PROGRAMA

Diplomado en Prevención y Gestión del Riesgo de Fraude

Formación Continua · PUCV

VICERRECTORÍA DE VINCULACIÓN CON EL MEDIO

PONTIFICIA UNIVERSIDAD CATÓLICA DE VALPARAÍSO

PONTIFICIA UNIVERSIDAD CATÓLICA DE VALPARAÍSO
Comisión Nacional de Acreditación CNA-Chile
7 AÑOS
UNIVERSIDAD ACREDITADA NIVEL DE EXCELENCIA
DOCENCIA DE PREGRADO
GESTIÓN INSTITUCIONAL
DOCENCIA DE POSTGRADO
INVESTIGACIÓN
VINCULACIÓN CON EL MEDIO
HASTA ENERO 2029

PONTIFICIA
UNIVERSIDAD
CATÓLICA DE
VALPARAÍSO

PONTIFICIA UNIVERSIDAD CATÓLICA DE VALPARAÍSO

FORMACIÓN CONTINUA PUCV

www.formacioncontinuapucv.cl

Antecedentes Generales

Fecha de inicio

14 de Octubre 2026

Fecha de cierre

18 de Enero 2027

Horas Totales

90 Horas

> Online con clases en vivo

Objetivo General

El Diplomado en Prevención y Gestión del Riesgo de Fraude tiene por finalidad formar profesionales capaces de prevenir, detectar y gestionar potenciales eventos de fraude y otros delitos económicos que pudiesen impactar a la organización, mediante herramientas de auditoría forense, investigación interna, análisis criminal, ciberseguridad y modelos integrales de gestión, contribuyendo a la protección de su patrimonio, el fortalecimiento del control interno y el cumplimiento normativo en materia penal.

Objetivos Específicos

Al finalizar el diplomado, los participantes serán capaces de:

- **Comprender** los fundamentos, modelos explicativos y principales tipologías del fraude ocupacional, corporativo y financiero, en concordancia con los lineamientos de la ACFE.
- **Analizar** mecanismos de manipulación de estados financieros, señales de alerta e inconsistencias contables asociadas a fraude.
- **Interpretar** el marco normativo aplicable al fraude, lavado de activos, responsabilidad penal de las personas jurídicas y delitos económicos.
- **Examinar** tipologías, modus operandi y alertas tempranas de fraude, considerando los marcos de referencia y herramientas de gestión para el diseño de mecanismos de control adecuados a cada organización.
- **Implementar** herramientas de ciberseguridad, minería de datos (Big Data) e inteligencia artificial (IA) para prevenir, detectar e investigar fraudes.
- **Ejecutar** investigaciones internas y auditorías forenses ante denuncias o hallazgos de fraude, asegurando su trazabilidad, el resguardo de evidencias y la elaboración de reportes técnicos.
- **Estructurar** un modelo de gobernanza y gestión del riesgo de fraude, sustentado en políticas, herramientas e indicadores clave, que permitan la prevención, respuesta oportuna y toma de decisión.

Dirigido a

Profesionales de las áreas de contabilidad, auditoría, finanzas, administración, gestión de riesgos y disciplinas afines, interesados en fortalecer sus competencias para asumir cargos en áreas ligadas a la prevención de delitos, gestión de riesgos de fraude, criminal compliance y auditoría forense. De igual modo, se orienta a empresarios, emprendedores, inversionistas, directores y administradores que deseen fortalecer sus sistemas de control para proteger el patrimonio organizacional y personal contra el fraude.

Actividad Promocional Sugerida

Profesionales de las áreas de contabilidad, auditoría, finanzas, administración, gestión de riesgos y disciplinas afines, interesados en fortalecer sus competencias para asumir cargos en áreas ligadas a la prevención de delitos, gestión de riesgos de fraude, criminal compliance y auditoría forense. De igual modo, se orienta a empresarios, emprendedores, inversionistas, directores y administradores que deseen fortalecer sus sistemas de control para proteger el patrimonio organizacional y personal contra el fraude.

Contenido

Módulo 1: Teoría del Fraude

- La participación de los examinadores de fraudes en los fraudes contables.
- ¿Somos un país Fraudulento?.
- El cambio de concepto de triangulo de fraude al rombo del fraude.

Módulo 2: El fraude en los EE.FF.

- ¿Qué es el fraude a los Estados Financieros? - Reportes Fraudulentos según ACFE.
- ¿Cómo un requerimiento de una NIIF puede volverse doloso? Transacciones cotidianas que se vuelven fraudulentas.
- El criterio profesional para registrar los cuestionamientos técnicos para discriminar lo íntegro de lo doloso.

Módulo 3: Evidencia e Informes de Auditoría

- La participación de los examinadores de fraudes en los fraudes contables.
- La evidencia contable dubitativa.
- La confección de Informes independientes. La objetividad de los organismos técnicos.

Módulo 4: Análisis Fundamentales de EE.FF.

- Relaciones e inconsistencias en EE.FF. Banderas de Alerta.
- Análisis Fundamentales.
- Casos prácticos Evaluativos.

Módulo 5: El Fraude y la Gestión Corporativa para su mitigación

- Tipologías, Modus Operandi y Alertas de Fraude.
- Perfilamiento psicológico y social del defraudador.
- Normas Técnicas para Gestión del Riesgo de Fraude (COSO v/s ISO).
- Herramientas para la Gestión del Riesgo de Fraude.
- Medidas de control preventivas, detectivas y correctivas.

Módulo 6: Criminal Compliance

- Fundamentos del Compliance Corporativo vs Criminal.
- Fenomenología de la Corrupción Pública y Privada.
- Obligaciones legales contra el Lavado de activo (Ley 19.913).
- Criptomonedas y otros mecanismos de lavado de activo.
- Responsabilidad Penal de las Personas Jurídica (Ley 20.393).
- Herramientas de Gestión para el Criminal Compliance.

Módulo 7: Investigación de Fraude y Auditoría Forense

- Gestión de los Canales de Denuncia.
- Metodología de Investigación de Fraude.
- Auditoría Forense para lo obtención de evidencia.
- Consideraciones éticas y legales en las investigaciones organizacionales.
- Recolección de datos desde fuentes OSINT.
- Uso de Inteligencia Artificial (IA) para la recopilación y análisis de datos.
- Tratamiento de la Evidencia en sus diferentes tipos.
- Reporte a la Alta Administración.
- Asesoramiento en la Gestión Penal y laboral de los hallazgos de Fraude.

Módulo 8: Taller de Criminal Compliance e investigación de Fraude

- Análisis Casuístico de denuncia.
- Consideraciones normativas en materia de Criminal Compliance.
- Aplicación de Investigación para obtención de evidencia.
- Emisión de reporte con sugerencia en materia y laboral.

Módulo 9: Normas Técnicas de Ciberseguridad

- Introducción a las normas de Auditoria TI.
- La familia ISO 27000 y la seguridad de la información.
- ISO 27043: Investigación de incidentes.
- ISO 27037: Adquisición y preservación de evidencia digital.
- ISO 27042: Análisis forense e interpretación.

Módulo 10: Minería de datos contra el fraude

- La Minería de Datos como primer filtro para la detección del fraude.
- Minería de Datos en el análisis del fraude financiero.
- Herramientas TI para Minería de Datos.
- Aplicación de técnicas en Minería de Datos para la detección del fraude financiero.

Módulo 11: Herramientas TI contra el fraude

- El valor de los datos.
- Detección del fraude financiero mediante Big Data.
- Herramientas TI para Big Data. (SQL Server / Python)
- Aplicaciones Big Data en detección de fraudes.

Módulo 12: Implicancias del Procedimiento Penal

- Notificaciones y citaciones MP y Tribunales (Testigos / Peritos).
- Investigación Penal y sujetos procesales.
- Informes de Peritos (Párrafo 6° del CPP).
- Juicio Oral y Procedimientos especiales.

Módulo 13: Principales delitos económicos cometidos por funcionarios públicos

- Fraude al Fisco y Organismos del Estado (tipicidad y penas).
- Malversación de Caudales Públicos (tipicidad y penas).
- Cohecho y Soborno (tipicidad y penas).
- Negociación Incompatible (tipicidad y penas).

Módulo 14: Principales delitos cometidos por empleados en empresas

- Estafa y Otras defraudaciones (tipicidad y penas)
- Apropiación indebida y otros del art. 470 CP.(tipicidad y penas)
- Hurto agravado (tipicidad y penas)
- Corrupción entre particulares (tipicidad y penas)
- Delitos Informáticos de la Ley 21.459 (Fraude informático y receptación de datos (tipicidad y penas)
- Ejercicio Práctico Evaluativo

Módulo 15: Introducción a la ciberseguridad

- Conceptos básicos del ciberespacio, ciberdefensa y ciberseguridad.
- Evolución de las amenazas digitales e identificación de los ciberataques según motivación Ataque interno - ataque externo.
- Fraude Informático desde el punto de vista forense informático

Módulo 16: Pirámide del conocimiento y uso en la ciberseguridad

- Teorema del conocimiento, pirámide DIKW orientado al fraude y ciberseguridad.
- Registros Logs como Dato, Información y Conocimiento.
- Recuperación de datos - carving y los Metadatos de los archivos.
- Criterio/decisión para determinar si hay riesgo, fraude, abuso o se debe investigar.

Módulo 17: Evidencia Forense Digital

- Evidencia digital y su tratamiento.
- Procedimientos y sus riesgos.
- Identificación de fuentes de información virtuales.
- Levantamiento de la cadena de custodia.

Módulo 18: Aplicación de un SIEM

- El fraude moderno ya no se detecta solo con auditoría, se detecta con telemetría.
- ¿Implementación de SIEM en mi organización? Tipos de SIEM Open Source o de pago.
- Levantamiento de SIEM gratuito (práctico).
- Aplicación de datos en un SIEM (práctico).

Módulo 19: Gobernanza del Riesgo

- Gobernanza del riesgo de fraude, políticas, manuales y procedimiento
- Consideraciones prácticas del apetito y tolerancia al riesgo para la toma de decisiones
- Medición del riesgo vía análisis de contexto y criterios de probabilidad e impacto
- Respuesta al riesgo y comunicación efectiva al Directorio, Comités y Administración.
- **Taller de aplicación:** Diagnóstico de Gobernanza de una compañía e institución en base a información pública.

Módulo 20: Herramientas de Gestión

- Herramientas para la identificación del riego, medición y efectividad de control
- Metodología de análisis de riesgos, aspectos cualitativos y cuantitativos.
- Identificación de riesgos desde sistemas y uso de datos para la prevención
- Matriz y perfilamiento del riesgo de fraude.
- **Taller de aplicación de caso:** Aplicar una herramienta de identificación, medición y efectividad de control en una actividad de una compañía o institución.

Módulo 21: Indicadores para gestionar el riesgo de fraude

- Indicadores clave de riesgo y su relación con el apetito y la tolerancia al riesgo.
- Integración de los indicadores al sistema de gestión y a la auditoría continua.
- Inputs para la definición de KRIs aplicados al riesgo de fraude.
- Journey de conductas, definición de parámetros y configuración de alertas.
- **Taller de aplicación de caso:** Seleccionar un tipo de fraude y nivel organizacional, proponer journey y alertas.

Equipo Docente

VÍCTOR ESCOBAR CISTERNA

Magister en Gestión mención Finanzas y Contabilidad, Pontificia Universidad Católica de Valparaíso.

Diplomado en Prevención, Detección e Investigación de fraudes, Universidad de Chile.

Diplomado en Normas Internacionales de Información Financiera (NIIF), INACAP.

Contador Auditor - Licenciado en Comercio y Ciencias Económicas con mención en Finanzas de la Pontificia Universidad Católica Valparaíso.

Se desempeña como Senior Manager de Assurance en la Compañía auditora PWC.

FRANCISCO RIFFO PÉREZ

Magister en Gestión de Riesgos Corporativos y Lavado de Activos, Universidad Central de Chile.

Diplomado en Auditoría Forense, Universidad de Concepción

Diplomado en Prevención del Fraude, Universidad Central de Chile.

Diplomado en Ciberseguridad, Universidad de Santiago de Chile.

Contador Auditor - Licenciado en Comercio y Ciencias Económicas con mención en Finanzas de la Pontificia Universidad Católica Valparaíso.

Se desempeña como Oficial PDI - Brigada Investigadora Anticorrupción - Brigada Investigadora de Delitos Económicos Metropolitana

LEONARDO TAPIA ALFARO

Magister en Derecho Penal, Centro de Estudios de Derecho Penal de la Universidad de Talca.

Diplomado en Derecho Penal, Centro de Estudios de Derecho Penal de la Universidad de Talca.

Abogado - Licenciado en Ciencias Jurídicas y Sociales de la Universidad de Talca.

Se desempeña como Fiscal Jefe en la Unidad de Análisis Criminal y Focos Investigativos de la Fiscalía Regional Metropolitana Occidente.

FRANCISCO ORTIZ TAPIA

Diplomado en Estrategia y Control de Gestión, Universidad de Chile.

Seminario Regional de Cibercrimen para la Américas, dictado por el FBI

Ingeniería de Ejecución Electrónico mención en Telecomunicaciones, Universidad Técnica Federico Santa María.
Ex Oficial de la PDI, Brigada Investigadora del Cibercrimen.

Se desempeña como Analista de Ciberinteligencia en Banco Estado.

HANS MÖLLER LIBERONA

Magister en Ingeniería Informática, Universidad Santiago de Chile.

Diplomados en Big Data y Data Science, Pontificia Universidad Católica de Valparaíso.

Ingeniería Civil Informática, Universidad Santiago de Chile.

Se desempeña como Perito Forense de la sección Info-ingeniería, Laboratorio de Criminalística de la PDI

SANDRA FRITIS MORALES

Global MBA, Universidad De Barcelona, OBS Business School.

Máster en Gestión de Riesgos, Escuela de Administración, Liderazgo, Dirección y Emprendimiento, Universidad del Rey Juan Carlos.

Diplomado de Activos Alternativos, Escuela de Seguros.

Ingeniero en Información y Control de Gestión; Contador Auditor, Universidad de Chile.

Ex Subgerente de Riesgo en AFP CUPRUM

Se desempeña como Strategic project risk Assistant Director- LATAM en PRINCIPAL FINANCIAL GROUP.

PONTIFICIA UNIVERSIDAD CATÓLICA DE VALPARAÍSO

FORMACIÓN CONTINUA PUCV

www.formacion**continuapucv**.cl