DIPLOMADO EN CIBERSEGURIDAD

Modalidad #VIRTUAL

ÍNDICE

DESCRIPCIÓN 3

OBJETIVOS 3

A QUIÉN VA DIRIGIDO 3

METODOLOGÍA 4

PLAN DE ESTUDIO 4

PROYECTO 7

FACILITADORES 9

CERTIFICADO 13

INVERSION Y FORMA DE PAGO 15

FORMULARIO INSCRIPCIÓN 16

CONTACTO 17

DESCRIPCIÓN:

Este diplomado está orientado a la gestión táctica y operativa de los aspectos de ciberseguridad, siendo así su enfoque a los profesionales que son responsables de la misma y de la correcta administración, gobierno y cumplimiento de las normativas de seguridad institucional.

Con esto se busca que los participantes de este curso puedan aprender las buenas prácticas y metodologías del sector y aplicarlas en el día a día de la gestión de riesgos e incidentes en materia de seguridad de la información.

La correcta gestión de la ciberseguridad requiere de previa planificación y del desarrollo de habilidades técnicas para la prevención y respuesta frente a las posibles vulnerabilidades. Es por ello por lo que se contemplan en este curso los fundamentos, métodos y estrategias para garantizar la integridad de la data de la empresa, así como la continuidad de operaciones. Convirtiendo de esta forma las medidas de seguridad en tareas cotidianas que impacten la empresa o institución.

OBJETIVOS:

Dotar a los participantes de los conocimientos y herramientas necesarias para la gestión de la ciberseguridad a nivel táctico y operativo, tomando en consideración los principales avances y vulnerabilidades de los sistemas de información tanto para el sector público como privado.

A QUIÉN VA DIRIGIDO:

Profesionales y personal de empresas privadas, públicas y organizaciones no gubernamentales, así como también, de gerentes o miembros de equipos de tecnología de la información que estén vinculados a los aspectos de la seguridad de información e infraestructura. También está dirigido a profesionales en el ámbito de asesoría empresarial para el diseño de estrategias de diseño de la ciberseguridad.

METODOLOGÍA:

El Diplomado de Ciberseguridad consta de 81 horas. La formación fomenta la participación variada, distribuyéndose entre:

- Clases Online
- Seguimiento en línea
- Análisis y resolución de casos de estudios.
- Documentación sobre cada módulo: apuntes en pdf, infografías, lecturas recomendadas, e-books.
- Evaluaciones Continuas consistentes en prácticas que el alumno deberá realizar en clases y fuera de ella, tanto individual como grupalmente donde aplicará los conocimientos desarrollados en cada módulo.
- Presentación de proyecto final.

PLAN DE ESTUDIOS:

Módulo 1: El Ecosistema de la Ciberseguridad Operativa.

1. Introducción.
2. Conociendo el ecosistema de la ciberseguridad.

Objetivo:
Lograr que los participantes conozcan el término ecosistema en lo que a tecnología se refiere, como se expresa el entorno de la ciberseguridad Operativa, logrando identificar cuáles son las entidades, activos, capacidades, relaciones y amenazas que se encuentran involucrados en ese espacio digital.

Tiempo del módulo: 3 Horas

PLAN DE ESTUDIOS:

Módulo 2: Ciberseguridad Normativa

1. Entorno Global y Marco Normativo de la Ciberseguridad.
2. Aspectos legales en la Gestión de la Ciberseguridad local e internacional.
3. Gobierno de Seguridad de la Información.

Objetivo:

Conocer los paradigmas y modelos de gobernanza a nivel global, obteniendo conocimientos sobre la visión general de las normativas nacionales e internacionales sobre ciberseguridad.

Tiempo del módulo: 9 Horas

PLAN DE ESTUDIOS:

Módulo 3: Ciberseguridad Operativa

1. El proceder de un hacker.
2. Importancia de las Contraseñas
3. Qué es la Criptología y su importancia
4. Aplicaciones criptográficas.
5. Control de acceso.
6. Técnicas generales de ataques.
7. Web segura y vulnerabilidades online.
8. Programación segura.
9. Transacciones electrónicas, seguridad y riesgos.
10. Ethical Hacking.

Objetivo:
Que los participantes conozcan los desafíos y eventos maliciosos cibernéticos, puedan identificar las prioridades de confidencialidad, integridad y disponibilidad, así como los criterios de
seguridad para los equipos. Conocer que es, como y cuando se aplica el ciclo de la Ciberseguridad Operativa.

Tiempo del módulo: 9 Horas

PLAN DE ESTUDIOS:

Módulo 4: Ciberseguridad Táctica

1. Gobernanza de la ciberseguridad y Administración de Riesgos.
2. Gestión de incidentes críticos, amenazas y SLA de respuesta.

Objetivo:

Que los participantes aprendan a resguardar la infraestructura, servicios y aplicaciones en las fases de desarrollo, implementación y administración, de acuerdo con estándares internacionales en ciberseguridad, y mantener el robustecimiento de la seguridad tecnológica.

Tiempo del módulo: 9 Horas

Módulo 5: Ciberinteligencia

1. Orígenes y Fundamentos de la Ciberinteligencia.
2. Aplicación de la Inteligencia de Fuentes Abiertas.
3. Qué son los Metadatos y cómo sacar provecho de ellos.
4. Conociendo la Deep Web y que se puede hacer en ella.

Objetivo:

Conocer cómo a través de la ciberinteligencia podemos identificar, rastrear y predecir las capacidades, intenciones y actividades cibernéticas que apoye la toma de decisiones, usando la adquisición y el análisis profundo de la información.

Tiempo del módulo: 9 Horas

PLAN DE ESTUDIOS:

Módulo 6: Como impacta la Ciberseguridad el Internet de las cosas, los entornos en la nube e industriales.

1. Cloud Computing y seguridad.
2. Internet de las Cosas y el reto de la ciberseguridad.
3. Seguridad en Entornos Industriales.
4. Seguridad persistente avanzada.
5. Análisis Forense en Cloud y Aplicaciones Móviles.

Objetivo:

Proveer al estudiante de técnicas que les permitan crear escenarios de protección de la información e infraestructura a los diferentes entonos, tanto Cloud o empresarial y que medidas aplicar en esta era del Internet de las cosas.

Tiempo del módulo: 9 Horas

PLAN DE ESTUDIOS:

Módulo 7: Computación Forense

1. Etapas de un análisis forense.
2. Adquisición de evidencias digitales.
3. Preservación de la integridad e identidad de las evidencias.
4. Cadena de custodia de las evidencias.
5. Análisis de las evidencias.
6. Laboratorio de análisis forense.

Objetivo:

Dotar al estudiante de herramientas y conocimientos que les ayude a la utilización de la Informática forense como una herramienta preventiva, en primera función. Y poner en sus manos técnicas de auditorías técnicas que permitan recoger datos probatorios de un ataque o fallo en el ecosistema de ciberseguridad, rastreando el origen y los daños causados para la generación de informes y la creación de nuevas estrategias que conlleven al fortalecimiento de la seguridad de la infraestructura tecnológica.

Tiempo del módulo: 9 horas

PLAN DE ESTUDIOS:

Módulo 8: Hablando de Ciberdefensa

1. Ciberpatrullaje.
2. Estrategias de Ciberdefensas.
3. Ciberdefensa Personal.
4. Ciberdefensa Organizacional.
5. Seguridad Perimetral Tecnológica

Objetivo:

Dar a conocer la diferencia entre lo que es ciberseguridad y lo que es ciberdefensa, de manera que los participantes del diplomado puedan generar acciones activas o pasivas desarrolladas en la infraestructura de comunicaciones y datos que impidan que los atacantes puedan penetrar la seguridad y que las medias tomadas cumplan con el rol de protección del entorno de sistemas.

Tiempo del módulo: 9 horas

PLAN DE ESTUDIOS:

Módulo 9: Gestión de proyectos en entornos críticos: Ciberseguridad, accesibilidad y protección.

1. ¿Qué es un Proyecto y qué es la gestión de Proyectos?
2. Planificación estratégica.
3. Cuáles son los Tipos de Información que maneja tu empresa
4. Mapa de Servicios de Ciberseguridad
1. Estrategia y Gestión de la Ciberseguridad
2. Conformidad
5. Diseño e Implantación de la Seguridad
6. Gestión, evaluación, implementación y tratamiento de Riesgos
7. Metodología para la evaluación de riesgos
8. Concienciación y Comunicación

Objetivo:

Dotar al estudiante del conocimiento, estrategias y herramientas que permitan gestionar los riesgos, el cambio y la implementación adecuada de la ciberseguridad de acuerdo con los marcos de gestión de proyectos actuales.

Tiempo del módulo: 9 horas

Proyecto:
Diseño de un Programa
De Ciberseguridad

1. Diseño del Programa.
2. Modelización de Amenazas.
3. Respuesta a Incidentes críticos.
4. Reacción inmediata en Ciberseguridad.
5. Funciones y responsabilidades del Director de Seguridad

Presentación del proyecto: Diseño de un programa de Ciberseguridad

Los participantes de este diplomado deberán de entregar proyecto final el cual está basado en el Diseño de un programa o propuesta de Ciberseguridad para una empresa o institución del sector que les sea asignado. Para esto se formarán grupos de estudios de no más de 6 participantes, entre los cuales podrán ir aplicando de manera práctica los aprendizajes obtenidos. Es parte integral del desarrollo del diplomado, que los especialistas en ciberseguridad aprendan a trabajar en equipo, estudiar las diferentes situaciones, negociar en las mejores condiciones de ganar-ganar, y aprender de sus colegas.

Para recibir su diploma los participantes deben presentar el Proyecto Final de cada grupo con los principales hallazgos resultantes de los diferentes estudios, y las evaluaciones finales realizadas a través del Diplomado.

Cronograma

Cronograma	Facilitadores	Horas	Día	Mes
Módulo 1: El Ecosistema de la Ciberseguridad Operativa.	Federico Montero	3		
Módulo 2: Ciberseguridad Normativa				
Entorno Global y Marco Normativo	Junior Santana	3		
Aspectos Legales de la ciberseguridad local e internacional	Junior Santana	3		
Gobierno de Seguridad de la Información	Johan Rodríguez	3		
Módulo 3: Ciberseguridad Operativa	Fausto Richardson	9		
Módulo 4: Ciberseguridad Táctica	César Rosario Brador	9		
Módulo 5: Ciberinteligencia	Carolina Almonte	9		
Módulo 6: Como impacta la Ciberseguridad el Internet de las cosas, los entornos en la nube e industriales.	Jimmy Rosario	9		
Módulo 7: Computación Forense	Félix José Rodríguez	9		
Módulo 8: Hablando de Ciberdefensa	Jimmy Rosario	9		

FACILITADORES:

FEDERICO MONTERO, MGP, COORDINADOR

Es egresado de la carrera de Ingeniería de Sistemas, con Maestría en Gerencia y Productividad de la Universidad APEC, y Posgrado en Ciberseguridad por NEXT IBS y la Universitat de Llaida. Ha participado de diversos talleres y diplomados acerca de la gestión de proyectos, con los cuales busca generar cambios dentro de las diferentes agrupaciones sociales e institucionales con las que interactúa.

Es miembro del Project Management Institute (PMI) Capítulo República Dominicana donde desempeña la función de Director de la Fundación Educativa de PMIef (Project Management Institute Educational Foundation) proyecto dentro del cual se encarga de llevar los conocimientos de la administración de proyectos por medio de capacitaciones y talleres a ONG's, comunidades, jóvenes, niños y adolescentes.

Realizó funciones como Encargado de la Unidad Equipamiento e Infraestructura en el Ministerio de Educación en la Unidad Ejecutora del Programa República Digital Educación. También es voluntario en varios proyectos como con el Centro de Políticas Públicas, Desarrollo y Liderazgo (CPDL-RD) donde funge como Director de Tecnologías y es el Director Ejecutivo de la Fundación TRUCANO que trabaja con niños y adolescentes de la provincia de Barahona.

Se ha desempeñado en otros cargos en los cuales ha sido reconocido por sus esfuerzos. También se desempeña como Catedrático Universitario en las áreas de ingeniería de sistemas y proyectos desde el año 2015.

FACILITADORES:

CAROLINA ALMONTE

Es egresada de la Universidad Nacional Pedro Henríquez Ureña (UNPHU). Especialista en auditoría de Sistemas, Máster en Ingeniería de Sistemas Mención Gerencial, Catedrática universitaria, con vasto conocimiento en Gestión y evaluación de proyectos de TI, Planificación estratégica, Metodología SCRUM, Quality Asurence, Gobierno de TI, Ciberseguridad, con habilitación docente virtual. Experiencia en transformación digital y la tecnología aplicada al desarrollo, estudios que ha realizado en China. Amante de la tecnología y apasionada de la enseñanza.

FACILITADORES:

JIMMY ROSARIO BERNARD

Doctorado en Ingeniería Informática, Diplomado en Estudios Avanzados (DEA), Maestría en Ingeniería en Informática, Bachelor of Science Computer Engineering, Cybercrime Forensic Investigator y Certified Network Defense Professional (Ethical Hacking), Experto en Diseño Instruccional y Educación Virtual, Diplomados en Proyectos, Aplicaciones Web y Educación. Ha desempeñado la función de Asesor en materia de Tecnología y Director General de Tecnología de la Información, Universidad Autónoma de Santo Domingo (UASD).

Ha fungido como Director de Innovación y Tecnología Educativa, UNICARIBE, profesor en el Instituto Tecnológico de Santo Domi- ngo (INTEC), Profesor Adscrito de la Universidad Iberoamericana (UNIBE) y legal main contact CISCO. Así mismo fungió como Profesor Investigador Titular en el Centro de Investigación en Alta Tecnología, CREA, Instituto Tecnológico de las Américas ITLA, profesor a tiempo completo y Director del Depto. de Bienestar Estudiantil, Calidad Académica, Becas y Egresados de esta misma institución, siendo a su vez consultor en varios proyectos del Programa de Naciones Unidas para el Desarrollo (PNUD) y el Banco Interamericano de Desarrollo (BID).

Autor de más de una docena de papers en revistas científicas e indexadas y congresos nacionales e internacionales. Además, ocupó el cargo de segundo Vicepresidente de la Cámara de Tecnologías de la Información y la Comunicación (CAMARA-TIC), actualmente ocupando el puesto de secretario del Consejo Directivo, miembro de la Asociación Dominicana de Inteligencia Artificial (ADIA). De igual forma ha sido colaborador de la Facultad Ingeniería de la Universidad Pontificia de Salamanca en Madrid (UPSAM), el Observatorio para la Cibersociedad y el Instituto para el Fomento de la Investigación Económica (Instituto FIEC) España.

FACILITADORES:

CÉSAR TOBÍAS ROSARIO BRADOR

Egresado de la Facultad Ciencias y Tecnología, escuela de Informática de la Universidad Católica Santo Domingo (UCSD), Maestría en Gerencia Moderna (UCSD), Maestría en Planificación y Gestión de la Educación (UCSD) y Especialidad en Crímenes y Delitos de Alta Tecnología.

Docente de la Facultad de Ciencias y Tecnología, escuela de Informática, de las asignaturas, Seguridad Informática, Ingeniera de Software, Ingeniera de Requisitos, Diseño y Administración de Centro de Datos, Calidad de Software y Sistemas & Procedimientos.

Apoyando al crecimiento intelectual y emocional de los futuros profesionales para que apliquen los conocimientos transmitidos, para el desenvolvimiento personal y profesional.

FACILITADORES:

FÉLIX RODRÍGUEZ

El Sr. Rodríguez es actualmente Gerente en los temas de Gobierno, Riesgos y Cumplimiento (GRC), así como los temas de Auditoría de Sistemas en Gorico Advasory Group, certificado como Auditor de Sistemas de Información (CISA) y Riesgos y Controles Tecnológicos (CRISC), de las más importantes certificaciones internacionales del área de Tecnología y vinculado al área de aseguramiento, riesgo y auditoría de TI desde hace más de diez años.

En su experiencia ha mantenido experiencia con importantes marcos como CobiT, COSO, PCI DSS, PMBOK, ISO 27000, entre otros que van directamente alineados a ciertas áreas operativas y financieras. De igual forma presenta experiencia en la alineación estratégica del Gobierno de TI con la Organización, revisiones del Control Interno, Seguridad de la Información, Centro de Cómputos, Mesa de Servicios, Desarrollo y Ciclo de Vida de Proyectos, Continuidad del Negocio y Recuperación ante Desastres, entre otras.

Con experiencia en las prácticas a nivel de los servicios de tecnología como ITIL, planes de continuidad del negocio y recuperación ante desastres (BCP-DRP).

Es Ingeniero de sistemas, graduado en la Universidad APEC (UNAPEC), posee maestría en gerencia de proyectos, Así como cursos especializados en temas de gobernanza y riesgos de TI, servicios tecnológicos y operaciones. Cuenta con la certificación de auditor CISA, así como en proceso de aplicación para la certificación de riesgos tecnológico CRISC (Certified in Risk and Information Systems Control) de ISACA. Posee conocimientos y experiencia docente en: Evaluaciones de Riesgos y Análisis de Impacto al Negocio (BIA), Control Interno y revisiones con el enfoque financiero, Infraestructura de TI, entre otras.

FACILITADORES:

FAUSTO RICHARDSON

Maestría en Ciberseguridad de la Universidad IMF Business Scholl y actual Estudiante de término del Doctorado en Proyectos en la Universidad Internacional Iberoamericana UNINI con maestría en gestión Universitaria con la universidad de Alcalá de Henares, España; y Maestría en sistemas de información con el Stevens Instituto of Tecnología. USA. Con una especialidad en Seguridad Nacional Ciberseguridad y otra en Derechos Humanos y Derecho Internacional Humanitario. Ha ocupado puestos como director de carrera de tecnología en universidades del país. Ha gestionado de manera satisfactoria proyectos de gran importancia para el ámbito militar y privado.

Ha acumulado vasta experiencia en ciberseguridad orientada al aseguramiento de los sistemas de información e infraestructura tecnológica. También como profesor de diversas áreas de TI, junto a esto también ha ocupado diversos cargos como encargado de áreas de TI y es actual encargado de la Dirección de Planificación y Desarrollo DNCD.

JUNIOR SANTANA

Es licenciado en Derecho por la Universidad Acción Pro-Educación y Cultura (UNAPEC), es Especialista en Derechos Humanos y Derecho Internacional Humanitario de la Escuela de Graduados en DDHH y DIH del Instituto Superior para la Defensa (INSUDE). Posee diplomados en Derecho administrativo constitucionalizado, derecho tributario y formulación y gerencia de proyectos.

Fungió como docente de introducción al estudio del Derecho, Derecho constitucional I y II en la en la Academia Naval de Estudios Superiores Vicealmirante César A. De Windt Lavandier, Armada de República Dominicana. Asimismo, docente sustituto en las cátedras de Derecho penal, Derecho procesal penal y Derecho procesal constitucional en la Universidad Católica de Santo Domingo. Fue Coordinador del ámbito de Justicia Penal en el Observatorio Judicial Dominicano (2014-2016). Investigador a tiempo completo del ámbito de justicia
constitucional y justicia administrativa (2016-2019) y coordinador de investigaciones por la misma institución hasta enero de 2020. Actualmente, es abogado del buffet de abogados Luna & Asociados, en las competencias penal y administrativo.

FACILITADORES:

JOHAN RODRÍGUEZ

Es Ingeniero en Tecnología de la Información y Comunicación (TIC) en la Universidad Iberoamericana UNIBE, posgrado en Transformación Digital Y Big Data y un Master en Comunicación Institucional ambos títulos otorgados por la Universidad Next Internacional Business School; Tecnólogo en Desarrollo de Software del Instituto Tecnológico de las Américas ITLA, con especialidades en gestión de requerimientos, arquitectura de software, gestión estratégica de las TIC, Entre otras, apasionado por los procesos de transformación e Innovación. En 2012 recibió el Premio UNIBE Ciencia Ambiental, por el trabajo de investigación sobre el uso dañino de los dispositivos electrónicos para el medio ambiente. Siendo así el primer equipo del área TIC en obtener este reconocimiento.

En su trayectoria profesional, ha dirigido proyectos de desarrollo y fortalecimiento institucional, implementación de nuevas tecnologías e infraestructuras que soportan a las mismas, así como procesos de innovación. Algunos de estos son: el Centro de Convenciones del Ministerio de Relaciones Exteriores y del Edificio de Tecnología de este ministerio. Además, coordinó y fue responsable de la parte tecnológica de la 46 Asamblea General de la OEA, celebrada en Santo Domingo, trabajó en el diseño de productos, procesos de levantamiento de información, planificación, entre otras actividades de República Digital en sus primeras etapas de Justicia Penal en el Observatorio Judicial Dominicano (2014-2016). Investigador a tiempo completo del ámbito de justicia constitucional y justicia administrativa (2016-2019) y coordinador de investigaciones por la misma institución hasta enero de 2020. Actualmente, es abogado del buffet de abogados Luna & Asociados, en las competencias penal y administrativo.

Ha trabajado en instituciones como: Dirección General de Contrataciones Públicas, apoyando sus procesos de transformación tecnológica, Ministerio de Relaciones Exteriores donde se desempeñó como Director General del Departamento de Tecnologías de la Información y comunicación. También ocupó el cargo de Director Ejecutivo de la Unidad Ejecutora del Componente Educación del Programa de República Digital, en el Ministerio de Educación.

Inversión y forma de pago:

El costo es de RD$ 25,000.00

Las formas de pago admitidas son: Efectivo, Tarjeta de Crédito, Cheque de Administración y Transferencia a cuenta bancaria.

1. Inscripción individual:

A. Pago convencional
- Llenar formulario SI-01
- Pagar el 40% de avance: RD$ 8, 800.00 pesos.
- Pagar dos (2) cuotas de: RD$ 6, 600.00 pesos.

Nota:
Al cumplirse el mes de haber iniciado el diplomado se vence la 1era. cuota. Si se paga con retraso se pagará un cargo de un 10% del valor adeudado.

B. Depósito o transferencia:

· Banco Popular Dominicano
Cuenta corriente número: 828134031

Nota: Enviar vía correo electrónico el voucher a: ventas@icda.edu.do con copia a cobros2@icda.edu.do. Teléfono: 809-535-0665 ext. 2321 y 2322.

C. Línea de crédito de FUNDAPEC:
- Llenar formulario SI-01
- Completar e imprimir formulario de solicitud de crédito en línea: https://www.fundapec.edu.do/

2. Inscripción Empresarial:
a) Llenar formulario SI-01
b) Carta compromiso de la empresa, sellada y firmada

Descuento:

Se dispone de descuentos aplicables en las siguientes condiciones:

1. Público General:
a) 10% de descuento por pago total en efectivo o depósito en cuenta.
b) 7.5% de descuento por pago total con tarjeta de crédito.

2. Público Empresarial:
c) 5% de descuento de 3 a 5 participantes
d) 10% de descuento de 6 a 10 participantes
e) 15% de descuento de 11 participantes en adelante

“PRECIOS SUJETOS A CAMBIOS”

CERTIFICADO:

El certificado del diplomado en Ciberseguridad será expedido por la Universidad Domínico Americano.
El alumno recibirá un diploma certificando la formación recibida tras superar satisfactoriamente todas las evaluaciones, prácticas y las horas del diplomado que no deben ser menor al 80% de participación.

BIBLIOGRAFÍA RECOMENDADA

1. Ezequiel Sallis, Claudio Caracciolo y Marcelo Rodríguez - Ethical Hacking. Un enfoque metodológico para profesionales
2. Antonio Salas - Los hombres que susurraban a las máquinas
3. Nassim Nicholas Taleb - El cisne negro.
4. Richard Bejtlich -The Practice of network security monitoring: Understanding incident detection and response
5. Chris Anley - The Shellcoder's Handbook; discovering and exploiting security holes
6. Mónica Valle - Ciberseguridad: consejos para tener vidas digitales más seguras
7. Simon Singh - Los Códigos Secretos: El arte y la ciencia de la criptografía, desde el antiguo Egipto a la era del Internet.
8. Angel Gómez Agreda - Mundo Orwell
9. Ben Clark - Rtfm: Read Team Field Manual
10. Andre Honing y Michael Sikorski - Practical Malware Analysis: a hands-on guide to dissecting malicious software
11. Peter Kim The hacker Playbook 3: practical guide to penetration testing

FORMULARIO INSCRIPCIÓN

UNICDA
UNIVERSIDAD DOMÍNICO AMERICANO

FORMULARIO DE INSCRIPCIÓN Y SOLICITUD DE CRÉDITO
SI-01

A CREDITO SI ( ) NO ( )

PAGADO POR EMPRESA SI ( ) NO ( )
% QUE PAGA LA EMPRESA _____% RD$_____

FACTURAR A LA EMPRESA		RNC	FECHA DE INSCRIPCION / /
NOMBRES		APELLIDOS	NIVEL ACADEMICO ALCANZADO
CEDULA O PASAPORTE - -	SEXO FEM. ( ) MASC. ( )	FECHA NACIMIENTO / /	LUGAR DE NACIMIENTO
ESTADO CIVIL SOLTERO ( ) CASADO ( )	TELEFONO RESIDENCIAL ( ) -	CELULAR / BEEPER ( ) -	E-MAIL
DIRECCION ACTUAL		LOCALIDAD	TRABAJA SI ( ) NO ( )
NOMBRE DE LA EMPRESA DONDE TRABAJA		PERSONA DE CONTACTO/ PAGO	DIRECCION DE EMPRESA
CARGO ACTUAL	DEPARTAMENTO	TELEFONO (S) EMPRESA ( ) -	EXTENSION ( ) FAX ( ) -
HA PARTICIPADO ANTERIORMENTE EN OTROS CURSOS DE UNICDA SI ( ) NO ( )		NOMBRE CONYUGE O PARIENTE	TELEFONO CONYUGE O PARIENTE ( ) -
FACTURA O CARTA AUTORIZADA DE EMPLEADOR SI ( ) NO ( )		PORQUE MEDIO SE ENTERO DE ESTE CURSO	

PROGRAMA

TITULO DEL DIPLOMADO O CURSO			GRUPO
DURACION	HORARIO-DIAS	FECHA INICIO / / 20	FECHA TERMINO / / 20

PARA USO EXCLUSIVO DE UNICDA

COSTO TOTAL DEL DIPLOMADO O CURSO RD$		COSTO A PAGAR POR INSCRIPCION RD$	BALANCE PENDIENTE A PAGAR RD$	
MODALIDAD DE PAGOS	1ERA CUOTA RD$	2DA CUOTA RD$		
FECHA DE PAGOS	1RA / / 20	2DA / / 20		

POLITICA DE REEMBOLSO Y COMPROMISO DE PAGO

Se devolverá el dinero que pague el participante solamente en el caso de que el curso o diplomado sea cancelado.	COMPROMISO DE PAGO: Me comprometo a pagar en las fechas indicadas y los montos estipulados en este formulario.En caso de faltar, autorizo a cancelar mi derecho de seguir participando en clases.

FIRMA DEL PERSONAL DE UNICDA Y/O CENTRO DE GERENCIA	FIRMA DEL PARTICIPANTE	FIRMA AUTORIZADA POR REGISTRO

CONTACTO:

Información adicional e inscripción

Universidad Domínico Americano

Web: www.unicda.edu.do

Twitter: @ElDominico

Facebook e Instagram:
@unicdard

Tel.: 809-535-0665 opción 3

Flotas: 829-417-1464 / 1465 y
829-748-5144 /5145

Email: ventas@icda.edu.do

Av. Abraham Lincoln #21. Santo Domingo,
República Dominicana