquisition.
Scientific Working Group on Digital Evidence (SWGDE): «Best Practices for Computer Forensic Examination», v. 1.0, July 2018. Disponible en: https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20Computer%20Foren

sic%20Examination.
European Network of Forensic Science Institutes (ENFSI): «Best Practice Manual for the Forensic Examination of Digital Technology», ENFSI-BMP-FIT-01, v. 0.1, November 2015. Disponible en: http://enfsi.eu/documents/best-practice-manuals/.
Interpol: «Global Guidelines for Digital Forensics Laboratories». Mayo de 2019, disponible en: https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf.
Di Iorio, A.H. et al; “Guía Integral de empleo de la Informática Forense en el Proceso Penal” - 1a ed. - Mar del Plata. Universidad FASTA, 2015. Disponible en: https://info-lab.org.ar/descargas/libros-y-guias
[12] Procuración General de la Nación.“Guía de obtención, preservación y tratamiento de la evidencia digital”. Publicada en PGN-0756-2016-001. 2016
https://merida.anahuac.mx/noticias/que-es-violencia-digital
https://farodigital.org/wp-content/uploads/2019/10/informe-perspectivas.pdf
https://www.un.org/es/hate-speech/impact-and-prevention/targets-of-hate
https://www.infoem.org.mx/es/iniciativas/micrositio/violencia-digital#:~:text=%C2%BFQu%C3%A9%20es%20la%20violencia%20digital,o%20en%20su%20imagen%20propia

Derecho en materia de ciberseguridad

Ley 26.388 de Delitos Informáticos.
Código Penal Argentino.
Convención de Budapest sobre Cibercrimen.
Di Iorio, Ana et. al. \"El Rastro Digital del Delito\". Edit. Universidad FASTA, 2017.
Sain, G. \"Qué son los delitos informáticos\"; Edit. Rubinzal Culzoni.
RC-D-875/2015. Competencias Institucionales de la Dirección Nacional de Ciberseguridad. Anexo ll de la Disposición Administrativa 1865-2020.
Decreto 577-2017. Creación del Comité de Ciberseguridad.
Decreto 480-2019. Modificación del Comité de Ciberseguridad
Disposición ONTI 2-2013. Creación ICIC-CERT.
Resolución JGM 580-2011. Creación del Programa Nacional de Infraestructuras Críticas de la Información y Ciberseguridad.
Disposición ONTI 1-2015. Modelo de Política de Seguridad de la Información.
(Aclaración: esta bibliografía está sujeta a modificaciones normativas que pudieran suceder antes o durante la realización de este curso).

Evaluación de los aprendizajes

Evaluación de proceso: Se realizará en forma continua a lo largo del cursada. Se valorará la participación en los debates durante cada encuentro. A su vez, los participantes realizarán actividades de autocomprobación que remiten a cuestionarios con respuestas múltiples choice sobre cada unidad trabajada.

Evaluación de producto: Se realizará a partir de una actividad de autocomprobación que consistirá en la presentación distintas situaciones similares a las que pueden presentarse en el ámbito laboral, que los participantes deberán analizar y resolver aplicando los contenidos abordados en la cursada.

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

Se solicitará una asistencia a cinco de los seis encuentros virtuales sincrónicos. Realización y aprobación de todas las actividades de autocomprobación con el 70% de las respuestas correctas.

Duración (Hs.)

12

Detalle sobre la duración

12 horas distribuidas en 6 encuentros semanales virtuales sincrónicos de 2 horas de duración cada uno.

Lugar

Plataforma de videoconferencias CISCO Webex
Campus Virtual INAP

Perfil Instructor

Especialistas en la temática:
María Patricia Prandini
Nancy Garnica
Carina González
Ana Di Iorio
Sabrina Lamperti
Marcela Pallero
María Florencia Zerda

Origen de la demanda

INAP- Dirección Nacional de Ciberseguridad

Prestadores Docentes

CUIT/CUIL	APELLIDO Y NOMBRE
27251940776	DI IORIO,ANA HAYDÉE
27228591950	GARNICA,NANCY EVA
27229802033	GONZÁLEZ ,CARINA VERÓNICA
27307205764	LAMPERTI,BEATRIZ
23234525204	PALLERO,MARCELA INES
23135307564	PRANDINI,MARIA PATRICIA
27311648891	ZERDA,MARÍA FLORENCIA