ANEXO I

DISEÑO CURRICULAR
TRAYECTO DE FORMACIÓN PROFESIONAL CONTINUA
ESPECIALIZACIÓN PROFESIONAL EN PROGRAMACIÓN SEGURA

I. IDENTIFICACIÓN DE LA CERTIFICACIÓN PROFESIONAL: "ESPECIALIZACIÓN PROFESIONAL EN PROGRAMACIÓN SEGURA"

I.1. Sector/es de actividad socio productiva: **Informática - Software y Servicios Informáticos**
I.2. Perfil profesional de referencia: **Programador**
I.3. Familia profesional: **Informática**
I.4. Denominación del certificado de referencia: **Especialización Profesional en Programación Segura**
I.5. Ámbito de la trayectoria formativa: **Formación Profesional**
I.6.Tipo de certificación: **Certificado de Formación Profesional Continua (especialización)**
I.7. Nivel de la certificación: **III**

II. REFERENCIAL AL PERFIL PROFESIONAL

La propuesta de formación profesional continua de especialización en Programación Segura está dirigida a programadores formados en el trayecto de formación profesional inicial de Programador (Certificación de FP inicial de Nivel III, aprobada en CABA por Resolución Nº 4170-MEGC/2016) y a otros/as profesionales egresados/as de la educación técnico profesional (Técnico/a en Computación, Técnico/a en Programación, entre otros/as) cuyos perfiles profesionales incluyen funciones de programación de aplicaciones informáticas, que requieren especializarse en el análisis de la seguridad de aplicaciones y la implementación de técnicas de programación segura en los procesos de desarrollo de software en los que interviene el/la Programador/a.

Las funciones propias del Programador (definidas en el trayecto de FP inicial) consisten en:

- Escribir código de programación de acuerdo con las especificaciones formales.

- Interpretar especificaciones de diseño de las asignaciones a programar en el contexto del desarrollo de software en el que participa.

- Planificar su trabajo en el contexto del equipo de desarrollo del proyecto.

- Verificar el código desarrollado y depurar estructuras lógicas o códigos de programas.

- Manejo y manipulación de los datos y su relación con las aplicaciones a desarrollar o desarrolladas.

- Realizar la documentación técnica y de usuarios de acuerdo con los requerimientos Funcionales y técnicos recibidos.

La intervención profesional que se toma como referencia para la presente especialización, supone el desarrollo de las funciones descriptas en ámbitos productivos especialmente dedicados a desarrollo de productos informáticos específicos. No involucra, por tanto, una modificación de las funciones propias del programador. En términos formativos, esta especialización implica la incorporación

de un conjunto de conocimientos y habilidades de particular relevancia para la intervención profesional del programador en el ámbito del desarrollo de software seguro y monitoreo de la ciberseguridad en el software.

La especialización en Programación Segura brinda al Programador conocimientos y habilidades de aplicación específica para:

- Identificar e interpretar políticas organizacionales y normativas de protección en ciberseguridad.

- Implementar, en el marco de las funciones propias de su perfil profesional, las acciones requeridas y previstas en los planes de prevención definidos por la organización.

- Analizar el nivel de seguridad requerido por las aplicaciones, verificando los medios que permiten a ciberdelincuentes transmitir código malicioso.

- Configurar la seguridad de los sistemas informáticos y de redes para minimizar las probabilidades de exposición a ataques

- Implementar estrategias de seguridad en el desarrollo del software.

- Detectar e investigar incidentes de ciberseguridad del software, documentando lo ocurrido.

- Realizar análisis de riesgos para identificar activos, amenazas, vulnerabilidades y medidas de seguridad en las aplicaciones de software.

- Configurar la seguridad de sistemas informáticos para minimizar las probabilidades de exposición a ataques.

III. ESTRUCTURA MODULAR

La presente propuesta de FP continua en Seguridad de Software se integra mediante dos módulos:

Módulos	Horas reloj
I. Incidentes de Ciberseguridad	60
II. Programación Segura	120
Carga horaria total del trayecto	**180**
Carga horaria de prácticas formativas profesionalizantes	**120**

Respecto de la organización y secuencia de cursado del trayecto, para iniciar el cursado del módulo II es recomendable haber completado el cursado el módulo I. La aprobación del módulo correlativo será condición para la aprobación del módulo, no así para su cursado.

IV. DESCRIPCIÓN DE LOS MÓDULOS

Módulo I: INCIDENTES DE CIBERSEGURIDAD

Carga horaria total: 60 horas reloj
Carga horaria de prácticas formativas profesionalizantes: 30 horas reloj

Presentación

Este módulo es de carácter *común* a la formación continua en ciberseguridad, por actualización y/o por especialización, de profesionales del desarrollo de software, del soporte de infraestructura y de la administración de redes informáticas (programadores/as, instaladores/as administradores/as de redes, técnicos/as en computación, entre otros/as).

Su propósito general es que dichos profesionales accedan a un marco técnico y conceptual general y actualizado sobre ciberseguridad, enfatizando en los estándares y normas técnicas de ciberseguridad de información, aplicaciones y redes.

Se orienta en particular al desarrollo de las capacidades de:

- Identificar e interpretar políticas organizacionales y normativas de protección en ciberseguridad.

- Implementar, en el marco de las funciones propias de su perfil profesional, las acciones requeridas y previstas en los planes de prevención definidos por la organización.

- Analizar el nivel de seguridad requerido por las aplicaciones, verificando los medios que permiten a ciberdelincuentes transmitir código malicioso.

- Configurar la seguridad de los sistemas informáticos y de redes para minimizar las probabilidades de exposición a ataques

En función de sus propósitos generales, los contenidos del módulo se organizan en los siguientes bloques:

- **Incidentes y amenazas de ciberseguridad**: dominios de la seguridad de la información, tipologías de incidentes y amenazas, grados de criticidad de incidentes; vulnerabilidad y riesgo en ciberseguridad; herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes. Auditorías internas de prevención. Documentación de incidentes. Tipos de auditoría: Forense, web, de código, de redes, de sistema operativo. Seguridad en entornos Cloud. Seguridad en mobility cloud.

- **Estándares de ciberseguridad**: organismos reconocidos; normas técnicas en gestión de seguridad de información y de incidentes, en aplicaciones y redes, entre otros.

- **Políticas de ciberseguridad en las organizaciones**: componentes, medidas de prevención y de actuación, documentación.

Objetivos de aprendizaje

Son objetivos específicos de aprendizaje del presente módulo:

- Identificar y comprender los criterios empleados en el campo profesional para la tipificación y clasificación de vulnerabilidades, riesgos, amenazas e incidentes de ciberseguridad y sus grados de criticidad.

- Identificar distintos tipos de herramientas, mecanismos de detección y alertas de seguridad empleados en el análisis de incidentes de ciberseguridad.

- Identificar y comparar estándares técnicos en ciberseguridad de aplicación en distintos sectores

y ámbitos.

- Interpretar planes organizacionales de prevención y concientización en ciberseguridad.

- Conocer y utilizar procedimientos y estándares para la documentación de incidentes y políticas de ciberseguridad en las organizaciones.

Desarrollo del módulo

Bloques de contenidos	Prácticas Formativas Profesionalizantes
Incidentes y amenazas de ciberseguridad Dominios de la seguridad de la información: política de seguridad, organización de la seguridad de la información, seguridad de los recursos humanos, gestión de las operaciones y comunicaciones, control de accesos Tipologías de incidentes y amenazas Grados de criticidad de incidentes Vulnerabilidad y riesgo en ciberseguridad Herramientas y mecanismos de monitorización: herramientas libres y propietarias (Nessus, ManageEngine, IBM QRadar, SolarWinds, Sumo Logic, AlientVault, Rapid7 InsightIDR) Antivirus, firewall perimetral de red, servidor proxy, End Point Disk Encryption, escáner de vulnerabilidades Identificación, detección y alerta de incidentes Documentación de incidentes Auditorías internas de prevención Tipos de auditoría: Forense, web, de código, de redes, de sistema operativo Seguridad en entornos Cloud Seguridad en mobility cloud **Estándares de ciberseguridad** Organismos reconocidos Normas técnicas en gestión de seguridad de información y de incidentes, en aplicaciones y en redes **Políticas de ciberseguridad en las organizaciones** Componentes Medidas de prevención y de actuación Documentación	A partir de casos seleccionados para su estudio, y/o de la simulación de incidentes en la seguridad de sistemas de información, se espera que las/os estudiantes puedan: - Identificar, analizar y comprender políticas de seguridad previstas y/o aplicadas en casos de detección y corrección de incidentes. - Investigar y reconocer los accesos a la información en la red. - Analizar los diferentes controles de acceso a partir de una aplicación. -Tipificar incidentes y amenazas específicas en función de características de sistemas de información específicos y de las políticas de uso y de seguridad fijadas por la organización, para casos reales o simulados. - Plantear las posibles medidas de contención de los incidentes para limitar los posibles daños causados. - Identificar y analizar los posibles riesgos en la información tales como: fallas del sistema, corte de conexión de internet, interrupción del consumo eléctrico. - Determinar medidas de ciberseguridad en redes dirigidas a minimizar riesgos. - Reconocer y clasificar las herramientas adecuadas de monitorización de acuerdo a la red y/o sistema a monitorear. - Identificar los procedimientos adecuados para dar respuesta, mitigar, eliminar o contener distintos tipos de incidentes. - Identificar los sistemas de autenticación web, destacando sus debilidades y fortalezas.

	- Identificar los puntos principales de aplicación de seguridad para verificar el cumplimiento normativo. - Analizar y evaluar los riesgos de diferentes tipos de organizaciones de acuerdo con la normativa vigente. - Para los distintos casos y situaciones analizadas, realizar la documentación de análisis forense mediante informes conforme estándares establecidos en materia de ciberseguridad.

Módulo II: **PROGRAMACIÓN SEGURA**
Carga horaria total: 120 horas reloj
Carga horaria de prácticas formativas profesionalizantes: 90 horas reloj

Presentación

Este módulo es de carácter *específico* a la formación continua en ciberseguridad, por especialización, de profesionales de Programación (programadores de FP, técnicos/as en computación, entre otros/as).

Centralmente el propósito formativo de este módulo es la construcción de habilidades y conocimientos por parte de las/os estudiantes para aplicar seguridad en el código fuente de un software con el objetivo de encontrar y solucionar la vulnerabilidad del software.

Se orienta en particular al desarrollo de las capacidades de:

- Implementar estrategias de seguridad en el desarrollo del software.

- Detectar e investigar incidentes de ciberseguridad del software, documentando lo ocurrido.

- Realizar análisis de riesgos para identificar activos, amenazas, vulnerabilidades y medidas de seguridad en las aplicaciones de software

- Configurar la seguridad de sistemas informáticos para minimizar las probabilidades de exposición a ataques.

En función de sus propósitos generales, los contenidos del módulo se organizan en los siguientes bloques:

- Seguridad de aplicaciones
Seguridad en los lenguajes de programación y sus entornos de ejecución ("*sandboxes*"). Entorno aislado donde ejecutar procesos sospechosos de manera controlada antes de su implantación en el resto del sistema. Listas de riesgos de seguridad habituales. Requisitos de verificación de acuerdo al nivel de seguridad establecido. Comprobaciones de seguridad a nivel de aplicación: *ASVS (Application Security Verification Standard).*

- Seguridad de aplicaciones *web*

Desarrollo seguro de aplicaciones *web*. Listas públicas de vulnerabilidades de aplicaciones web. *OWASP Top Ten.* Entrada basada en formularios. Validación de la entrada. Estándares de autenticación y autorización. Vulnerabilidades *web*. Almacenamiento seguro de contraseñas. Criptografía de clave pública y clave privada. Seguridad de portales y aplicativos web. Soluciones *WAF (Web Application Firewall*).

- Seguridad en aplicaciones para dispositivos móviles
Modelos de permisos en plataformas móviles. Llamadas al sistema protegidas. Firma y verificación de aplicaciones. Almacenamiento seguro de datos. Fuga de información en los ejecutables.

- Hacking ético
Elementos esenciales del *hacking* ético. Diferencias entre *hacking*, *hacking* ético, test de penetración y hacktivismo. Los objetivos y las fases del *hacking* ético. Las herramientas de seguridad y *hacking*. La administración remota de sistemas. El ataque ético a redes de comunicaciones, a sistemas y a las aplicaciones *web*.

Objetivos de aprendizaje

Son objetivos específicos de aprendizaje del presente módulo:

- Identificar los sistemas de control de acceso y autenticación en los sistemas informáticos, controlando el cumplimiento de los requisitos de seguridad y minimizando las posibilidades de exposición a ataques.

- Analizar el nivel de seguridad requerido por las aplicaciones y los vectores de ataque más habituales, evitando incidentes de ciberseguridad.

- Implantar sistemas seguros de desplegado de software con la adecuada coordinación entre los desarrolladores y los responsables de la operación del software.

- Combinar técnicas de hacking ético interno y externo para detectar vulnerabilidades que permitan eliminar y mitigar los riesgos asociados.

- Conocer y utilizar procedimientos y estándares para la documentación de incidentes

Desarrollo del módulo

Bloques de contenidos	Prácticas Formativas Profesionalizantes
Seguridad de aplicaciones Seguridad en los lenguajes de programación y sus entornos de ejecución ("*sandboxes*"). Listas de riesgos de seguridad habituales. Comprobaciones de seguridad a nivel de aplicación: *ASVS (Application Security Verification Standard).* **Seguridad de** aplicaciones ***web*** Desarrollo seguro de aplicaciones *web:* controles de identidad y autenticación, protección de datos. *OWASP Top Ten.* Entrada basada en formularios. Validación de la entrada.	A partir de casos seleccionados para su estudio, y/o de la simulación de incidentes en la seguridad de aplicaciones, se espera que las/os estudiantes puedan: -Conocer, configurar y utilizar sandbox para programar aplicaciones seguras -Ante incidentes simulados, listar y determinar los riesgos detectados -Desarrollar, añadir y probar características de seguridad dentro de las aplicaciones para evitar vulnerabilidades. -Conocer, seleccionar y utilizar parámetros para las consultas validando las entradas a

Estándares de autenticación y autorización. Vulnerabilidades *web*. Almacenamiento seguro de contraseñas. Criptografía de clave pública y clave privada. Seguridad de portales y aplicativos web. Soluciones *WAF (Web Application Firewall*). **Seguridad en aplicaciones para dispositivos móviles** Modelos de permisos en plataformas móviles. Llamadas al sistema protegidas. Firma y verificación de aplicaciones. Almacenamiento seguro de datos. Fuga de información en los ejecutables. **Hacking ético** Elementos esenciales del *hacking* ético. Diferencias entre *hacking*, *hacking* ético, test de penetración y hacktivismo. Objetivos y las fases del *hacking* ético. Herramientas de seguridad y *hacking*. Administración remota de sistemas. Ataque ético a redes de comunicaciones, a sistemas y a las aplicaciones *web*.	una aplicación web seleccionada para el trabajo. - Configurar el sitio web aplicando políticas de seguridad dadas. - Configurar sistemas de control de identidad y autenticación en aplicaciones, cumpliendo los requisitos de seguridad y minimizando las posibilidades de exposición a ataques. - Desarrollar algoritmos criptográficos seguros para almacenar las contraseñas de usuario. - Detectar y corregir vulnerabilidades de aplicaciones web analizando su código fuente y configurando servidores web. - Implementar medidas para evitar los ataques a contraseñas, envío masivo de mensajes o registros de usuarios a través de programas automáticos (bots). -Implementar un sistema de validación de compras integradas en la aplicación haciendo uso de validación en el servidor. - Documentar las tareas realizadas y los procedimientos a seguir para la recuperación ante desastres.

V. ENTORNO FORMATIVO

La implementación del trayecto de Especialización Profesional en Programación Segura se realizará en entornos formativos de características adecuadas a los requerimientos de cada uno de los módulos, en particular de las prácticas definidas en el diseño curricular. En este apartado se fijan algunas definiciones generales para orientar a los Centros de Formación Profesional en la configuración de los espacios formativos requeridos para una adecuada implementación de esta oferta.

El siguiente cuadro enumera los espacios suficientes para satisfacer las necesidades del dictado de los módulos que componen el presente trayecto formativo.

a) Matriz de relación entre los espacios formativos y los módulos del trayecto

Módulo	Laboratorio/Taller de Ciberseguridad
Incidentes de Ciberseguridad	**X**
Programación Segura	**X**

b) Características generales de los espacios

Infraestructura

- Para las prácticas de enseñanza a desarrollarse en los Laboratorio_Taller de Ciberseguridad se requiere una superficie de 2 m^2 como mínimo por estudiante en grupos no mayores de 12 estudiantes.
- La potencia eléctrica del laboratorio/taller deberá considerar la carga a conectar, seccionando la alimentación de luminarias, equipos de climatización y línea de tomas y con elementos de protección adecuados.
- Instalación eléctrica monofásica tanto para el laboratorio_Taller. Se recomienda la instalación de bandejas portacables para permitir una mayor flexibilidad en las actividades a desarrollar y optimizar la instalación de luminarias, tomas y equipos.
- Circuito de señales (por ejemplo: TV, video, internet, telefonía).

Requerimientos físico-ambientales

- Iluminación general con valores de iluminancia entre 250 y 350 lux, con luminarias uniformemente distribuidas para lograr niveles de iluminación homogéneos en el recinto.
- Utilización de colores de alta reflexión en paredes, cielorrasos, pavimentos y mobiliario, para aumentar la eficiencia.
- Iluminación focalizada hacia los planos de trabajo que permita alcanzar niveles de iluminación de 500 lux.
- Ventilación natural para garantizar la renovación del aire conforme al código de edificación del GCABA.
- Climatización adecuada.
- Aislamiento de aquellas habitaciones en que el ruido supera el admitido por la normativa vigente.

Equipamiento mobiliario

- El laboratorio/taller deberá contar con sillas/taburetes ergonómicas, y mesas robustas de medidas tales de poder distribuir con comodidad los equipos de medición más módulos didácticos y tener lugar suficiente para que los estudiantes puedan apoyar elementos de escritura. De ser metálicas, deberán estar conectadas rígidamente a masa.
- Se recomienda la utilización de mobiliario modular para permitir la reconfiguración del mismo con la finalidad de facilitar el trabajo individual o en grupos.
- Armarios, estanterías, gabinetes y cajoneras para alojar documentación técnica, componentes, instrumentos y herramientas necesarios para lograr que el dictado de las clases sea operativo y eficiente.
- Bibliografía específica en distintos tipos de soporte.
- Pizarra. Proyector y pantalla.

c) Características particulares de los espacios

Laboratorio/Taller de Ciberseguridad

En relación con las prácticas formativas que en él se desarrollarán, este espacio debe contar con el equipamiento y los insumos que permitan a los estudiantes realizar las actividades sugeridas en los módulos. De acuerdo a las prácticas de enseñanza a desarrollar este espacio debe contar con:

- **Computadoras personales (PC)** más equipamiento de soporte (alimentación regulada, con seguridad e ininterrumpida, monitor).
- **Software de aplicación, simuladores y software de base.**
- **Equipos routeadores y de switching**, impresoras.

- Racks abiertos.
- Doble red (para evitar que las prácticas de laboratorio interfieran con la administración de la red en uso).
- Repetidores y amplificadores de señal Wi Fi.
- Pacheras para rack modular.
- Switch con puertos fibra óptica.
- Switch configurable.

- Pizarra. Proyector y pantalla.

VI. REFERENCIAL DE INGRESO

Al momento de iniciar el cursado del presente trayecto de especialización, el estudiante deberá:

a) Poseer alguna de las siguientes certificaciones de educación técnico profesional:

- Certificado de Formación Profesional inicial “Programador” (Resolución Nº 4170-MEGC/2016)

- Título Técnico en Computación (Resolución SSGECP 4147/12)

- Título Técnico en Programación (conforme marco de referencia CFE 148/11 Anexo I y correspondiente resolución provincial).

- Títulos Técnicos de nivel terciario, aprobados por las correspondientes resoluciones jurisdiccionales, basados en perfiles profesionales con funciones propias de la administración de redes informáticas.

O bien:

b) En caso de no contar con alguna de las certificaciones de educación técnico profesional mencionadas en (a), poseer terminalidad de Nivel Secundario y acreditar experiencia o desempeño profesional –no menor de cinco años- en el sector Informática, subsector de Programación / Desarrollo de sistemas de Información en funciones de programación de aplicaciones informáticas.

O bien:

c) En atención a lo dispuesto por la Ley de Educación Nacional respecto de la educación de adultos, certificar saberes producidos a partir de la experiencia de vida y de trabajo, referenciados en perfiles profesionales aprobados por los organismos intervinientes y acreditar experiencia o desempeño profesional –no menor de cinco años- en el sector Informática, subsector de Programación / Ciencia de datos / Desarrollo de sistemas de Información en funciones de programación de aplicaciones informáticas (excluyente).