ÍTEM	DESCRIPCIÓN
1	**DIPLOMADO EN ETHICAL HACKING Y SEGURIDAD DE LA INFORMACION**
1.1	**Cantidad de funcionarios a Capacitar:** 03
1.2	**Intensidad horaria:** De acuerdo con la programación que realice la Universidad
1.3	**Modalidad:** 100% virtual con acceso a los contenidos y actividades durante todo el periodo del diplomado. Incluye una sesión sincrónica semanal, en horarios previamente concertados con los participantes del programa académico.
1.4	**Entrega de certificación:** Entrega certificado digital de participación a cada asistente que haya cumplido, como mínimo, con el 80% de las actividades programadas y se encuentre a paz y salvo con los compromisos económicos adquiridos.
1.5	**Objetivo:** El Diplomado en ETHICAL HACKING Y SEGURIDAD DE LA INFORMACION: Desarrollo de Capacidades es un portafolio de competencias que mejora en las condiciones académicas de los funcionarios de la Policía Nacional y con esto generar mayor profesionalismo en el desempeño de los cargos relacionados con los procesos gerenciales, misionales y de soporte, se fortalecen las competencias profesionales del personal que integran la jefatura nacional de administración de recursos de la policía nacional, en los cargos del Grupo de tecnología de la información y las comunicaciones.
1.6	**Metodología:** El Diplomado en Ethical Hacking y seguridad de la información: Desarrollo de Capacidades se dictará de manera 100% virtual: Metodología que utiliza plataformas tecnológicas para conectar a las clases de forma sincrónica. 1.Competencia tecnológica: Es la capacidad de seleccionar y utilizar de forma responsable, pertinente y eficiente herramientas tecnológicas entendiendo los principios que las rigen, las diversas formas de combinarlas y las licencias que implican. 2. Competencia comunicativa: Es la capacidad de poder expresarse, establecer contacto y relacionarse en espacios virtuales y audiovisuales a través de múltiples medios y la implementación de varios lenguajes; de forma sincrónica y asincrónica. 3. Competencia pedagógica: Es la capacidad de utilizar las TIC para fortalecer los procesos de aprendizaje y enseñanza, identificando los alcances y limitaciones de la vinculación de este tipo de tecnologías en la formación integral de los estudiantes y su desarrollo personal. 4. Competencia de gestión: Es la capacidad de utilizar las TIC en la planeación, organización, administración y evaluación de manera efectiva y óptima de los procesos educativos; tanto para prácticas pedagógicas como de desarrollo institucional. 5. Competencia investigativa: Es la capacidad de utilizar las TIC para la transformación del saber y la generación de nuevos conocimientos.
1.7	Los componentes propuestos deben contemplar la solución integral y la gestión que se requiere para obtener los resultados de la capacitación, para contribuir al mejoramiento de la calidad educativa a través de las TIC, permitiendo un acceso a la educación de todos los estudiantes en sus prácticas educativas.

1.8

Contenido del diplomado

Módulo	Objetivo y Duración	Temática
Módulo 1 Fundamentos de SI y Criptografía	Familiarizar al estudiante en los conceptos fundamentales y la importancia de laCriptografía en la SI [2 semanas]	1.- Principios de la SI 2.- Seguridad física y lógica 3.- fundamentos de criptografía
Módulo II Ethical Hacking I (Introducción – Metodologías)	Iniciar el estudio de Ethical Hacking, cuáles son los tipos de análisis, metodologías utilizadas . [3 semanas]	1.- Introducción 2.- Tipos de análisis de seguridad 3. Metodologías utilizadas 4.- Presentación de informes
Módulo III Ethical Hacking II (Actividades prácticas)	Adquirir las destrezas y habilidades n las diferentes técnicas utilizadas. [4 semanas]	1.- Escaneo de redes 2.- Virus y gusanos 3.- Secuestro de sesión 4.- Hackeo de servidores web 5.- Hackeo de aplicaciones web 6.- Inyección de SQL 7.- Hackeo de redes inalámbricas 8.- Evasión de IDS, Firewalls, HoneyPots 9.- Desbordamiento de memoria 10.- Pruebas de penetración
Módulo IV Gestión del Riesgo, Auditoría de Sistemas de gestióny continuidad Negocio	Orientar al estudiante sobre los conceptos Fundamentales para llevar a cabo una gestión de riesgos efectiva, evaluara través del proceso de auditoría y .0diseñar y establecer un plan de continuidad de negocio.	1.- Conceptos generales de la gestión de riesgos. 2.- Metodología para la identificación, análisis. 3.- Metodología para diseñar, implementar y mantener un PCN. 4.- Planeación y ejecución de un programa de auditoría de sistemas de gestión. 5.- Estándares de auditoría a sistemas de información.

De igual forma, el proceso de formación se encuentra alineado con los principios de pertinencia, practicidad, acompañamiento, colaboración e inspiración.

1. **Pertinencia:** Los procesos de desarrollo profesional atienden los intereses y necesidades de los funcionarios y directivos teniendo en cuenta su rol; su área de formación, el nivel educativo en el que se desempeñan; sus saberes previos y el contexto cultural en el que se desenvuelven. Por encima de todo, deben estar encaminados a mejorar el aprendizaje de los funcionarios.
2. **Practicidad:** Los funcionarios aprenden utilizando directamente las TIC, explorando las herramientas de manera vivencial y aplicando lo aprendido en situaciones cotidianas de su profesión. Acompañamiento: Los procesos de desarrollo profesional se concentran en la institución educativa y en el aula, apoyados en la didáctica, brindan acompañamiento a los funcionarios para que reconozcan las necesidades y estilos de aprendizaje de sus estudiantes y puedan así transformar sus prácticas, a partir de la construcción de currículos diversos y la evaluación de aprendizajes y valoración de sus propias actuaciones.

1.9	**3. Colaboración:** Los procesos de desarrollo profesional facilitan y propician espacios para el aprendizaje conjunto, la creación colectiva, el intercambio entre pares y la participación en redes y comunidades de práctica. **4. Inspiración:** Los procesos de desarrollo profesional promueven la imaginación, la reflexión, el pensamiento crítico, la creatividad, el desarrollo de los talentos de los participantes y el deseo de aprender a aprender
1.10	El CONTRATISTA se obliga a no suministrar información que obtenga o conozca con ocasión de la ejecución del contrato, y que se encuentra marcada como confidencial; así como sobre los lugares a los cuales tenga acceso con ocasión de su desarrollo y sea revelada información marcada como confidencial. Por tal motivo, el contratista diligenció el formulario "ACUERDO DE CONFIDENCIALIDAD".
1.11	El contratista deberá cumplir con la implementación del Sistema de Gestión de la Seguridad y Salud en el Trabajo, para lo cual la contratista diligenció el formulario "SISTEMA DE GESTIÓN DE LA SEGURIDAD Y SALUD EN EL TRABAJO".
1.12	El contratista se obliga a cumplir con el compromiso de anticorrupción estando dispuesta a suministrar la información propia que resulte necesaria para aportar transparencia al mismo y si se comprueba el incumplimiento del contratista, sus empleados, representantes, asesores o de cualquier otra persona que actúe en su nombre, es causal para la terminación anticipada del contrato, para lo cual la contratista diligenció el formulario "COMPROMISO ANTICORRUPCIÓN".
	Valor unitario por estudiante de PRESTACIÓN DE SERVICIOS PROFESIONALES DIPLOMADO EN ETHICAL HACKING Y SEGURIDAD DE LA INFORMACIÓN PARA TRES (3) FUNCIONARIOS DE LA POLICÍA NACIONAL.

Capitán **JORGE ANDRES BEDOYA ARIAS**
Jefe Grupo de Tecnologías de la Información y las Comunicaciones-JENAR

Patrullero. **Luis Fernando Mosquera Barbosa**
Estructurador del Estudio Previo