ECUADOR: NECESIDADES DE COOPERACION EN MATERIA DE CIBERDELITO

1. **Desarrollo de marcos legales nacionales para la penalización, asuntos procesales, prevención y cooperación internacional en el contexto de la Convención**

   Ecuador estaría interesado en recibir cooperación para la implementación de aspectos procesales, así como de prevención y de cooperación internacional en el contexto de la Convención de Budapest y de la futura Convención de Naciones Unidas contra el ciberdelito.

   Además, se agradecería recibir asesoría para elaborar manuales, instructivos y guías para el tratamiento de la evidencia digital, así como soporte legal y técnico para la implementación y operación del Centro de Seguridad Cibernético de la Policía Nacional.

   Adicionalmente, se requiere recibir asistencia técnica sobre los procedimientos a seguir en investigaciones de ciberdelitos con un alto grado de complejidad.

2. **Las áreas en las que Ecuador requiere capacitación son las siguientes:**

   Análisis estadístico y dinámico de códigos maliciosos
   Análisis y estudios criptográficos
   Análisis forense de servidores
   Análisis forense de infraestructuras híper convergentes
   Análisis forense en Sistemas Operativos Windows, Linux y iOS
   Análisis forense en dispositivos de almacenamiento
   Análisis de Malware
   Aplicación de la ciencia forense en los delitos informáticos y su punibilidad
   Aplicación del derecho sustantivo y procesal, así como sobre solicitudes y prestaciones de asistencia judicial recíproca en materia penal en temas vinculados al ciberdelito.
   Aspectos de jurisdicción para la investigación y juzgamiento de ciberdelitos
   Capacitación a los operadores de infraestructuras críticas en temas relacionados a ciberseguridad
   Desarrollo de procedimientos y herramientas de seguridad específicas tanto públicos como privados.
   Centro de respuesta emergente a incidentes de seguridad (CERT)
   Ciberseguridad
   Ciberdelitos
   Ciberinvestigación
   Ciberejercicios periódicos que pongan a prueba la capacidad de reacción frente a incidentes de ciberseguridad
   Concientización sobre la prevención de incidentes cibernéticos y ciberseguridad
   Derecho Informático
   Derecho de la Ciberseguridad y Entorno Digital
   Descifrado de base de datos de mensajería electrónica como WhatsApp
   Gestión de denuncias y prevención ante delitos cibernéticos
   Hacking ético
   Investigación en Cibercrimen
   Inglés técnico informático
   Investigación de incidentes en Base de Datos

Investigación en la DeepWeb
Investigación de Criptomonedas y Criptoactivos
Investigación en la Dark Web
Investigación de incidentes informáticos
Informática Forense y evidencia digital
La prueba en los ciberdelitos presentación y valoración
Nuevas modalidades del Ciberdelito
Manejo de herramientas OSINT avanzado
Minería de datos para la toma de decisiones en el combate a la ciberdelincuencia.
Pentesting
Protocolos y Directrices de agente encubierto en línea
Protección de las infraestructuras críticas y la eficacia de la respuesta a los incidentes que puedan afectarles: capacidades de detección y alerta temprana
Programación Básica y Avanzada
Preservación, adquisición y análisis de la evidencia digital
Procedimiento Técnico para la Investigación, Cadena de Custodia de la Evidencia Digital, Identificación de IP internacionales y presentación de los elementos de convicción en las Etapas del Proceso Penal
Respuesta a Incidentes cibernéticos
Reconocimiento, identificación e individualización de las evidencias digitales o materiales con el fin de determinar si un hecho es delito, cómo se cometió, dónde, cuándo y quién lo cometió.
Vulneración de propiedad intelectual en línea
Técnicas Especiales de Investigación de Ciberdelitos
Técnicas para la captura y análisis de tráfico de datos
Técnicas de Litigación Oral
Tecnología de apoyo investigativo

3. Equipo, software e infraestructura para la recolección y análisis de evidencia digital, y para la investigación y enjuiciamiento de delitos en el marco de la Convención

a. Dotación de herramientas tecnológicas que permitan adquirir, preservar, procesar y analizar la evidencia digital sin afectar su integridad, a fin de que pueda ser valorada adecuadamente en la etapa de juicio.

b. Desarrollo de un laboratorio para investigación, análisis, valoración y recuperación de evidencia digital, que cuente con tecnología forense digital, de acuerdo a las últimas tendencias, para investigar el uso de las TICS con fines delictivos, análisis de software malicioso como ramsomware, análisis de información en el metaverso, análisis de información en el dark web, etc.

c. Equipos, software e infraestructura para la adquisición, recolección y análisis de evidencia digital; procesos necesarios para el desarrollo de la investigación frente a hechos cometidos en el ciberespacio, tendientes a la obtención de evidencia digital que podrá ser utilizada en etapa de juzgamiento.

Hardware y Software

- Cuarto limpio para el análisis forense de dispositivos de almacenamiento
- Estaciones de trabajo forense

- Herramientas de Hardware y Software para Hacking Ético
- Herramientas para la extracción y análisis avanzado de datos
- Hardware de recolección de información in situ (Duplicador Forense)
- Para recolección, almacenamiento temporal de evidencia digital
- Plataforma de inteligencia web, para investigación digital a través de fuentes abiertas y cerradas
- Para mejoramiento y análisis de imagen y video
- Plataforma tecnológica para el monitoreo 24/7 de ciber amenazas internas y externas a nivel nacional e internacional
- Plataforma para el bypass o descifrado de contraseñas de dispositivos de telefonía celular
- Plataforma para la investigación de código malicioso
- Software de mejoramiento de imagen y video
- Software de recolección de información in situ (triage)
- Software para análisis dinámico y estático de código malicioso
- Software para rastreo de carteras criptográficas
- Software de análisis forense licenciado para PC multiplataforma
- Software para el descifrado de datos

Infraestructura

- Adecuación de la Unidad Nacional Especializada en Investigaciones de Ciberdelito
- Infraestructura de almacenamiento masivo de imágenes forenses e indicios recolectados dentro de la investigación para su análisis y protección
- Infraestructura para el monitoreo 24/7 en la DeepWeb
- Infraestructura tecnológica para fortalecer las unidades de la Policía Nacional y operar el Centro de Seguridad Cibernético
- Equipar a los vehículos policiales con herramientas tecnológicas para el monitoreo y análisis de redes

4. **Intercambio de mejores experiencias sobre la creación y desarrollo de relaciones efectivas con proveedores de servicios de internet y empresas del sector tecnológico.**

   Metodología de las alianzas existentes en los diferentes países con los sectores tecnológicos, así como también con proveedores de servicios a fin de que estos sean replicados en el Ecuador con el propósito de combatir la ciberdelincuencia.

   Conocer qué tipo de información se solicita a las diferentes proveedoras de servicio de Internet, así como las principales dificultades encontradas en el relacionamiento con el sector privado y cómo superarlas.

OFERTAS

La Policía Nacional del Ecuador, es pionera a nivel de Latinoamérica, en disponer de una herramienta informática para la obtención de reportes telefónicos en el marco de investigaciones de ciberdelitos.