CURSO.
INFRAESTRUCTURAS CRÍTICAS, CIBERDEFENSA Y CIBERSEGURIDAD.

Del 24 de Mayo al 16 de Julio de 2021.

Ofrece:

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

Inteligencia Ref. ESI-CFCI-2021-1	Nombre del Curso
Modalidad de Aprendizaje: A Distancia	**Infraestructuras Críticas Ciberdefensa y Ciberseguridad**

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

Componentes	Actividades	Horas/Curso
Docencia	• Actividades de aprendizaje asistido por el profesor (Tutorías sincrónicas). • Actividades de aprendizaje colaborativo (Trabajo en grupo incluye las tutorías)	40
Prácticas y de aplicación y experimentación de los aprendizajes	• Resolución de problemas • Talleres	160
Aprendizaje autónomo	• Lecturas • Análisis y comprensión de materiales bibliográficos y documentales • Generación de datos y búsqueda de información • Elaboración individual de ensayos, trabajos y exposiciones	160
Total Horas		360

ANTECEDENTES

Las inffraestructuras que prestan servicios sin los cuales es imposible la vida, denominadas infraestructura críticas, tradicioanlmente han tendio defensas de carácter físico pero se encuentran la mayoría de ellas en indefensión casi total ante ataques de carácter lógico.

OBJETIVO

Proporcionar los conocimientos que permitan crear planes, estrategías, tácticas y mecanismo efectivos de defensa de las infraestructura críticas ante ataques de carácter lógico.

DIRIGIDO A:

Personas encargadas de las políticas y estrategias de seguridad nacional, ciudadana e integral, como: militares del Comando Conjunto de las Fuerzas Armadas, militares de todas las fuerzas, personal policial directivo, del poder legislativo y judicial, desarrolladores de políticas públicas y regulación, oficinas de intelgencia, ministerios de defensa, seguridad, y gobierno, ejecutivos de empresas de seguridad, sector financiero, sector de seguros, autoridades de universidades. Administradores y responsables de la, instalación y operación de las infraestruturas críticas, tales como: las financieras, energéticas, militares, de salud, de agua potable y residuales, aeropuertos, puertos terrestres y marítimos, sistemas de logística (ductos y sistemas de transporte vía ferroviaria y carretera), centros de datos, servidores en nube instituciones gubernamentales, entre otros.

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.

Conferencistas autores:

Msc. Zoila Ramos, Msc., Esp., Ing., PhD (c). **Directora General** de la consultoría sobre ¨Seguridad de la Información y los Datos en Colombia¨ 2012 y sobre ¨**Estudio Socioeconómico de la adopción de IPv6 en Colombia¨ 2011** para el Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC. **Council para Ecuador del Forum IPv6** desde el 2015. **Miembro Participante del Instituto Europeo de Normas de Telecomunicaciones (ETSI) Grupo de Especificación de la Industria (ISG) sobre Innovación Mejorada de IPv6 (IPE) 2021.** Consultora 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. Directora General de CITIC. Ph.D. (c). En Ingeniería de Telecomunicaciones, Especialista Radiocomunicaciones, Especialista en Derecho de las Telecomunicaciones, Diplomada en Innovación Pedagógica, Ingeniera Electrónica, Candidata a Abogada del Ecuador.

Dr. Mauro Flórez Calderón. PhD, Msc., Esp., Ing. PhD. **Director Científico** de la consultoría sobre ¨**Estudio de Impacto Socioeconómico de la adopción de IPv6 en Colombia¨ 2011 y** sobre ¨Seguridad de la Información y los Datos en Colombia¨ 2012 para Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC. Conferencista a nivel nacional e internacional. **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). Presidente de CITIC. PhD en Ingeniería de Telecomunicaciones. Msc. Ciencias Políticas. Esp. En Multimedia Ing. Electrónico. PhD (c) en Ciencias Políticas y Relaciones Internacionales.

VALOR DE LA INVERSIÓN.

Total curso: Tres cientos noventa y cinco dólares americanos USD 395, oo más IVA
Descuento para todos los países del 5% por pago total del diplomado **hasta un día antes** del inicio 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 Evento, excepto las instituciones del Estado ecuatoriano que deben enviar carta, fax, correo y/o mensaje electrónico con la lista de inscritos. Documentos físicos y/o electrónicos que serán válidos para el envío de la factura.

CUENTAS BANCARIAS.

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: Cuenta de Ahorros Banco de Colombia. BANCOLOMBIA. No. 675-000001-80
Beneficiario: Fundación CITIC
NIT: 901129690