

**MINISTERIO DE HACIENDA****CERTIFICADO DE APROPIACION PRESUPUESTARIA**

Sistema de Información de la Gestión Financiera

Período Fiscal : 2020

No. Expediente :

Fecha :	13	02	2020
	DD	MM	AAAA

No. Documento : EG1581605620510nwsTy

Capítulo : 0203-MINISTERIO DE DEFENSA  
 Sub Capítulo : 01-MINISTERIO DE DEFENSA  
 Unidad Ejecutora : 0026-Cuerpo Especializado de Seguridad Aeroportuaria y de Aviación Civil (CESAC)  
 Proceso : Participación en IV Congreso de informática forense y ciberseguridad IFC 2020.  
 No. Referencia :  
 Monto Total Proceso :  
 Moneda : PESOS DOMINICANOS

Se CERTIFICA que el Presupuesto General del Estado para el año 2020, aprobado por Ley No.506-19, dispone de balance de Apropiación Presupuestaria suficiente para iniciar procesos de contratación de bienes, obras y servicios por el monto indicado en este documento, en cumplimiento a lo establecido en el Decreto 15-17 del 08 febrero de 2017. De acuerdo al siguiente detalle :

Cuenta Presupuestaria	Nombre de la Cuenta Presupuestaria	Apropiación Presupuestaria 2020
2.2.8.7.04	Servicios de capacitación	170,240.00
Total		170,240.00

El monto de : \*\*Ciento setenta mil doscientos cuarenta con 00/100 (170,240.00)

Número de Preventivo	Fecha de Preventivo	Monto de Preventivo
2020.0203.01.0026.221-Versión 1	13/02/2020	170,240.00



Para la verificación de la integridad de este documento electrónico, ingresar a la siguiente dirección web:

<http://api-sigef.hacienda.gob.do/servicios/general/reporte/publico/RP1581606542407zE8qqBAn8N>





REPÚBLICA DOMINICANA  
MINISTERIO DE DEFENSA

CUERPO ESPECIALIZADO EN SEGURIDAD AEROPORTUARIA Y DE LA AVIACIÓN CIVIL  
CESAC

“LA SEGURIDAD ES RESPONSABILIDAD DE TODOS”

“Año de la Consolidación de la Seguridad Alimentaria”

AEROPUERTO INT.  
JOSÉ FRANCISCO  
PEÑA GÓMEZ  
Dirección de Seguridad  
Tel.: 809-549-8211  
Fax: 809-549-8215  
(MDSB)

AEROPUERTO INT.  
PUNTA CANA  
Dirección de Seguridad  
Tel.: 809-959-0289  
(MDPC)

AEROPUERTO INT.  
DEL CIBAO  
Dirección de Seguridad  
Tel.: 809-275-8079  
Fax: 809-233-8001  
(MDST)

AEROPUERTO INT.  
DE LA ROMANA  
Dirección de Seguridad  
Tel.: 809-813-9306  
(MDLR)

AEROPUERTO INT.  
GREGORIO LUPERÓN  
Dirección de Seguridad  
Tel.: 809-586-0335  
(MDPP)

AEROPUERTO INT.  
PRESIDENTE  
DR. JOAQUÍN BALAGUER  
Dirección de Seguridad  
Tel.: 809-826-4031  
(MDJB)

AEROPUERTO INT.  
PRESIDENTE  
JUAN BOSCH  
Dirección de Seguridad  
Tel.: 809-338-0075  
(MDCY)

AEROPUERTO INT.  
MARÍA MONTEZ  
Dirección de Seguridad  
Tel.: 809-524-4295  
(MDBH)

AERÓDROMO  
DOMÉSTICO  
ARROYO BARRIL  
Dirección de Seguridad  
Tel.: 809-538-3169  
(MDAB)

ESCUELA DE  
SEGURIDAD DE LA  
AVIACIÓN CIVIL  
Tel.: 809-549-8027  
Ext. 2061  
(ESAC)

1246

11 FEB 2020

**PRIMER ENDOSO:**

Del : Director General del Cuerpo Especializado en Seguridad Aeroportuaria y de la Aviación Civil (CESAC).

Al : Director Financiero del CESAC.

Asunto : Solicitud de dos (2) plazas para participar en el “IV Congreso Informática Forense & Ciberseguridad (IFC-2020)”, a ser impartido por la Empresa Technologyint, ICT.

Anexo : Oficio No.035, de fecha 4-2-2020, del Director de Tecnología de la Información y Comunicaciones del CESAC; y anexo.

1.- REFERIDO cortésmente, para los fines procedentes.

**ARACENIS CASTILLO DE LA CRUZ,**  
General de Brigada de Defensa Aérea, FARD

CC  
SV/PM  
mr.

Copia al: Director de Recursos Humanos,  
Director de Operaciones,  
Director de Tecnología de la Inf. y Comunicaciones del CESAC.





REPÚBLICA DOMINICANA  
MINISTERIO DE DEFENSA

CUERPO ESPECIALIZADO EN SEGURIDAD AEROPORTUARIA Y DE LA AVIACIÓN CIVIL  
CESAC

“LA SEGURIDAD ES RESPONSABILIDAD DE TODOS”

“Año de la Consolidación de la Seguridad Alimentaria”

04 de febrero de 2020.

**OFICIO-DTIC-035:**

Al : Director General del **CESAC**.

Del : Director de Tecnología de la Información y Comunicaciones del **CESAC**.

Asunto : Solicitud de 02 plazas para participar en el IV Congreso Informática Forense & Ciberseguridad IFC 2020; a impartir por la Empresa Technologyint.

Anexo : Brochure de la actividad. ✓

**Respetuosamente**, me permito solicitar a ese Superior Despacho, que salvo su más elevado parecer, a quien suscribe y al **Ing. José Alb. Montero de Peña**, se nos conceda la participación en el **IV Congreso Informática Forense y Ciberseguridad (IFC-2020)**, organizado por la empresa TechnologyInt, del 02 al 05 de abril del año en curso, a efectuarse en el Paradisus Punta Cana Resort, como lo indica el brochure anexo; hacemos este requerimiento con la intención de elevar nuestro conocimiento en el tema y de esta manera, brindar un mejor servicio en el desempeño de nuestras funciones.



**ING. TOMAS GARCIA**  
Capitán, ERD.

AEROPUERTO INT.  
JOSÉ FRANCISCO  
PEÑA GÓMEZ  
Dirección de Seguridad  
Tel.: 809-549-8211  
Fax: 809-549-8215  
(MDSB)

AEROPUERTO INT.  
PUNTA CANA  
Dirección de Seguridad  
Tel.: 809-959-0289  
(MDPC)

AEROPUERTO INT.  
DEL CIBAO  
Dirección de Seguridad  
Tel.: 809-275-8079  
Fax: 809-233-8001  
(MDST)

AEROPUERTO INT.  
DE LA ROMANA  
Dirección de Seguridad  
Tel.: 809-813-9306  
(MDLR)

AEROPUERTO INT.  
GREGORIO LUPERON  
Dirección de Seguridad  
Tel.: 809-586-0335  
(MDPP)

AEROPUERTO INT.  
PRESIDENTE  
DR. JOAQUÍN BALAGUER  
Dirección de Seguridad  
Tel.: 809-826-4031  
(MDJB)

AEROPUERTO INT.  
PRESIDENTE  
JUAN BOSCH  
Dirección de Seguridad  
Tel.: 809-338-0075  
(MDCY)

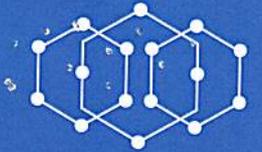
AEROPUERTO INT.  
MARÍA MONTEZ  
Dirección de Seguridad  
Tel.: 809-524-4295  
(MDBH)

AERÓDROMO  
DOMÉSTICO  
ARROYO BARRIL  
Dirección de Seguridad  
Tel.: 809-538-3169  
(MDAB)

ESCUELA DE  
SEGURIDAD DE LA  
AVIACIÓN CIVIL  
Tel.: 809-549-8027  
Ext. 2061  
(ESAC)

¡Somos Calidad!





IV CONGRESO DE INFORMÁTICA FORENSE Y CIBERSEGURIDAD

**IFC 2020**

Informática Forense & Ciberseguridad

ifcforensic.com

# IV CONGRESO DE INFORMÁTICA FORENSE & CIBERSEGURIDAD

02 al 05 de Abril del 2020

Hotel Paradisus, Punta Cana, República Dominicana

## PROGRAMA ACADEMICO

### JUEVES 2 (1er DÍA)

7:30 PM Cóctel de Bienvenida

### VIERNES 3 (2do DÍA)

8:30 AM



**Dr. Jeimy Cano**  
Colombia

Modelando al atacantes. Reto de defender y anticipar

El Doctor Cano es Ingeniero y Magister en Ingeniería de Sistemas y Computación por la Universidad de los Andes. Especialista en Derecho Disciplinario por la Universidad Externado de Colombia. Ph.D en Business Administration por Newport University, CA, USA, y Ph.D en Educación por la Universidad Santo Tomás, Colombia. Tiene más de 23 años de experiencia como académico, ejecutivo y profesional en seguridad de la información, privacidad, ciberseguridad, sistemas de información, gobierno y auditoría de TI. En 2014 fue condecorado por la Policía Nacional por su apoyo en la lucha contra la ciberdelincuencia y las investigaciones digitales en Colombia.

9:30 AM



**Ing. James Pichardo**  
Venezuela

Diseño y creación del Ciber-Escudo Nacional y su Impacto en las infraestructuras críticas y entidades gubernamentales.

Profesional en el área de Seguridad de Información con más de 10 años de experiencia en diversos sectores: comercial, académico, telecomunicaciones y gubernamental.  
- Director actual del Centro Nacional de Ciberseguridad, Presidencia de la República.  
- Gerente de Seguridad de Información (durante 3 años) del conglomerado de juegos en línea y apuestas más grande de Europa (bwin + party).  
- Ex-miembro de Dragón Research Group, un equipo de profesionales provenientes de diferentes partes del mundo, dedicados al estudio de la criminalidad en línea.  
- Fundador de DO-CSIRT, una organización dedicada a estudiar los aspectos relevantes de la seguridad en RD y dar soporte a la creación de CSIRTS

11:30 AM



**Ing. Seolito Rodríguez**  
Estados Unidos

Ataques tipo BEC y otros ataques sofisticados de PHISHING

El Ing. Seolito Rodríguez cuenta con más de 25 años de experiencia en el área de TI y seguridad de la información en los Estados Unidos, trabajando para compañías multinacionales, tanto del sector privado como del sector público. Actualmente se desempeña como Ingeniero en Sistemas en GoodwinLaw una de las principales corporaciones de abogados de EU con sede en Boston la cual cuenta además con oficinas en Europa y Asia.  
Seolito es experto en servidores de correos electrónicos entre otras tecnologías. Ingeniero en sistemas, tiene una Maestría en Administración de Empresas y cuenta con varias certificaciones: CISSP, CISM, CISA, CompTIA Security+, MCSE, MCT, VCP, ITIL, CCNA.

3:00 PM



**Ing. Carlos Leonardo**  
Rep. Dominicana

Operaciones de CSIRT-RD - Analisis de Amenazas en el Ciberespacio Dominicano

Director de Respuesta ante Incidentes Cibernéticos (CSIRT-RD), Centro Nacional de Ciberseguridad (DO), Dirección de Inteligencia (I2), Ministerio de Defensa, Asesor Tecnología y Ciberseguridad, Dirección de Inteligencia (I2), Ministerio de Defensa, DICAT (Departamento de Investigación de Crímenes y Delitos de Alta Tecnología), PN, Encargado Cooperación Internacional (PoC 24/7 Cibercrimen) - Analista Forense Digital, DICAT (Departamento de Investigación de Crímenes y Delitos de Alta Tecnología), PN, Policía Nacional, Coordinación de Proyecto de Mejoras, Análisis e Investigación de Ciberdelitos y Fraudes Electronicos, Análisis Forense Digital, Analista de Inteligencia de Datos.

3:30 PM



**Dra. Gabriela Saucedo**  
México

Analisis del informe anual de la Encuesta Latinoamericana de Seguridad de la Información

La doctora Gabriela Saucedo es Licenciada en Sistemas Computacionales y Maestra en Desarrollo Organizacional y Humano, ambos títulos conferidos por la Universidad del Valle de Atemajac (UNIVA) en Guadalajara, México. Ph.D en Educación por la Universidad Santo Tomás, Colombia. Fue Coordinadora de proceso de Acreditación Institucional y de proyectos institucionales de la UNIVA y Vicerrectora Académica y de Investigación del Instituto Politécnico Internacional, Bogotá, durante más de 5 años. Docente de Especializaciones en seguridad informática y riesgos informáticos en la Universidad Pontificia Bolivariana, sede Bucaramanga y Universidad Externado de Colombia respectivamente.

4:30 PM



**Lic. Félix Uribe**  
Estados Unidos

El Internet de las cosas (IoT) como vector d e ataques e incidentes de privacidad

Profesional de la ciberseguridad y la privacidad en la tecnología de la información (TI) con más de 20 años de experiencia en los sectores públicos y privados.

En el ámbito Académico, es Profesor Asociado Adjunto en la Escuela de Ciberseguridad y Tecnología de la Información de la Universidad de Maryland, Global Campus (UMGC) donde imparte cursos de ciberseguridad, privacidad y cibercriminalidad.

En el ámbito gubernamental y en el gobierno federal de los Estados Unidos, actualmente es un Oficial Federal de Privacidad y Analista de Seguridad de TI en el Departamento del Interior. En el Departamento de Justicia trabajo como auditor de ciberseguridad de TI en la Oficina de Auditoría del Inspector General donde fue responsable de auditorías de sistemas y programas informáticos para la seguridad nacional del país.

# FORO DE DISCUSIÓN

## "Diseño de arquitecturas digitalmente resilientes"

5:00 P.M.

Moderador  
Dr. Jeirny Cano  
Colombia

Laura Requena  
España

Lic. Luis Rauli Valencia  
México

Jose Antonio Ruiz  
México

Ing. James Pichardo  
Venezuela

# SABADO 04 (3er DÍA)

8:30 AM

Dra. Laura Requena  
España  
Comenzar desde el principio de Ciberseguridad

9:30 AM

Ing. Jean Carlos Bardot  
Venezuela  
DMARC - Configuración y Análisis

10:30 AM

Lic. Luis Rauli Valencia  
México  
RedTeam & DFIR, importancia en el entorno empresarial

11:30 AM

Ing. José Antonio Ruiz  
México  
Caerita de amenazas. El papel del SIEM y el SOC en la prevención de los ataques cibernéticos.

12:30 PM

Ing. Jesús García  
España  
La ciberseguridad en las infraestructuras críticas vista desde un CERT gubernamental

1:30 PM

Gral. Licurgo Yunes  
Rep. Dominicana  
Seguridad & Privacidad de los Datos, Impacto económico en las Organizaciones.

# SABADO 05 (4to DÍA)

# DOMINGO 05 (4to DÍA)

## NETWORKING Y SALIDA

## Entrega de regalos, certificados y clausura.

Se desempeña en la actualidad como Cyber Security Advisor & Security Analyst. Tiene más de diez años de experiencia en Pruebas de Intrusión (PenTest), Ingeniería Inversa, experto en manejo de incidentes y Security Intelligence mediante fuentes abiertas OSINT, Ethical Hacking, Project Management, Incident Handler, Secure Developer, Revers Engineering, México, 2017 - Certified Ethical Hacker, EC Council, 2017 - Certified Security Analyst, EC Council, 2012 - Certified Secure Program Manager, EC Council, 2013 - ISO/EIC 27001:2005 Information Security Management System Lead Auditor, RABQSA, 2016 - ISO/EIC 22301:2012 Business Continuity Management System Lead Auditor NYCE.

Ingeniero superior en Informática por la Universidad de León. Trabaja dentro del equipo de gestión de incidentes de ciberseguridad en el CERT gubernamental de España de INCIBE: INCIBE-CERT. Miembro de la vigente campeona selección española del campeonato mundial de hacking Cyber Shield 2019.

En materia de Ciberseguridad ha realizado cursos de entrenamiento y especialización en la academia del FBI, en Virginia, así como en la Guardia Civil de España. En materia de tecnología de la información ha obtenido entrenamiento y certificaciones en decenas de Países, en lo que podemos destacar: EE.UU., Israel, Japon y Francia. Es un profesional de tecnología de la Información y la Comunicación, con Postgrado en Gobierno Electrónico y maestría en Comercio Electrónico Internacional ha ocupado el puesto por más de 10 años como Comandante del Departamento contra Crimenes y Delitos de Alta tecnología en la República Dominicana, a ocupado puestos importantes tanto nacionales como internacionales dentro de sus 24 años de carrera policial y profesional.

# POLÍTICAS Y ESTRATEGIAS DE LA CIBERDEFENSA Y CIBERSEGURIDAD

## DIPLOMADO A DISTANCIA 2020 - I

FEBRERO 5 A JULIO 31 DE 2020

**¡NUEVA COHORTE! 20% de Descuento\***

\*Pagando antes del 31 de diciembre de 2019.

**CURSO 1**  
FEB 5 - MAR 31

Lineamientos de políticas y estrategias de la Ciberdefensa y Ciberseguridad

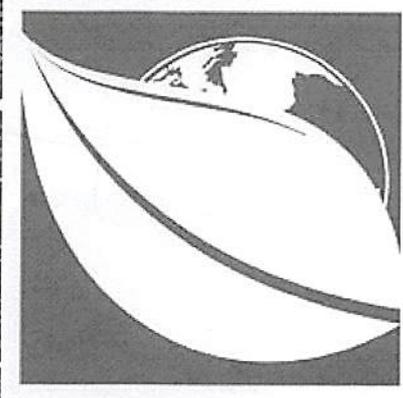
**CURSO 2**  
ABR 6 - MAY 29

Infraestructuras críticas Ciberdefensa y Ciberseguridad

**CURSO 3**  
JUN 8 - JUL 31

Lineamientos de uso de la información, datos y Big Data

Profesor Autor, Dr. Mauro Fábregas Calderón (PhD, Msc, Esp, Ing.)  
Director Escuela de Ciencias Políticas



# CITIC

☎ (+593) 2 233 3103  
☎ (+593) 98 778 5104  
@ citic@citic.org.ec

Centro de Capacitación Regional de  
CITEL - OEA  
www.citic.org.ec

**CURSO1. LINEAMIENTOS DE POLÍTICAS Y ESTRATEGIAS DE LA CIBERDEFENSA Y LA CIBERSEGURIDAD**

**Del 5 de febrero de al 31 de marzo de 2020**

**CONTENIDO Módulos/Semana**

- Módulo1.** Caracterización de la Ciberdefensa y de la Ciberseguridad.
- Módulo 2.** Ciber Territorio y Soberanías Nacionales.
- Módulo 3.** La Geopolítica Cibernética.
- Módulo 4.** Ciberarmamento
- Módulo 5.** Tipologías sobre el Ciberreclutamiento.
- Módulo 6.** Escenarios de Solución de Ciberconflictos.
- Módulo 7.** Ciberdefensa y Ciberseguridad Nacional
- Módulo 8.** Propuesta de Estructura de la Ciberdefensa Nacional y Regional

**CURSO 2. INFRAESTRUCTURAS CRITICAS, CIBERDEFENSA Y CIBERSEGURIDAD**

**Del 6 de abril al 29 de mayo de 2020**

**CONTENIDO Módulos/Semanas**

- Módulo 1.** Caracterización de la Ciberdefensa y la Ciberseguridad
- Módulo 2.** Nuevos desafíos de la Seguridad Nacional
- Módulo 3.** Definiciones de Infraestructura Crítica
- Módulo 4.** Protección de Infraestructuras Críticas en la Unión Europea y otros países.
- Módulo 5.** Protección de Infraestructuras Críticas en América Latina y el Caribe
- Módulo 6.** Plan Nacional de Infraestructuras Críticas
- Módulo 7.** Catálogo de Infraestructura Críticas susceptibles de Ciberataques
- Módulo 8.** Propuesta de Estructura de la Ciberdefensa Nacional y Regional

**CURSO 3. LINEAMIENTOS DE USO DE LA INFORMACIÓN, DATOS Y BIG DATA**

**Del 8 de junio al 31 de julio de 2020**

**CONTENIDO Módulos/Semanas**

- Módulo 1.** Revisión de Conceptos sobre Información y Datos
  - Módulo 2.** Revisión de conceptos sobre seguridad de la información.
  - Módulo 3.** Metadatos
  - Módulo 4.** Datos Abiertos
  - Módulo 5.** Enfrentando el desafío de los grandes volúmenes de datos (Big Data)
  - Módulo 6:** Generación de valor comercial, empresarial y de seguridad a partir de grandes volúmenes de datos (Big Data).
  - Módulo 7.** Detección y combate del fraude con herramientas como Big Data
  - Módulo 8.** Casos de éxito del uso de Big Data en la Seguridad.
- NOTA:** Incluye material de Oracle del curso de Introducción de Big Data (E-Kit en pdf) además del Certificado de Asistencia de Oracle

**CURSO1. LINEAMIENTOS DE POLÍTICAS Y ESTRATEGIAS DE LA CIBERDEFENSA Y LA CIBERSEGURIDAD**

**Del 5 de febrero de al 31 de marzo de 2020**

**CONTENIDO Módulos/Semana**

- Módulo1.** Caracterización de la Ciberdefensa y de la Ciberseguridad.
- Módulo 2.** Ciber Territorio y Soberanías Nacionales.
- Módulo 3.** La Geopolítica Cibernética.
- Módulo 4.** Ciberarmamento
- Módulo 5.** Tipologías sobre el Ciberreclutamiento.
- Módulo 6.** Escenarios de Solución de Ciberconflictos.
- Módulo 7.** Ciberdefensa y Ciberseguridad Nacional
- Módulo 8.** Propuesta de Estructura de la Ciberdefensa Nacional y Regional

**CURSO 2. INFRAESTRUCTURAS CRÍTICAS, CIBERDEFENSA Y CIBERSEGURIDAD**

**Del 6 de abril al 29 de mayo de 2020**

**CONTENIDO Módulos/Semanas**

- Módulo 1.** Caracterización de la Ciberdefensa y la Ciberseguridad
- Módulo 2.** Nuevos desafíos de la Seguridad Nacional
- Módulo 3.** Definiciones de Infraestructura Crítica
- Módulo 4.** Protección de Infraestructuras Críticas en la Unión Europea y otros países.
- Módulo 5.** Protección de Infraestructuras Críticas en América Latina y el Caribe
- Módulo 6.** Plan Nacional de Infraestructuras Críticas
- Módulo 7.** Catálogo de Infraestructura Críticas susceptibles de Ciberataques
- Módulo 8.** Propuesta de Estructura de la Ciberdefensa Nacional y Regional

**CURSO 3. LINEAMIENTOS DE USO DE LA INFORMACIÓN, DATOS Y BIG DATA**

**Del 8 de junio al 31 de julio de 2020**

**CONTENIDO Módulos/Semanas**

- Módulo 1.** Revisión de Conceptos sobre Información y Datos
  - Módulo 2.** Revisión de conceptos sobre seguridad de la información.
  - Módulo 3.** Metadatos
  - Módulo 4.** Datos Abiertos
  - Módulo 5.** Enfrentando el desafío de los grandes volúmenes de datos (Big Data)
  - Módulo 6:** Generación de valor comercial, empresarial y de seguridad a partir de grandes volúmenes de datos (Big Data).
  - Módulo 7.** Detección y combate del fraude con herramientas como Big Data
  - Módulo 8.** Casos de éxito del uso de Big Data en la Seguridad.
- NOTA:** Incluye material de Oracle del curso de Introducción de Big Data (E-Kit en pdf) además del Certificado de Asistencia de Oracle