DJ (1419)

SANTIAGO 28 OCTUBRE 2025

RESOLUCIÓN N° 04565 EXENTA

VISTOS: lo dispuesto en la Ley Nº 19.239; en el D.S. Nº 96 de 2025; en la letra d) del artículo 11 y el artículo 12 del D.F.L. Nº 2 de 1994, ambos del Ministerio de Educación; en la Resolución Exenta N°05339 de 2012; Resolución Exenta N°02489 de 2005 que aprueba el Manual de Procedimientos de la Dirección de Educación Continua; la Resolución Exenta N°5107 de 2022; y lo solicitado por el Director de Educación Continua mediante memorándum N°839 de 2025; y

CONSIDERANDO:

1. Lo dispuesto en el punto 2.13 de la Resolución Exenta N°05339 de 2012 que aprueba la Operacionalización para el Diseño, Aprobación, Dictación, Administración y Modificación de Planes de Estudios.

2. Lo dispuesto en la Resolución Exenta N°05107 de 2022, que establece requisitos para la aprobación y dictación de programas de cursos de capacitación generados en la DIRECAP de carácter cerrado, cuyo origen sea un requerimiento formal de una institución o entidad externa a la Universidad Tecnológica Metropolitana.

3. El Informe Técnico Evaluación Curricular: Presentación Planes de Estudio: Cursos; Seminarios; Diplomas y Postítulos, de la Unidad de Innovación Curricular, de fecha 30 de agosto de 2025.

4. El memorándum N°839 de 2025, y documentación adjunta, del Director de Educación Continua dirigido al Director Jurídico, solicitando gestionar resolución de aprobación del Curso Respuestas a Incidentes de Seguridad: Ataques Cibernéticos, Ransomware o Violaciones de Datos**,** código 060128.

5. Que, así las cosas, el memorándum N°839 de 2025, dirigido al Director Jurídico es procedente; por tanto

RESUELVO:

I. **Apruébese,** el Curso **RESPUESTAS A INCIDENTES DE SEGURIDAD: ATAQUES CIBERNÉTICOS, RANSOMWARE O VIOLACIONES DE DATOS,** código 060128, que ofrecerá la Universidad Tecnológica Metropolitana, a través de la Dirección de Educación Continua, dirigido a quienes ejerzan como funcionarios públicos y requieran aplicar procesos de respuesta ante incidentes de seguridad informática, como a continuación se indica:

II. El objetivo General del Curso será aplicar procedimientos y metodologías de gestión de incidentes de seguridad cibernética, a partir de la identificación, contención y erradicación de amenazas en un entorno empresarial, para garantizar la continuidad operacional y la protección de datos.

III. Requisito de Ingreso:

- Certificado Laboral que acredite experiencia en el Estado u otras afines que requieran utilizar la normativa de seguridad ISO 27035.

IV. Al finalizar el curso, el o la estudiante alcanzará los siguientes logros de aprendizaje:

1. Identificar los conceptos, terminologías y tipos de incidentes de seguridad cibernética en diferentes ámbitos, en base a sus características, impactos, roles y responsabilidad.

2. Contrastar los incidentes de seguridad cibernética, empleando metodologías de respuesta (NIST, SANS), en base a indicadores de compromiso y técnicas de análisis forense digital.

3. Emplear estrategias de contención y erradicación de amenazas cibernéticas, utilizando técnicas de manejo de incidentes y violación de datos.

4. Identificar Aplicar procedimientos y procesos de recuperación de datos y sistemas afectados, considerando el contexto institucional de una empresa y la normativa vigente.

V. El curso es un plan cerrado que se dictará en régimen modular grupal a distancia, E-learning, sincrónica, con una duración de 14 horas cronológicas y 4 módulos, cuya descripción, objetivos específicos, unidades, contenidos, metodología y sistema de evaluación, son los que se indican en el documento que como ANEXO 1 se acompaña a la presente resolución exenta formando parte integrante de la misma.

Los Módulos y/o Temáticas son las siguientes:

Objetivos Específicos	Contenidos	Horas Cronológicas			
		T	P	e-l	TH
Módulo I Fundamentos de respuestas a incidentes **Objetivo** Identifica los conceptos, terminologías y tipos de incidentes de seguridad cibernética en diferentes ámbitos, en base a sus características, impactos, roles y responsabilidad.	• Introducción a la respuesta a incidentes: conceptos clave y terminología. • Tipos de incidentes de seguridad: ataques cibernéticos, ransomware, violaciones de datos. • Marcos de trabajo de respuesta a incidentes: NIST, SANS, ISO 27035. • Roles y responsabilidades del equipo de respuesta a incidentes (CSIRT).			3	3
Módulo II Detección y análisis de incidentes. **Objetivo** Contrasta los incidentes de seguridad cibernética, empleando metodologías de respuesta (NIST, SANS), en base a indicadores de compromiso y técnicas de análisis forense digital.	• Monitoreo de seguridad: logs, SIEM, IDS/IPS. • Análisis de logs y correlación de eventos. • Técnicas de análisis forense digital. • Identificación de indicadores de compromiso (IOCs).			3	3

Módulo III Contención y erradicación de amenazas. **Objetivo** Emplea estrategias de contención y erradicación de amenazas cibernéticas, utilizando técnicas de manejo de incidentes y violación de datos.	• Estrategias de contención: segmentación de red, aislamiento de sistemas. • Técnicas de erradicación: eliminación de malware, parcheo de vulnerabilidades. • Manejo de incidentes de ransomware: negociación, recuperación de datos. • Manejo de violaciones de datos: notificación, gestión de la reputación.			4	4
Módulo IV Recuperación y lecciones aprendidas. **Objetivo** Aplica procedimientos y procesos de recuperación de datos y sistemas afectados, considerando el contexto institucional de una empresa y la normativa vigente.	• Procesos de recuperación de datos y sistemas. • Validación de la integridad de los sistemas recuperados. • Elaboración de informes post-incidente. • Análisis de lecciones aprendidas y mejora continua. • Obligaciones legales y normativas relacionadas con la notificación de incidentes.			4	4
	Sub Total de horas			**14**	**14**
	Total de horas				**14**

T: trabajo teórico / P: trabajo práctico / E-l: e-learning / TH: total horas

VI. Los cupos, horas, fechas, horarios y lugar en que se impartirá el Curso se establecerán en las resoluciones exentas que autoricen la dictación de cada una de las versiones de este.

Regístrese y comuníquese,

Firmado digitalmente por Mario Ernesto Torres Alcayaga
Fecha: 2025.10.28 17:56:15 -03'00'

MARISOL PAMELA DURAN SANTIS
Firmado digitalmente por MARISOL PAMELA DURAN SANTIS
Fecha: 2025.10.28 16:32:22 -03'00'

DISTRIBUCIÓN:
Vicerrectoría Académica
Vicerrectoría de Vinculación con el Medio
Vicerrectoría de Administración y Finanzas
Contraloría Interna
Dirección General de Análisis Institucional y Desarrollo Estratégico
Dirección Jurídica
Dirección de Finanzas
Dirección Educación Continua (Anexo 1)
Dirección General de Docencia (Anexo 1)
Subdirección General de Docencia (Anexo 1)
Unidad de Títulos y Grados (Anexo 1)

UNIVERSIDAD TECNOLOGICA METROPOLITANA

DOCUMENTO TOTALMENTE TRAMITADO

PCT
PCT/ppp