DIPLOMADO
¨CIBERDEFENSA Y CIBERSEGURIDAD ¨

Inteligencia Ref. No. ESI-D-CDS-2024	Nombre del Diplomado
Modalidad de Aprendizaje: A Distancia	Ciberdefensa y Ciberseguridad

Distribución por horas y Actividades de Aprendizaje por Componente POR CURSO/POR DIPLOMADO

Componentes	Actividades	Horas/Curso	Horas/Diplomado
Aprendizaje en contacto con el docente	• Clases, Tutorías, Conferencias, Seminarios, Talleres, Proyectos en aula (presencial o virtual).	30	90
Aprendizaje práctico – experimental	• Aplicación de contenidos conceptuales, procedimentales, técnicos, a la solución de: problemas prácticos, comprobación, experimentación, replicación.	5	15
Aprendizaje autónomo	• Lecturas, Análisis y comprensión de materiales bibliográficos y documentales, Generación de datos y búsqueda de información, Elaboración individual de ensayos, artículos, trabajos y exposiciones.	5	15
Total Horas		**40**	**120**

ANTECEDENTES:

La gran inmensidad de la nueva manifestación territorial, el ciberespacio, llegó para permanecer, llegó con grandes promesas de justicia, de educación, de desarrollo económico, social y cultural, de equidad, de integración, de instrumento eficaz para combatir el cambio climático y la pobreza material y moral, de liberación de trabajos repetitivos y embrutecedores.

Actualmente, es imposible concebir nuestra existencia sin el ciberespacio, que se ha insertado literalmente en todas las manifestaciones de las actividades humanas, pero también a él se han trasladado los conflictos y las contradicciones sociales en sus más diversas manifestaciones como la inseguridad en sus múltiples aspectos, han tomado forma los ataques contra los derechos individuales, colectivos, ambientales e informacionales, contra los Estados Nacionales, contra las infraestructuras críticas como las de aguas potables, el sistema energético, el sistema de salud, entre otros, por parte de muy variados actores.

El Ciberespacio como quinta manifestación territorial, de reciente evolución, necesita de formulación permanente y dinámica en términos de políticas públicas, gestión empresarial, tecnológica y seguridad cibernética.

OBJETIVO:

Proporcionar a los participantes los conocimientos integrales sobre ciberdefensa, ciberseguridad, ciberinteligencia, infraestruturas críticas, datos e información para fortalecer la seguridad cibernética, las infraestructuras críticas y el manejo de datos, de tal forma que puedan formular políticas, acciones concretas, para garantizar de mejor forma la soberanía y la integridad territorial de la nación, además, la seguridad de las instituciones, de las empresas públicas y privadas y, de las personas en el ciberespacio.

DIRIGIDA A:

Personas encargadas de la de seguridad nacional, ciudadana e integral, como: gerentes, directores y líderes en tecnología, militares directivos de todas las fuerzas, personal policial, integrantes del poder legislativo y judicial, desarrolladores de políticas públicas y regulación, organismos de inteligencia, ministerios de defensa, seguridad, y gobierno, ejecutivos de empresas de seguridad, sector financiero, sector de seguros, sector académico y de investigación. Administradores y responsables de la, instalación y operación de las infraestruturas críticas, tales como: las financieras, energéticas, militares, de salud, de agua potable, residuales, aeropuertos, puertos terrestres y marítimos, infraestructura petrolera, sistemas de logística (ductos y sistemas de transporte vía ferroviaria y carretera), centros de datos, servidores en nube instituciones gubernamentales, entre otras.

ESTRUCTURA:

La estructura del Diplomado se basa en el Reglamento para Carreras en la Modalidad en Línea y a Distancia. La organización del aprendizaje se sustenta en la estructura de las especializaciones, sin el componente de titulación. Cada curso tienen su base reglamentaria en el mencionado reglamento.

CONTENIDO:

El Diplomado está compuesto por tres cursos de educación contínua avanzada que pueden tomarse de forma independiente y tienen su propio certificado. El Certificado de asistencia y aprobación del Diplomado se otorgará a quienes hayan completado, aprobado los tres cursos y entregado el ensayo o artículo correspondiente.

Curso 1. Fundamentos de Ciberdefensa, Ciberseguridad y Ciberinteligencia.
Curso 2. Infraestructuras Críticas, Ciberdefensa y Ciberseguridad.
Curso 3. Datos y Seguridad Cibernética.

CURSO 1.
¨Fundamentos de Ciberdefensa, Ciberseguridad y Ciberinteligencia¨

Ofrece:

CITIC, Centro Internacional de Investigación Científica y Creación en Telecomunicaciones, Tecnologías de la Información y las Comunicaciones, Miembro Académico e la Unión Internacional de Telecomunicaciones UIT, organismo de Naciones Unidas ONU. Centro Regional de Capacitación de la Comisión Interamericana de Telecomunicaciones CITEL, organismo de la Organización de Estados Americanos OEA.

Seguridad Ref No. ESI - FCDSI -2024	Nombre del curso
Modalidad de aprendizaje: a distancia	Fundamentos de Ciberdefensa, Ciberseguridad y Ciberinteligencia

Distribución por horas y Actividades de Aprendizaje por Componente POR CURSO/POR DIPLOMADO

Componentes	Actividades	Horas/Curso
Aprendizaje en contacto con el docente	• Clases, Tutorías, Conferencias, Talleres, Proyectos en aula presencial o virtual	30
Aprendizaje práctico – experimental	• Aplicación de contenidos conceptuales, procedimentales, técnicos, a la solución de: problemas prácticos, comprobación, experimentación, replicación.	5
Aprendizaje autónomo	• Lecturas, Análisis y comprensión de materiales bibliográficos y documentales, Generación de datos y búsqueda de información, Elaboración individual de ensayos, artículos, trabajos y exposiciones.	5
Total Horas		**40**

ANTECEDENTES:

El ciberespacio ya se concibe como quinta manifestación territorial, actualmente, es imposible concebir nuestra existencia sin el ciberespacio, que se ha insertado literalmente en todas las manifestaciones de las actividades humanas, pero también a él se han trasladado los conflictos y las contradicciones sociales en sus más diversas manifestaciones como la inseguridad en sus múltiples aspectos, han tomado forma los ataques contra los derechos individuales, colectivos, ambientales e informacionales, contra los estados nacionales, las infraestructuras críticas, entre otros, por lo que es necesario tener un conocimiento diferenciado de la ciberdefensa, ciberseguridad y ciberinteligencia para fortalecer la seguridad cibernética, que trasciende los estados y las naciones a través del ciberespacio.

OBJETIVO: Proporcionar a los participantes los conocimientos integrales sobre los fundamentos de la ciberdefensa, la ciberseguridad y la ciberinteligencia, como estructuras fundamentales de la seguridad cibernética, de tal forma que puedan formular políticas, estrategias y acciones concretas para garantizar de mejor forma la soberanía y la integridad territorial de la nación, la seguridad de las instituciones, de las empresas públicas y privadas , así como de las personas, atacadas a través del ciberespacio.

DIRIGIDA A: Personas encargadas la ciberdefensa, la ciberseguridad y la ciberinteligencia así cómo a aquellas interesadas en profundizar temas relacionados con la seguridad cibernética a nivel nacional e internacional.

Conferencistas autores:

Dr. Mauro Flórez Calderón. PhD, Msc., Esp., Ing. PhD. Ingeniería de Telecomunicaciones. Msc. Ciencias Políticas. Esp. En Multimedia Ing. Electrónico. PhD (c) en Ciencias Políticas y Relaciones Internacionales. Profesor e investigador universitario, sobre el ciberespacio, por más de 30 añosProfesor de la Asignatura de Ciberseguridad y Ciberdefensa a los señores coroneles y capitanes de Navío, curso de Estado Mayor Conjunto de Ecuador en 2016 y 2017. Director Científico de la consultoría sobre ¨Seguridad de la Información y los Datos en Colombia¨ 2012 y del ¨Estudio de Impacto Socioeconómico de la adopción de IPv6 en Colombia¨ 2011 para Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC. Miembro Participante del Instituto Europeo de Normas de Telecomunicaciones (ETSI) Grupo de Especificación de la Industria (ISG) sobre Innovación Mejorada de IPv6 (IPE) 2021. Consultor de la Unión Internacional de

Telecomunicaciones UIT. Perito de la Comisión de Regulación de Telecomunicaciones de Colombia (hoy Comisión de Regulación de Comunicaciones CRC). Conferencista a nivel nacional e internacional. Consultor de la Unión Internacional de Telecomunicaciones UIT. Perito de la Comisión de Regulación de Telecomunicaciones de Colombia (hoy Comisión de Regulación de Comunicaciones CRC). Presidente de CITIC. Presidente de CITIC. PhD en Ingeniería de Telecomunicaciones. Msc. Ciencias Políticas. Esp. En Multimedia Ing. Electrónico. PhD (c) en Ciencias Políticas y Relaciones Internacionales.

Msc. Zoila Ramos Rodríguez, Msc., Esp., Ing., PhD (c). Directora General de la consultoría sobre ¨Seguridad de la Información y los Datos en Colombia¨ 2012 y del ¨Estudio Socioeconómico de la adopción de IPv6 en Colombia¨ 2011 para Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC. Council para Ecuador del Forum IPv6. Conferencista a nivel nacional e internacional. Consultora de la Unión Internacional de Telecomunicaciones UIT. Miembro Participante del Instituto Europeo de Normas de Telecomunicaciones (ETSI) Grupo de Especificación de la Industria (ISG) sobre Innovación Mejorada de IPv6 (IPE) desde el 2021. Perito de la Comisión de Regulación de Telecomunicaciones de Colombia (hoy Comisión de Regulación de Comunicaciones CRC). Directora General de CITIC. Ph.D. (c) y Msc. En Ingeniería de Telecomunicaciones, Especialista Radiocomunicaciones, Especialista en Derecho de las Telecomunicaciones, Diplomada en Innovación Pedagógica, Ingeniera Electrónica, Candidata a Abogada del Ecuador. Con estudios en Dirección de Empresas, autora y coautora de varios libros y artículos, Docente Investigadora Universidad Nacional de Colombia (jubilada), Consultora, Asesora, Interventora. Miembro Fundadora y Directora General de CITIC.

CONTENIDO:

Semanas.	**Módulos.**
	Módulo1. Caracterización de la ciberdefensa, de la ciberseguridad y la ciberinteligencia.
1	**Gestación de la ciberinteligencia.** Definiciones: ciberdefensa, ciberseguridad, seguridad informática, infraestructuras críticas, ciberguerra, y seguridad cibernética. Del telégrafo a la radio telegrafía. **Radiointeligencia.** La radio inteligencia y el conflicto Ruso – Japonés, 1905. Primera guerra mundial y la radio inteligencia. La radio difusión sonora y la televisión como ciberarmamento. **Guerra electrónica.** Radio navegación. El radar. El cifrado y el caso enigma. Los radioespias. Casos de esponje electrónico. El NORAD, La NASA, la NSA, El DARPA. **Seguridad cibernética.** Las manifestaciones territoriales. Beses ideológicas de la defensa nacional. Los nuevos actores en el ciberespacio. Etapas del ciberespacio.
2	**Módulo 2. Ciberterritorios.** Estructura del ciberespacio como manifestación territorial. La convención de Chicago. **Órbitas y sus tipologías.** Los países ecutoriales y la órbita geoestacionaria. Guerra y basura espacial. Oficina de Naciones Unidas para Asuntos del Espacio Exterior (UNOOSA).

	Espectro radioeléctrico. Rangos frecuenciales y propagación. Administración del radio espectro. Terminología espectral. Modelos de gestión espectral. Mecanismos de asignación. Regulación asimétrica. Las ciberembajadas.
3	**Módulo 3. La geopolítica y soberanías cibernéticas.** Ejemplos de múltiples hechos cibernéticos geopolíticos en las diferentes etapas de Internet. Los ciberespacios nacionales. Las grandes transnacionales del ciberespacio. El ciberespacio, las confrontaciones, las rutas de la seda y 5G. La lucha por las cibersoberanías nacionales y sus actores principales. La gobernanza, la seguridad cibernética y las soberanías en el ciberespacio. La ciberdiplomacia.
4	**Módulo 4. Ciberarmamento.** Marco de referencia argumentativo sobre el ciberarmamento. Necesidad del ciberarmamneto, el deber ser vs. el ser. Tipologías y clasificación del ciberarmamento. El cifrado. El cifrado y la Deep Web. Los malware. Las bombas de fuerza electromagnéticas. Señales, algoritmos, drones y redes sociales como ciberamamento. Control y robo de ciberarmamento. Empleo legítimo y traficantes de ciberarmamento. Ejemplos de múltiples fuentes de ciberarmamento. Grandes programas nacionales de ciberespionaje.
5	**Módulo 5. Tipologías del ciberreclutamiento y formación de los ciberguerreros**. Formación integral. Formación específica. Ciberreservas.: de concientización, operativas y de influencia. Formación de las élites. La salud mental. El cuadribiun . La oratoria militar y policial como poder individual e institucional. El cibereclutamiento. Industria nacional de seguridad cibernética. Algunas experiencias internacionales en la formación de ciberguerreros.
6	**Módulo 6. Escenarios de solución de ciberconflictos**. La ciberpaz. Carta de las Naciones Unidas. Consejo de Seguridad. Corte Internacional de Justicia. Consejo Europeo.

	Las ciberguerras y el derecho internacional. Convenio de Ginebra. Carta de la OEA. La OTAN y la seguridad cibernética. Manual de Tallin. Índice global de paz.
7	**Módulo 7. Estructura de la seguridad cibernética nacional integral.** Las amenzas **A**mbientales, **B**iológicas, **C**ibernéticas. Sistema Nacional de Seguridad Integral. Sistema Nacional de Seguridad Integral Cibernético. Matriz de riesgos. Ínide global de seguridad cibernética. Indicadores de la seguridad cibernética.
8	**Módulo 8. Ciberseguridad nacional, líneas de acción.** Objetivos globales de la seguridad cibernética. Las 9 líneas de acción para fortalecer la seguridad cibernética. Evaluación de la seguridad cibernética nacional. Guía Nacional estratégica de la seguridad cibernética nacional.

CURSO 2. INFRAESTRUCTURAS CRÍTICAS, CIBERDEFENSA Y CIBERSEGURIDAD.

Seguridad Ref No. ESI -C-ICCC – 2024
Modalidad de aprendizaje: a distancia.

CONTENIDO:

Semanas.	Módulos.
1	**Módulo 1. Evolución de la seguridad cibernética.** Panorama de amenazas globales. Paz e infraestructuras. Inicio de las telecomunicaciones. La radiointeligencia. La guerra electrónica. Inicio de las TIC. Seguridad cibernética. Ciberterritorios y soberanías nacionales.
2	**Módulo 2. Desafíos de la seguridad cibernética.** Étapas de extracción de información. Los servidores. Clasificación del ciberarmamento. El cifrado. Malware como ciberarmamento. Control del ciberarmamento. Formación de los ciberguerreros. Organismos y compromisos itternacionales.
3	**Módulo 3. Definiciones de infraestrutura crítica.** Definiciones de los sistemas integrantes de la seguridad cibernética. Definiciones varias de infraestructura crítica, de paises y de organismos internacionales. Infraestructura crítica. Infraestructura estratégica. Infraestructura de Información crítica. Operadores de infraestructuras críticas. Zonas críticas. Resiliencia.
4	**Módulo 4. Protección de las infraestructuras críticas en la Unión Europea y otros países.** Programa Europeo para la Protección de Infraestructuras Críticas, PEPIC. Justificación. Marco común del PEPIC. Principios básicos del PEPIC. Antecedentes del PEPIC. Objetivo global del PEPIC. Marco legislativo del PEPIC. Medidas de mejora del PEPIC. Coordinación del PEPIC. Plan de seguridad del operador.

	Experiencias de: Finlandia, Reino Unido, España.
5	**Módulo 5. Protección de infraestructuras críticas en América Latina y el Caribe.** Infraestructura verde y gris. Ciber amenazas en América Latina y el Caribe. Incidentes reportados por empresas Latina y el Caribe Controles de seguridad cibernética en América Latina y el Caribe. América Latina y el Caribe, grados de avances en seguridad cibernética.
6	**Módulo 6. Plan Nacional de Infraestructuras Críticas.** El Plan Nacional de Protección de las Infraestructuras Críticas. Responsabilidades de protección de la infraestuctura crítica. Módelo de protección de infraestructura crítica. Jerarquización del plan de protección de infraestructura crítica. Los Planes Estratégicos Sectoriales. Los Planes de Seguridad del Operador. Los Planes de Protección Específicos. Los Planes de Apoyo Operativo. Análisis de riesgo cibernético..
7	**Módulo 7. Catálogo de infraestructra críticas suceptibles de ciberataques.** Catalogación - Infraestructura crítica. Criticidad. Criticidad en el Reino Unido. Protección de infraestructura crítica. Indicadores de protección de infraestructura crítica. Los 15 indicadores de KPI. Formatos. Niveles de alarma. Experiencia Suiza.
8	**Módulo 8. Propuesta de protección de las infraestructuras críticas.** Marco Internacional para mejorar la seguridad cibernética de la infraestructura crítica Función Identificación, ID. Función Protección – PR. Función Detección - DE. Función Respuesta - RS. Función Recuperación – RC. Propuesta de proyecto de ley. CITIC. Visión holística.

CURSO 3. DATOS Y SEGURIDAD CIBERNÉTICA.

Seguridad Ref No. ESI – C - DSC – 2024

CONTENIDO:

1	**Módulo 1. Señales, datos, información y conocimiento.** Señales, datos, información y conocimiento. Información como gradiente entrópico. Significante, significado y signo. Código, criptografía y esteganografía. La hermenéutica y la hermética.
2	**Módulo 2. Conceptos básicos sobre seguridad de la información.** Confidencialidad, integridad, disponibilidad, seguridad, riesgo, vulnerabilidad. Ciberinteligencia, el cómo se recolectan los datos. Tipologías de ciberataques. Clasificación básica del ciberarmamento. Etapas y metodología de un ciberataque. Errores argumentativos frecuentes sobre protección de datos. Estándares y certificaciones de protección de datos. Guía de verificación de la seguridad de datos.
3	**Módulo 3. Metadatos.** Definicion de Metadatos. La OMPI y los metadatos. Ámbitos de los metadatos. Funciones de los metadatos. Ciclo de vida de los metadatos. Los riesgos de los metadatos. Herraminetas para acceder a los metadatos. Estándares de los metadatos. Ejemplos de metadatos.
4	**Módulo 4. Datos Abiertos.** Definición de Datos Abiertos. Los Objetivos del Desarrollo Sostenible y los datos abiertos. Justificaciones de la política de los datos abiertos. Declaración internacional sobre datos abiertos. Principios de los datos abiertos. Índice mundial de los datos abiertos. Correlación entre datos abiertos y los metadatos.
5	**Módulo 5. Los datos y la inteligencia artificial** Origen de los grande volúmenes de datos. Tipologías de la inteligencia. La inteligencia artificial en el sector financiero. La inteligencia artificial en diversos sectores. Riesgos de la inteligencia artificial. La inteligencia artificial y algunos impactos sociales. Antecedentes de la inteligencia artificial. La inteligencia artificial y la superinteligencia artificial.

6	**Módulo 6: Los datos y la seguridad con Ipv6** Los datos " el petroleo" de la sociedad de la información. Tipologías de los valores creados. Mercados de los datos. Desafios y oportunidades de los datos. Las transnacionales de los datos. IPV6 y la Seguridad Evolución. Transición y coexistencia. Errores comunes. Ventajas.
7	**Módulo 7. Los ciberdelitos.** Tipología de los fraudes. Ejemplos de ciberdelitos. Ejemplos de cibercriminales. El cibercrimen organizado transfronterizo. El convenio de Budapest. Medidas contra los ciberdelitos: ▪ Jurídicas. ▪ Técnicas. ▪ Organizativas. ▪ Capacitación. ▪ Cooperación.
8	**Módulo 8. Datos personales, derechos informacionales y ética.** Evolución de los derechos. De primera, segunda, tercera y cuarta generación. Los derechos informacionales. Los datos personales. ¿ Qué se entiende por datos personales? Los datos biométricos. La ONU y la privacidad. Las directices europeas sobre datos personales. Tendencias políticas sobre los datos personales. Elefecto dominó. ¿ Qué se entiende por ética? Ética Aristotélica. Virtudes occidentales y orientales. Reglas para la seguridad "éxitosa", de las TIC.

VALOR DE LA INVERSIÓN

POR CURSO:

Tres cientos noventa y cinco dólares americanos USD 395,oo más IVA.
BECA del 10% por pago total del curso hasta un día calendario antes del incio del curso.

POR DIPLOMADO:

Mil ciento ochenta y cinco (USD 1.185) más IVA.
BECA del 20% por pago total del diplomado hasta un día calendario antes del incio del curso.

PAGOS DIFERIDOS POR CURSO.

Pago 1: USD 95 hasta la fecha de inicio del curso.
Pago 2: USD 197,4 durante la tercera semana curso.
Pago 2: USD 150 durante la quinta semana del curso.

NOTAS IMPORTANTES.

NOTA1: favor remitir: los comprobantes de pago a pagos@citic.org.ec y enviar datos para la factura.
NOTA2.: enviar copia de la consignación (depósito) al correo: pagos@citic.org.ec. Incluir nombre de la empresa, institución participante y/o persona inscrita. No se harán devoluciones de dinero por concepto de pago de inscripciones y no asistencia al curso. El valor de la inscripción debe estar cancelado antes de iniciar el curso o diplomado, excepto las instituciones de los Estados que emitan la solicitud y aprobación de participar en el curso y/o diplomado a través de carta , fax, correo y/o mensaje electrónico con la lista de inscritos, documentos físicos y/o electrónicos que serán válidos para el envío y cobro de la factura.
NOTA3. Se abrirán los cursos y el diplomado con el número mínimo aprobado por CITIC y se aplazará para próxima fecha en caso de no completar. Si definitivamente no abrirse, a quienes hayan pagado se les devolverá el 100% del valor depositado en 30 días calendario máximo de declaratoria de cierre del curos o diplomado.

FORMAS DE PAGO.

EN ECUADOR: Cuenta Corriente Banco Internacional, No.000-027948-8
Beneficiario: CITIC
RUC: 1791942078001
DESDE EL EXTERIOR: Cuenta No. 000-027948-8 a nombre de CITIC
Código SWIFF: BINTECEQ
Banco destino: Banco Internacional
Dirección del Banco destino: Av. Patria E4-21 y 9 de Octubre, Quito – Ecuador
EN COLOMBIA:
Banco de destino: Bancolombia
Cuenta de ahorro No. 675-000001-80
Código SWIFT: COLOCOBM
Beneficiario: Fundación CITIC
NIT: 901129690
Dirección del Banco: Carrera 48 # 26 – 85, Medellín, Colombia