ANEXO No. 5
ESPECIFICACIONES TÉCNICAS

	CURSOS ESPECIALIZADO EN TEMAS CIBERNETICOS
Ref articulo	DETALLE
	OBJETO: CAPACITACIÓN EN CURSOS ESPECIALIZADOS EN TEMAS CIBERNÉTICOS El Comando General requiere los servicios de capacitación especializados en temas cibernéticos de acuerdo con las siguientes especificaciones: • (02) Cursos personalizados en resolución de eventos de seguridad informática, análisis forense, redes y ética en habilidades avanzadas en informática, cada uno de dos fases • (05) Cursos certificados Ec-Council CND. • (05)Cursos certificados Ec-Council CSA. Estos cursos deberán ser prestados de acuerdo con las especificaciones técnicas de mínimo cumplimiento relacionadas a continuación.
1.	**CURSO PERSONALIZADO EN RESOLUCION DE EVENTOS DE SEGURIDAD INFORMÁTICA, ANÁLISIS FORENSE, REDES Y ÉTICA EN HABILIDADES AVANZADAS EN INFORMÁTICA**
1.1.	**DESCRIPCION: E**l servicio de capacitación deberá ser prestado en las instalaciones de la Escuela de Inteligencia Aérea (ESINA) de la fuerza aérea ubicado en el Aeropuerto el Dorado (CATAM) de Bogotá, en la cual se dispondrá para la totalidad de los alumnos y los instructores sin costo adicional para el oferente lo siguiente: • Aula • VideoBeam • Pizarrón (tablero Acrílico) • Computadores de Mesa con acceso a Internet y la capacidad de procesamiento necesario para la ejecución del curso y los laboratorios. Este servicio de capacitación para deberá ser prestado de la siguiente forma: • Deberá ser efectuado en dos fases con un total de 200 horas **académicas** sumando las dos fases. • Cada fase deberá ser efectuada en fechas diferentes de acuerdo a coordinación con el supervisor del contrato.
1.2.	**REQUERIMIENTOS GENERALES POR CADA CURSO :** • **ALUMNOS:** 18 Alumnos • **MODALIDAD:** presencial • **FASES:** Dos (02)
1.3.	
1	**Intensidad Horaria**: 120 Horas **académicas**
1	**Temario**: Resolución de Eventos de seguridad informática y Análisis Forense **1. Modulo: Resolución de eventos de seguridad (40 Horas)** El modulo en resolución de eventos de seguridad pretende dar pautas para el manejo de incidentes del día a día que pueden llegar a comprometer una organización si no se les da la atención y cuidado adecuado.

El Modulo se centra en temas generales como el análisis y procedimientos para el manejo de malware, configuraciones seguras, metodologías de actualización de software y análisis de incidentes en el cual como mínimo se deberán incluir los siguientes temas.

1.1. Introducción
1.1.1. Introducción al modulo
1.1.2. Tipos de eventos y categorización de incidentes
1.1.3. Las 5 falencias de las organizaciones.

1.2. Actualizaciones
1.2.1. Metodologías de actualización
1.2.2. Cuando actualizar
1.2.2.1. Un sistema operativo
1.2.2.2. Una aplicación
1.2.3. WSUS
1.2.4. Mejores prácticas de actualización.
1.2.5. Otras herramientas de actualización.

1.3. Configuración
1.3.1. Problemas del aseguramiento de plataformas
1.3.2. Configuraciones seguras y malas prácticas “Seguras”
1.3.3. Configuraciones Default.
1.3.4. Aseguramiento de servicios básicos Unix (SSH, NTP, etc.)
1.3.5. Aseguramiento de sistemas con Windows con GPO de active directory

1.4. **Contramedida de Malwar**e
1.4.1. Descripción y funcionamiento y propiedades de un malware
1.4.2. Objetivos y ciclo de vida de un malware
1.4.3. Cómo encontrar un Malware
1.4.4. Procedimientos de búsqueda de soluciones
1.4.5. Eliminación de software malicioso – casos prácticos
1.4.6. Búsqueda de tratamiento

1.5. Casos prácticos
1.5.1. The Post-man
1.5.2. ¿Qué tan mal estoy?
1.5.3. Memorias de una intrusión
1.5.4. El mundo no basta
1.5.5. la implementación de SIEM

2. Modulo Análisis de Logs (40 Horas)
Este Módulo en manejo y análisis de logs está orientada al manejo de procedimientos y definición de requerimientos sobre el manejo de los logs de los sistemas de Información. Por otro lado, se orienta al entendimiento y análisis de los logs dados por diferentes sistemas de logs (syslog, WinLog, IDS). Este módulo deberá incluir como mínimo los siguientes temas:

2.1. Introducción
2.1.1. Introducción al modulo
2.1.2. Historia del manejo de información
2.1.3. Importancia de los logs
2.1.4. Casos de la vida real

2.2. Metodología y procedimientos de manejo de logs
2.2.1. Identificación de necesidades y objetivos
2.2.2. Centralización de logs
2.2.3. Procedimientos básicos del manejo de logs

	2.2.4. Metodología de lectura de logs 2.3. Análisis de logs de IDS (basados en SNORT) 2.3.1. Reportes y salidas de IDS 2.3.2. Conociendo la red 2.3.3. Identificación de falsos positivos 2.3.4. Lectura de Logs 2.4. SysLog y Winlog 2.4.1. Protocolo Syslog 2.4.2. Estructura de logs Syslog 2.4.3. Estrucutra de logs Winlog 2.4.4. Lectura de logs Syslog y Winlog 2.5. Otros logs 2.5.1. Entendimiento y análisis de logs de proxys 2.5.2. Introducción a trampas SNMP 2.5.3. Manejo de información SNMP **3. Modulo Informática forense y respuesta a incidentes (40 Horas)** El módulo la respuesta, manejo y análisis de incidentes, dando los parámetros y procedimientos generales para la respuesta a incidentes, manejo del entorno organizacional en un incidente, análisis forense. Adicionalmente se revisarán los aspectos legales de un incidente y el uso de las tecnologías de la organización (sistemas operativos, firewalls, etc.) para el levantamiento de información relevante en una investigación. 3.1. Preparación técnica para la respuesta a incidentes 3.2. Preparación organizacional para la respuesta a incidentes 3.3. Técnicas de respuesta a Incidentes 3.4. Actuación del primer respondiente en escena de crimen 3.5. Recolección y Preservación de Evidencias Digitales en entornos corporativos 3.6. Recolección y Preservación de Evidencias Digitales en entornos hostiles 3.7. Embalaje y traslado a laboratorios 3.8. Montaje del ambiente de análisis 3.9. Aspectos técnicos de los medios de almacenamiento 3.10. Aspectos técnicos del análisis de redes 3.11. Análisis forense sobre en diferentes escenarios 3.12. Artefactos 3.13. Consideraciones Legales 3.14. Reporte y sustentación forense
1.4.	**FASE 2**
1	**Intensidad horaria : 80 horas.**
1	**Temario:** Redes y Ética de Habilidades avanzadas en informática **1. Módulo 1 Redes (24 Horas)** La capacitación en redes tiene como finalidad preparar al alumno para que aprenda y sea capaz de : -Diseñar redes de comunicación informática -Mantener redes locales de tipo LAN -Conocer aspectos relacionados con los protocolos -Establecer una seguridad informática en el entorno de gestión de cualquier empresa -Encriptar parte de las comunicaciones internas y externas de una organización empresarial **1.1. Los modelos de referencia - IEEE 802.3** 1.1.1. Organismos de estandarización 1.1.2. Arquitectura de la red en capas 1.1.3. Modelo OSI 1.1.3.1. Capa de aplicación

1.1.3.2. Capa de presentación
1.1.3.3. Capa de sesión
1.1.3.4. Capa de transporte
1.1.3.5. Capa de red
1.1.3.6. Capa de enlace de datos
1.1.3.7. Capa física
1.1.4. Modelo TCP/IP
1.1.4.1. Capa de aplicación
1.1.4.2. Capa de transporte
1.1.4.3. Capa de internet
1.1.4.4. Capa de acceso a red
1.1.4.5.
1.1.5. Direccionamiento IP
1.1.5.1. IPV4
1.1.5.1.1. Estatus actual del espacio de direcciones IPv4
1.1.5.1.2. Cabecera IP
1.1.5.1.3. Agotamiento de Direcciones IPv4
1.1.5.2. IPV6
1.1.5.2.1. Breve historia de protocolo
1.1.5.2.2. Encabezado IPv6
1.1.5.2.3. Direccionamiento IPv6, formatos y políticas de distribución y asignación de recursos.
1.1.5.2.4. DNS y conceptos fundamentales. Happy Eyeballs.
1.1.5.2.5. Ruteo en IPv6. Interno y externo. Conceptos de IPv6 en MPLS.
1.1.5.2.6. Nuevas características de IPv6 vs IPv4
1.1.5.2.7. Ventajas y Desventajas
1.1.5.2.8. Encabezados de extensión y opciones
1.1.5.2.9. Tipos de direcciones
1.1.5.2.10. Ejemplo: Esquema de direccionamiento para una empresa.
1.1.5.2.11. Discusión general: consideraciones de seguridad en IPv6
1.1.5.2.12. migración de IPV4 a IPV6
1.1.5.2.12.1. Requisitos Básicos
1.1.5.2.12.2. Proceso Previo al Cambio
1.1.5.2.12.3. Proceso de Migración de IPv4 a IPv6en Colombia

2. Módulo Ética de Habilidades avanzadas en informática (56 Horas)

La capacitación en Ética de una personal con habilidades avanzadas en informática, busca capacitar al personal en temas como análisis de vulnerabilidades, interpretación de herramientas, manejo de técnicas de Hacking, análisis de riesgo de los resultados frente a una organización y riesgos comunes dentro de una organización.

2.1. Presentación del curso
2.1.1. Ética y responsabilidad en habilidades avanzadas en informática
2.1.2. Modus operandi de los grupos de personas con habilidades y conocimientos avanzados en informática y de defensa nacional y contra-inteligencia de otros países.

2.2. Escaneo de puertos y enumeración (Explicación y laboratorio práctico)
2.2.1. Escaneo de puertos
2.2.2. Enumeración y aprovechamiento de servicios
2.2.2.1. En la enumeración de servicios se detallarán diferentes servicios, su funcionamiento y debilidades. Se desarrollará el ejercicio analizando el código fuente de la herramienta Scylla, además de la documentación referente a los protocolos.

2.2.2.1.1. SMB
2.2.2.1.2. DB2
2.2.2.1.3. Oracle

2.2.2.1.4. FTP
2.2.2.1.5. MSSQL
2.2.2.1.6. Telnet
2.2.2.1.7. LDAP
2.2.2.1.8. MySQL
2.2.2.1.9. Postgres
2.2.2.1.10. HTTP
2.2.2.1.10.1.1. Análisis de directorios, uso de métodos inexistentes, métodos de autenticación
2.2.2.1.11. DNS
2.2.2.1.12. Protocolos de Correo.

2.3. Explotación práctica
2.3.1. Tipos de Acciones Ofensivas
2.3.1.1. Acciones Ofensivas a software y servicios (Desbordamientos de buffer, Integer overflow, etc)
2.3.1.2. Acciones Ofensivas a aplicaciones Web
2.3.1.3. Intrusiones y tipos de intrusión
2.3.1.4. Técnicas de piratas informáticos para el acceso a la información
2.3.1.5. Falsos positivos
2.3.2. Acciones de fuerza bruta sobre sistemas informáticos.
2.3.3. Metodología de explotación de funcionalidad de protocolos
2.3.4. Network Sniffing y ARP Poisson Routing (Ejercicio práctico y explicación)
2.3.5. Explotación vía Metasploit Framework
2.3.6. Laboratorio: Ejercicio de explotación de máquina de prueba

2.4. Acciones Ofensivas web (Explicación y laboratorio)
2.4.1. Inyección SQL
2.4.2. Inyección HTML y JS (XSS)
2.4.3. Cross-Site request Forgery
2.4.4. XML External Entity (XXE) Processing
2.4.5. Data Tampering

2.5. Acciones Ofensivas a aplicaciones
2.5.1. Reverse engeneering (Java y .Net)
2.5.2. Análisis de aplicaciones
2.5.3. Fundamentos de ASM (prerequisito buffer overflows)
2.5.4. Buffer y heap overflow - enfoque práctico

2.6. Seguridad Wireless
2.6.1. Cracking WEP y WPA

2.7. Criptografía y criptoanálisis
2.7.1. Principios de criptografía y criptoanálisis
2.7.2. Protocolos criptográficos
2.7.3. Implementaciones criptográficas

2.8. Seguridad orientada a negocio
2.8.1. Vulnerability Assesment

1.5. MATERIAL REQUERIDO PARA EL DESARROLLO DE CADA CURSO EN LAS DOS FASES

- Máquinas Virtuales para el desarrollo de los Laboratorios.
- 01 Libro Guía En español con las presentaciones en Power Point por fases con todo el contenido y los ejercicios propuestos (Impreso, el cual deberá ser entregado al Supervisor del Contrato y en medio digital a los Alumnos.
    - Este libro deberá ser revisado y avalado por el supervisor del contrato previo inicio de

	cada fase. • Certificación de asistencia de cada alumno por cada fase. • Deberá contar con un mínimo de (06) Antenas Wifi para la realización de las prácticas de los diferentes alumnos. ○ Una de las características de estas es que permitan modo promiscuo de forma nativa, de mínimo 5dBi de potencia y adaptador USB
2.	**CURSO CERTIFICADO CND de Ec-Council** **Cantidad de Personas: CINCO (05)** Se debe hacer entrega de CINCO (05) Boucher para la realización y certificación del curso CND de Ec-Council, el cual deberá contemplar lo siguiente: • Curso presencial o **Virtual** en español: En un centro autorizado de entrenamiento (ATC) por Ec-Council, con los respectivos libros digitales generados por Ec-Council. **O por un instructor certificado para dictar el curso por el EC-Council en idioma español con los respectivos libros digitales generados por Ec-Council**. • Presentación del examen código: 312-38 (EXAMEN ECC)
3.	**CURSO CERTIFICADO CSA Ec-Council** **Cantidad de Personas: CINCO (05)** Se debe hacer entrega de CINCO (05) Boucher para la realización y certificación del curso CSA de Ec-Council, el cual deberá contemplar lo siguiente: • Curso presencial o **Virtual** en español: En un centro autorizado de entrenamiento (ATC) por Ec-Council, con los respectivos libros digitales generados por Ec-Council. **O por un instructor certificado para dictar el curso por el EC-Council en idioma español con los respectivos libros digitales generados por Ec-Council.** • • Presentación del examen código: 312-39

_____, identificado con cc No. _____ Expedida en _____, actuando en calidad de representante legal de la firma (o persona natural), manifiesto que cumplo con todas las especificaciones técnicas y experiencia requeridas y me comprometo a cumplir con el objeto del proceso bajo las condiciones técnicas sin condición alguna.

Así mismo declaro bajo la gravedad del juramento, comprometiendo nuestra responsabilidad personal e institucional de las personas jurídicas que representamos, que la información antes consignada es totalmente cierta, corresponde única y exclusivamente a la entidad que representamos.

Para constancia firmo, en la ciudad de Bogotá a los _____

_____
NOMBRE Y FIRMA REPRESENTANTE LEGAL
CC.