**ANEXO 1**

**“CONSULTORÍA DE ETHICAL HACKING PARA LOS SERVIDORES Y SISTEMAS O APLICATIVOS EN EL AMBIENTE DE PRODUCCIÓN DEL MINISTERIO DE SALUD PÚBLICA PLANTA CENTRAL”**

## **DESCRIPCIÓN DE LA CONSULTORÍA**

La consultoría realizará dos hackeos éticos tanto interno como externo, su alcance y metodología se definirán según cada actividad.

El principal objetivo de esta consultoría es el ejecutar procedimientos de pruebas de penetración en los servidores y sistemas o aplicaciones en ambiente de producción del MSP, con la finalidad identificar, analizar y realizar una valoración de riesgo de las vulnerabilidades informáticas, realizar pruebas de explotación de vulnerabilidades informáticas encontradas bien conocidas o vulnerabilidades no conocidas, clasificadas como (criticas, altas, medias, bajas). Elaborar un informe técnico (que incluirá fotos de pantalla y pruebas de los hallazgos) mediante el cual describan los hallazgos y resultados, las estrategias/recomendaciones con base en los principios de seguridad de la información (disponibilidad, confidencialidad e integridad), lo cual permita remediar cualquier hallazgo intrusivo hacia los servidores y sistemas o aplicaciones de la institución.

La consultora deberá entregar un Plan de Trabajo, que contenga un cronograma con las actividades que se van a realizar como parte de la consultoría. Planificación de los recursos humanos y logísticos, que permitan cumplir con los objetivos.

El MSP a través de la Dirección de Tecnología de la Información y Comunicaciones (DTIC), entregará los insumos necesarios para contribuir al cumplimiento del objetivo solicitado, seleccionará y definirá los servidores y sistemas o aplicaciones en ambiente de producción aplicables para ser ejecutado en la consultoría. Las pruebas de penetración se llevarán a cabo utilizando herramientas automatizadas y manuales, que serán provistas por la consultora.

Las metodologías a utilizar durante las actividades de hackeo serán predeterminadas en conjunto con el equipo técnico del MSP y la empresa consultora.

Se deberá entregar un informe técnico e informe ejecutivo , sobre la identificación, análisis y realización de valoración de riesgo de las vulnerabilidades informáticas encontradas en los servidores y sistemas o aplicaciones en ambiente de producción, realización de las pruebas de explotación de vulnerabilidades informáticas encontradas bien conocidas y no conocidas clasificadas de nivel crítico, alto o mediano, estrategias/recomendaciones enfocadas en los principios de seguridad de la información (disponibilidad, confidencialidad e integridad). En función de los resultados obtenidos del procedimiento de hackeo ético (ethical hacking), el MSP generará en conjunto con el oferente el plan de acción para mitigar las vulnerabilidades encontradas. Esta documentación, así con los hallazgos encontrados y toda referencia a esta consultoría se entiende de alta confidencialidad y por consiguiente no puede ser divulgado sin autorización expresa de las autoridades pertinentes del MSP. Asimismo, los consultores que participen de la misma deberán firmar consentimientos de no divulgación y de reserva de la información, mediante la suscripción de un convenio de confidencialidad.

1. **ALCANCE**

Inicialmente el oferente deberá presentar un informe de plan de trabajo como instrumento de planificación, que permita ordenar y sistematizar la información de modo que pueda tenerse una visión de la consultoría a realizar, el mismo debe contener: objetivos, procesos de la ejecución del ethical hacking de los tipos caja negra, caja gris y caja blanca, procedimientos del ethical hacking, recursos, equipo de trabajo, cronograma de trabajo de la consultoría, conclusiones y recomendaciones.

Identificar, analizar y realizar una valoración de riesgo de las vulnerabilidades informáticas encontradas, además realizar pruebas de explotación de vulnerabilidades informáticas encontradas bien conocidas (clasificadas como críticas) siempre que se pueda llevar a cabo o en su defecto realizar la Prueba de Concepto (PoC) de explotación de las vulnerabilidades encontradas en los servidores y sistemas o aplicaciones en ambiente de producción del MSP (Anexo 8). La metodología de aplicación será mediante pruebas de penetración de seguridad tanto interna como externa de tipo caja negra (black-box), caja gris (gray-box) y caja blanca (white-box) según la necesidad del MSP.

La evaluación, detección de vulnerabilidades y pruebas de seguridad externa, será ejecutada por la consultoría sin denegación de servicio y de forma coordinada con el personal técnico del Ministerio de Salud Pública y en horarios que no afecten la disponibilidad de los servicios hacia los clientes. El análisis externo se lo ejecutará en modalidad “caja negra (black-box)”, es decir, las pruebas se hacen bajo la premisa de no conocimiento de las aplicaciones, sistemas, servidores a evaluar. Esto provee una simulación precisa de los tipos de ataque más comunes.

Posteriormente, la evaluación, detección de vulnerabilidades y pruebas de seguridad externa e interna, será ejecutada por la consultoría sin denegación de servicio y de forma coordinada con el personal técnico del Ministerio de Salud Pública y en horarios que no afecten la disponibilidad de los servicios hacia los clientes. El análisis externo como interno se lo ejecutará en modalidad “caja gris (gray-box)”, es decir, las pruebas realizadas se hacen bajo la premisa de conocimiento mínimo de las aplicaciones, sistemas, servidores a evaluar. Esto provee una simulación precisa de los tipos de ataque más comunes.

Luego, la evaluación, detección de vulnerabilidades y pruebas de seguridad interna será ejecutada por la consultoría sin denegación de servicio y de forma coordinada con personal técnico del Ministerio de Salud Pública y en horarios que no afecten la disponibilidad de los servicios hacia los clientes/usuarios. El análisis interno se lo ejecutará en modalidad “caja blanca (white-box)”, es decir, se realiza con pleno conocimiento de las aplicaciones, sistemas, servidores a evaluar y proporciona un examen sistemático de la arquitectura de seguridad existente.

Finalmente, la consultoría deberá analizar los resultados obtenidos a través de las tres modalidades caja negra (black-box), caja gris (gray-box) y caja blanca (white-box), presentará informes de Plan de Trabajo, Resultados Técnicos y Ejecutivo mediante el cual describan las estrategias/recomendaciones que permitan garantizar los principios de seguridad de la información (disponibilidad, confidencialidad e integridad), incluir conclusiones y recomendaciones, con la finalidad de que el personal del MSP pueda remediar las vulnerabilidades encontradas en los servidores y sistemas o aplicaciones en ambiente de producción. El tiempo de la consultoría y la entrega de todos sus productos será en un período máximo de 4 meses.

1. **METODOLOGÍA DE TRABAJO**

La consultoría se debe basar en mejores prácticas de Hacking Ético, así como metodología OWASP para la evaluación de aplicaciones Web y OSSTMM, NIST SP 800-115, ISSAF, PTES, PTF para las pruebas de Hacking Ético en general, según corresponda y deberá aplicar las buenas prácticas del Centro de Seguridad de Internet – CIS.

Con la finalidad de disminuir los falsos positivos, así como realizar un proceso más exacto y exhaustivo, se deben utilizar herramientas de nueva generación que permitan encontrar vulnerabilidades conocidas como no conocidas, clasificadas y no clasificas. Esta herramienta debe cubrir al menos los siguientes escenarios:

**Servidores:**

* Análisis de Sistema Operativo y Versión.
* Análisis de puertos y servicios.
* Análisis de Kernel/Procesador/Firmware (versión)
* Pruebas de acceso con credenciales por defecto.
* Explotación de vulnerabilidades bien conocidas (clasificadas como críticas) siempre que se pueda llevar a cabo o en su defecto realizar la Prueba de Concepto (PoC).

**Sistemas o aplicaciones a intervenir:**

* Análisis de Sistema Operativo y Versión.
* Análisis de puertos y servicios.
* Análisis de componentes Web (Ejm: PHP/APACHE/TOMCAT) y su versión.
* Análisis de componentes de BDD (Ejm: MySQL/SQL) y su versión.
* Pruebas de acceso con credenciales por defecto.
* Explotación de vulnerabilidades bien conocidas (clasificadas como críticas) siempre que se pueda llevar a cabo o en su defecto realizar la Prueba de Concepto (PoC).

1. **FASES DEL ANÁLISIS Y MONITOREO DE VULNERABILIDADES**

Durante la ejecución de las pruebas de vulnerabilidades de los servidores y sistemas o aplicaciones, tanto de tipo de caja negra, caja gris y de caja blanca, un equipo técnico del Ministerio de Salud Pública realizará actividades de monitoreo a los equipos y servicios ofrecidos por la institución para garantizar la disponibilidad de los servicios.

La consultoría debe, contar con las herramientas que cuenten con licenciamiento, suscripciones, y soporte técnico vigentes, que permitan disponer de todas las funcionalidades y servicios de análisis de vulnerabilidades requeridos.

Adicional, deberá cumplir con los criterios técnicos descritos en las siguientes fases en la ejecución de la consultoría:

|  |  |  |
| --- | --- | --- |
| **Fases** | | **Descripción** |
|  | Prerrequisitos | La empresa consultora como mínimo deberá contar con las certificaciones ISO 27001 o ISO 9001 o ISO 20000 o ISO 27700 y deberá ser miembro de entidades especializadas en respuestas de incidentes informáticos Foro Mundial de Equipos de Respuesta a Incidentes de Seguridad (FIRST).  El desarrollo de la consultoría deberá estar enmarcado en los lineamientos, metodologías y estándares internacionales OSSTMM, NIST 800-115, PTES, PTF, ISSAF, y OWASP, según correspondan. |
| Etapa Preliminar | Planificación | Al inicio de la consultoría, se mantendrá una reunión de trabajo entre la empresa Consultora y el Ministerio de Salud Pública, a fin de revisar el alcance de la consultoría y definir claramente las fechas de inicio de la consultoría y su finalización sin llegar a sobrepasar los 4 meses. Además, debido a que todas las actividades dentro de la presente consultoría serán manejadas bajo los más altos niveles de confidencialidad, se debe firmará un convenio de confidencialidad o de no divulgación |
| Se mantendrá una reunión de trabajo entre el equipo consultor y el Ministerio de Salud Pública para establecer prioridades, cronogramas de ejecución y la implementación de controles adecuados durante la ejecución del análisis de vulnerabilidades de tipo de caja negro, caja gris y caja blanca, de los servidores y sistemas o aplicaciones del MSP. |
| Ejecución | Las actividades a ejecutar serán las siguientes:   1. Descubrimiento inicial y escaneo de puertos externo (análisis y descubrimiento de recursos mediante el empleo de técnicas pasivas o activas, para determinar el perfil de los equipos a vulnerar, la arquitectura existente y sus posibles puntos de acceso) desde una o varias direcciones IP externas previamente notificadas al Ministerio de Salud Pública. 2. Detección y análisis de vulnerabilidades tipo black box (caja negra) de los servidores y sistemas o aplicaciones, desde una o varias direcciones IP previamente notificadas al Ministerio de Salud Pública (evaluación de la infraestructura pública visible desde el Internet; evaluación de dispositivos accesibles desde la red pública; evaluación de acceso de las aplicaciones expuestas en sitios públicos; evaluación del dominio msp.gob.ec). 3. Descubrimiento inicial y escaneo de puertos externo e interno (análisis y descubrimiento de recursos mediante el empleo de técnicas pasivas o activas, para determinar el perfil de los equipos a vulnerar, la arquitectura existente y sus posibles puntos de acceso) desde una o varias direcciones IP externas previamente notificadas al Ministerio de Salud Pública o desde una o varias direcciones IP internas propia de la red de producción del Ministerio de Salud Pública. 4. Detección y análisis de vulnerabilidades tipo gray box (caja gris) de los servidores y sistemas o aplicaciones, desde una o varias direcciones IP externa e interna previamente notificada al Ministerio de Salud Pública (evaluación de la infraestructura pública visible desde el Internet; evaluación de dispositivos accesibles desde la red privada; evaluación de acceso de las aplicaciones expuestas en sitios públicos; evaluación del dominio msp.gob.ec). 5. Descubrimiento inicial y escaneo de puertos internos (análisis y descubrimiento de recursos mediante el empleo de técnicas pasivas o activas, para determinar el perfil de los equipos a vulnerar, la arquitectura existente y sus posibles puntos de acceso) desde una o varias direcciones IP internas propia de la red de producción del Ministerio de Salud Pública. 6. Detección y análisis de vulnerabilidades tipo white box (caja blanca) de los servidores y sistemas o aplicaciones, desde una o varias direcciones IP interna previamente notificada al Ministerio de Salud Pública (evaluación de la infraestructura pública visible desde el Internet; evaluación de dispositivos accesibles desde la red privada; evaluación de acceso de las aplicaciones expuestas en sitios públicos; evaluación del dominio msp.gob.ec). 7. Formulación del perfil de riesgos técnicos identificados en el proceso de evaluación y propuesta del plan de mitigación y recuperación. |
| La empresa consultora deberá contar con al menos 4 fuentes de inteligencia licenciadas.  Además, la consultoría deberá contar e indicar las herramientas de última generación licenciadas, que se utilizará para gestionar y llevar adelante todos los requerimientos y objetivos planteados, así como para realizar el levamiento de información, su sistematización, documentación y dar seguimiento al avance del proyecto.  La metodología, instrumentos/herramientas ofertadas deberán contar con antecedentes comprobables de haber sido utilizadas y probadas en otras consultorías relacionadas, las mismas que podrían ser OSSTMM (Open Source Security Testing Methodology Manual), OWASP (Open Web Applications Security Project) Top 10, o Herramienta de pentest, etc. |
| La empresa consultora deberá brindar soporte para la gestión de incidentes con un pool de al menos 40 horas, dicho pool de horas podrá ser consumidas bajo demanda del MSP durante el periodo del contrato. |
| Nota importante: Si durante la ejecución del análisis de vulnerabilidades de las aplicaciones, sistemas y servidores tanto internas como externas, la consultoría detectará vulnerabilidades de seguridad críticas o altas que deban ser notificadas de forma inmediata al personal técnico del Ministerio de Salud Pública, para buscar su solución. |
| Etapa Final | Control | El equipo técnico de trabajo del MSP, en conjunto con la empresa Consultora, nombrado en la etapa de inicio, serán los encargados de la ejecución de las actividades programadas, En caso de requerir actualizar el cronograma de actividades, se deberá coordinar con el administrador del contrato. |
| Al cierre de la consultoría, la consultora deberá presentar los informes de hacking ético (black box, gray box y white box) que entre otros aspectos técnicos y conceptuales debe considerar al menos:   1. Estado de los servidores y sistemas o aplicaciones evaluadas con respecto a las mejores prácticas de la industria. 2. Impacto a la institución de las evidencias encontradas (Análisis de riesgos). 3. Recomendaciones de remediación y mejora con el grado de prioridad que debe contemplarse. 4. Informes técnicos de los resultados: detallados, descriptivo y ejecutivo. 5. Documentos de soporte que evidencien los resultados de las pruebas de penetración, indicando su forma de obtención y las herramientas que usó. |
| La consultora debe proporcionar la debida documentación técnica que se genere por la implementación de la herramienta de gestión de vulnerabilidades de los servidores y sistemas o aplicaciones. |

Tabla Fases del Análisis de vulnerabilidades

1. **INFORMES**

# INFORME DE PLAN DE TRABAJO

El Informe de Plan de Trabajo deberá reunir la información necesaria, que permita garantizar el desarrollo de las actividades, el cual deberá tener como mínimo la siguiente información:

* Objetivos
* Alcance
* Cronograma
* Prerequisitos técnicos
* Procesos para la ejecución del ethical hacking (caja negra/caja gris/caja blanca)
* Recursos
* Equipo de trabajo
* Conclusiones
* Recomendaciones

# INFORME DE RESULTADOS TÉCNICOS

Los resultados técnicos deberán ser entregados en tres informes separados uno de caja negra (black box), otro caja gris (gray-box) y finalmente uno de caja blanca (white box) con el formato previamente acordado por las partes, el mismo que tendrá el carácter de confidencial, donde se describirá detalladamente el estado en que se encuentra el nivel de seguridad del MSP, incluyendo información del hallazgo, fotos de pantalla del hallazgo, información de referencia de la vulnerabilidad identificada, y recomendaciones para la mitigación de cada riesgo.

El informe debe describir la identificación, análisis y realización de la valoración de riesgos de las vulnerabilidades informáticas encontradas en los servidores y sistemas o aplicaciones, también la realización de las pruebas de explotación de vulnerabilidades informáticas encontradas bien conocidas (clasificadas como críticas), finalmente debe incluir las estrategias/recomendaciones que permitan garantizar principios de seguridad de la información (disponibilidad, confidencialidad e integridad), en función de los resultados obtenidos del procedimiento de hackeo ético (ethical hacking).

El formato del como mínimo deberá contener un acápite que detalle lo siguiente:

* Introducción.
* Objetivo.
* Alcance.
* Identificación de vulnerabilidades
* Valoración de vulnerabilidades
* Análisis de riesgos
* Plan de remediación de vulnerabilidades.
* Matriz de involucrados.
* Metodología e instrumentos/herramientas de trabajo.
* Estrategia de abordaje
* Conclusiones.
* Recomendaciones.

# **INFORME EJECUTIVO**

Los informes (caja negra (black box), caja gris (gray box) y caja blanca (white box)) deberán constar de un informe resumen de tipo ejecutivo, el mismo que tendrá el carácter de confidencial, y que deberá ser presentado al nivel de autoridades del MSP en una reunión en la que se debe efectuar una presentación del mismo.

* 1. **RESPALDO EN MEDIO MAGNÉTICO**

La consultoría contratada, al final de la evaluación entregará los informes de Plan de Trabajo, Resultados Técnico y Ejecutivo en original y una copia impresos, en idioma español, adjuntando un CD con la información que contengan dichos informes y la información de respaldo (resultados de las pruebas).

1. **EQUIPO DE TRABAJO**

La consultoría tiene que demostrar documentadamente que cuenta con el personal técnico idóneo, infraestructura tecnológica y recursos necesarios para las prestaciones de ethical hacking que tiene objeto de la contratación, en cumplimiento de los requisitos mínimos solicitados en el presente documento.

El desarrollo de la consultoría deberá estar enmarcado en los lineamientos, metodologías y estándares internacionales OSSTMM, NIST 800-115, PTES, PTF, ISSAF, y OWASP, según correspondan, para lo cual en el cronograma detallado de ejecución se deberá establecer la aplicabilidad de los mismos, considerando adicionalmente las buenas prácticas emitidas por el Centro de Seguridad de Internet – CIS.

La consultoría proveerá de personal con experiencia comprobable en el área de análisis de vulnerabilidades y explotación de estas, seguridad informática, pruebas de penetración familiarizados con la arquitectura de servidores y sistemas o aplicaciones que se disponen en las diferentes entidades de preferencia en el área de Salud. Se deberán presentar certificados laborales que especifiquen la fecha certificado, empresa, periodo en que realizó los trabajos, monto del proyecto, nombre de la persona o personas a quien se emite el certificado que avale tal particular.

1. **Perfiles Técnicos**

Para certificar la experiencia del personal técnico, se debe adjuntar copia de la hoja de vida, títulos, actas, certificados laborales, de manera que la suma del plazo de los proyectos cumpla con el tiempo de experiencia requerida.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Función y Descripción** | **Cantidad** | **Nivel de Estudio** | **Título Académico** | **Tiempo de Experiencia** | **Número de Proyectos Mínimo** |
| Gerente de Proyecto: Experiencia en la Gerencia de proyectos de seguridad de la información. | 1 | Tercer nivel (pregrado) con título. | Ing. Sistemas, o Ing. en Telemática, o Ing. Electrónico, o Ing. En Redes, o Ing. de Desarrollo, o Ing. En Telecomunicaciones, o Ing. En Sistemas Informáticos y Computación. | Dentro de los últimos 5 años de experiencia | 3 Proyectos |
| Consultor Líder de Seguridad: Experiencia en Hacking Ético. | 1 | Tercer nivel (pregrado) con título | Ing. Sistemas, o Ing. en Telemática, o Ing. Electrónico, o Ing. En Redes, o Ing. de Desarrollo, o Ing. En Telecomunicaciones, o Ing. En Sistemas Informáticos y Computación. | Dentro de los últimos 5 años de experiencia | 3 Proyectos |
| Consultor de Seguridad: Experiencia en Hacking Ético. | 1 | Tercer nivel (pregrado) con título | Ing. Sistemas, o Ing. en Telemática, o Ing. Electrónico, o Ing. En Redes, o Ing. de Desarrollo, o Ing. En Telecomunicaciones, o Ing. En Sistemas Informáticos y Computación. | Dentro de los últimos 3 años de experiencia | 2 Proyectos |

*Tabla 3 Perfiles Técnicos*

El personal técnico como mínimo debe contar con los siguientes parámetros:

|  |  |  |
| --- | --- | --- |
| **N°** | **Parámetro** | **Dimension** |
| 1 | **Gerente de Proyecto:**  **\***Certificaciones de PMP  Certificación internacional PMP o SCRUM, proyectos, o título de cuarto nivel en administración de empresas/proyectos. | Certificado internacional PMP o certificado SCRUM, vigentes, o título de cuarto nivel. (copia simple), |
| 1 | **Consultor Líder de Seguridad:**  \*Certificaciones o cursos de:  Pentest/Penetración o cursos de Ethical Hacking, o cursos de seguridad informática, o cursos de seguridad de la información, o cursos de ciberseguridad, o Certificación CEH (Certified Ethical Hacker) o ISS (Information Security Specialist) o Offensive Security Certified Professional (OSCP) o Certificación eLearnSecurity Web Application Penetration Tester (eWPT) o CCTIA (Certified Cyber Threat Intelligence Analyst), o título de cuarto nivel en TIC en: Seguridad Informática, o Seguridad de la Información, o Seguridad de Redes/Datos, o Ciberseguridad, o Auditoría Informática. | Certificación de cursos, o título de cuarto nivel. (copia simple), |
| 1 | **Consultor de Seguridad:**  \*Certificaciones o cursos de:  Pentest/Penetración o cursos de Ethical Hacking, o cursos de seguridad informática, o cursos de seguridad de la información, o cursos de ciberseguridad, o  Certificación CEH (Certified Ethical Hacker) o ISS (Information Security Specialist) o Offensive Security Certified Professional (OSCP) o Certificación eLearnSecurity Web Application Penetration Tester (eWPT) o CCTIA (Certified Cyber Threat Intelligence Analyst), o título de cuarto nivel en TIC en: Seguridad Informática, o Seguridad de la Información, o Seguridad de Redes/Datos, o Ciberseguridad, o Auditoría Informática. | Certificación de cursos, o título de cuarto nivel (copia simple). |

*Tabla 4 Certificaciones para perfiles técnicos*

1. **RECURSOS**

Debido a la especialización requerida para cumplir con los objetivos, se entiende necesario y se valorará especialmente que la consultoría cuente con recursos en talento humano de alta especialización en experiencia, participación e implementación de programas similares, de preferencia en modelos de gestión de salud nacional, y proyectos nacionales de sistemas de información en salud.

La consultoría como mínimo deberá contar con las certificaciones ISO 27001 o ISO 9001 o ISO 20000 o ISO 27700 y deberá ser miembro de entidades especializadas en respuestas de incidentes informáticos Foro Mundial de Equipos de Respuesta a Incidentes de Seguridad (FIRST).

Además, la consultoría deberá contar e indicar las herramientas de última generación licenciadas, que utilizará para gestionar y llevar adelante todos los requerimientos y objetivos planteados, así como para realizar el levamiento de información, su sistematización, documentación y dar seguimiento al avance del proyecto.

La metodología, instrumentos/herramientas ofertadas deberán contar con antecedentes comprobables de haber sido utilizadas y probadas en otras consultorías relacionadas, las mismas que podrían ser OSSTMM (Open Source Security Testing Methodology Manual), OWASP (Open Web Applications Security Project) Top 10, o Herramienta de pentest, etc.

Durante el tiempo de ejecución de la consultoría el MSP podrá solicitar acceso a dichas herramientas, pero en ningún caso insumirá costos adicionales para éste, por lo cual deberá correr a cuenta de la consultoría.

1. **CAPACIDAD DE LA CONSULTORÍA**

La consultoría deberá presentar los sustentos que demuestren su experiencia dentro de los últimos 5 (cinco) años, en trabajos de: ethical hacking o seguridad en redes y telecomunicaciones, o en auditoría informática, o ciberseguridad, o en seguridad de la información ya sea en el Sector Público o Privado.

1. **PRODUCTOS ESPERADOS DE LA CONSULTORÍA**

El MSP espera que la consultoría proporcione los siguientes productos, mismo que se detallan en la siguiente Tabla 5.:

|  |  |  |
| --- | --- | --- |
| **Fases** | | **Producto Esperado** |
| Etapa Preliminar | Planificación | * Informe de Plan de Trabajo. |
| Ejecución |
| Etapa Final | Control | * Informe de Resultados Técnicos * Informe Ejecutivo. * Presentación de Resultados. * Respaldos en medio magnético del escaneo de vulnerabilidades en los servicios y sistemas o aplicaciones en ambiente de producción del MSP. |

*Tabla 5 Productos Esperados*

1. **CRONOGRAMA Y ENTREGABLES**

A continuación, se detallan los entregables mencionados y su cronograma de entrega a partir de la firma de contrato (días calendario), como se muestra en el siguiente cuadro:

|  |  |  |  |
| --- | --- | --- | --- |
| **Cronograma** | **Fases** | | **Producto Esperado** |
| 15 días | Etapa Preliminar | Planificación | * Informe de Plan de Trabajo.   Consiste en el cronograma y actividades a realizarse.  Temario de todos los temas o actividades a desarrollarse |
| 60 días | Ejecución | * Informe de Resultados Técnicos |
| 15 días | Etapa Final | Control | * Informe Ejecutivo. |
| 30 días | * Presentación de resultados a nivel de autoridades del MSP * Respaldos en medio magnético del escaneo de vulnerabilidades en los servicios y sistemas o aplicaciones en ambiente de producción del MSP * Preparación documental por parte del Administrador de Contrato para el pago |
| 120 días | **TOTAL** | | |

Tabla 6 Cronograma Entregables

El cronograma podrá estar sujeto a cambios siempre y cuando las dos partes (MSP y la empresa CONSULTORA) estén de acuerdo. Sin que esto afecte el plazo contractual.