GRUPO HORUS

Asunción, 13 de enero de 2023.

Señor
RICHARD FABIAN BADDOUH BERNI, Coordinador Proyectos TIC
Unidad Ejecutora de Programas y Proyectos (UEPP)
MINISTERIO DE EDUCACIÓN Y CIENCIAS (MEC)

REF.: Entrega del Producto 1 "Plan de Trabajo", conforme a la Orden de Inicio de Servicios de fecha 04 de enero de 2023, en el marco del Contrato N°07-22 CD – Contratación Directa Nº 01/2022 "CONSULTORIA PARA EL DIAGNOSTICO Y EVALUACIÓN DE LA SEGURIDAD DE LOS SISTEMAS TRANSACCIONALES DEL MEC (HACKING ETICO) - SEGUNDO LLAMADO" ID: 416.862.

De nuestra mayor consideración,

Tenemos el agrado de dirigirnos a Usted en el marco del *Contrato N°07-22 CD – Contratación Directa Nº 01/2022 "CONSULTORIA PARA EL DIAGNOSTICO Y EVALUACIÓN DE LA SEGURIDAD DE LOS SISTEMAS TRANSACCIONALES DEL MEC (HACKING ETICO) - SEGUNDO LLAMADO"ID: 416.862*, con el objeto de realizar la entrega del siguiente Producto:

- Producto 1: 1 (un) Plan de Trabajo: que contiene el enfoque técnico, la metodología de trabajo, el cronograma de actividades y la previsión de entrega de los productos esperados.

Aprovechamos la oportunidad para saludarlo muy atentamente.

George Temperley Ovalle
Representante Legal
GRUPO HORUS S.A.

GRUPO HORUS
GRUPO HORUS S.A.

U.E.P.P. MEC
Exp. Nº: 0373
Recibido por: Liz

DIA	MES	AÑO	HORA
13	ENE	2023	12:56

Avda. Brasilia 228 • CP 1208 • Asunción, Paraguay
+595 21 606 320
www.grupohorus.com.py
info@horustek.com

TEKOMBO'E HA TEMBIKUAA
Motenondeha
Ministerio de
EDUCACIÓN y CIENCIAS

GRUPO HORUS

Contrato N°07-22 CD – Contratación Directa Nº 01/2022

"CONSULTORIA PARA EL DIAGNÓSTICO Y EVALUACIÓN DE LA SEGURIDAD DE LOS SISTEMAS TRANSACCIONALES DEL MEC (HACKING ETICO) - SEGUNDO LLAMADO"

ID: 416.862.

PLAN DE TRABAJO

GRUPO HORUS
GRUPO HORUS S.A.
GEORGE TEMPERLEY

Historial de Cambio		
Fecha Elaboración	**Descripción**	Elaborado por
10/01/2023	Versión Inicial	Equipo GH

Contenido

1	**Resumen del Proyecto**	3
2	**Requisitos Funcionales y Definición de Alcance**	4
3	**Equipo De Proyecto**	5
4	**Plan De Comunicación Del Proyecto**	5
5	**Enfoque Técnico y Metodología**	6
6	**Metodología**	7
7	**Cronograma De Actividades**	8
8	**Aceptación y Entregables**	10

GRUPO HORUS
GRUPO HORUS S.A.
GEORGE TEMPERLEY

1 Resumen del Proyecto

Proyecto: Consultoría Para El Diagnóstico Y Evaluación De La Seguridad De Los Sistemas Transaccionales Del MEC (Hacking Etico) - Segundo Llamado	
Fechas Ejecutadas	
Fecha de Pedido – Emisión Orden de Inicio de Servicio	04/01/2023
Fecha de acuse de recibo del Proveedor	04/01/2023
Equipo de Proyecto Ejecutor	
Equipo Grupo Horus	Jorge Zunini Roberto Insfran Diego Meza
Contraparte MEC	Patricia Martínez Adriana Canclini Gustavo Toledo

Nombre del Producto

Consultoría Para El Diagnóstico Y Evaluación De La Seguridad De Los Sistemas Transaccionales Del MEC (Hacking Etico) - Segundo Llamado

Objetivo

Realizar una consultoría en la red y sistemas TICs en lo que se refiere al estado de protección de la misma ante amenazas de ciberseguridad. La misma tiene como foco principal la evaluación de la seguridad que puedan comprometer los activos principales, la infraestructura y organización de la misma. Se realizará una una consultoría de ciberseguridad en la red y sistemas transaccionales de gestión e información del MEC en su Datacenter principal en lo que se refiere al estado de protección de la misma ante amenazas de ciberseguridad. La misma tiene como foco principal la evaluación de la seguridad según metodología "Controles críticos de Ciberseguridad" aprobado por RESOLUCIÓN MITICNº277- 2020) siguiendo la estrategia del Plan Nacional de Ciberseguridad.

Objetivos Específicos

Análisis, Revisión y Evaluación del estado de ciberseguridad de la Institución, según metodología de revisión de Controles Críticos de Ciberseguridad:

GRUPO HORUS
GRUPO HORUS S.A.
GEORGE TEMPERLEY

- Utilización del Estandar de Revisión de controles críticos del Estado, según resolución MITIC Nº277-2020 o estandar compatible (NIS CIS Controls V7.1)
- Análisis de Brecha de Cumplimiento de los controles y estándar de ciberseguridad
- Elaborar un plan de acción y recomendaciones para mejora del cumplimiento de los niveles de ciberseguridad.

Análisis de Vulnerabilidades en el Datacenter principal del MEC:

- Detectar vulnerabilidades y/o problemas de seguridad que puedan ser aprovechados poratacantes
- Evaluar la efectividad y respuesta de los sistemas de seguridad implementados (firewalls,detección de intrusos y otros sistemas).
- Analizar y determinar el nivel de exposición de la infraestructura tecnológica de acuerdo conlas vulnerabilidades detectadas.
- Análisis de Seguridad a Nivel de Red mediante la recolección de datos, obtención deinformación y políticas de control de los sistemas analizados

Referencias

- Orden de Inicio de Servicio S/ Contrato No. 07/2022
- Resolución MITIC No. 277/2020 (https://gestordocumental.mitic.gov.py/share/s/mA9UAy9GTESLXCVJWJlgZw)
- Plan Nacional de Ciberseguridad https://gestordocumental.mitic.gov.py/share/s/zkKW1CkKScSvapqlB7UhNg
- CIS Controls for Internet Security V7.1 y V8

2 Requisitos Funcionales y Definición de Alcance

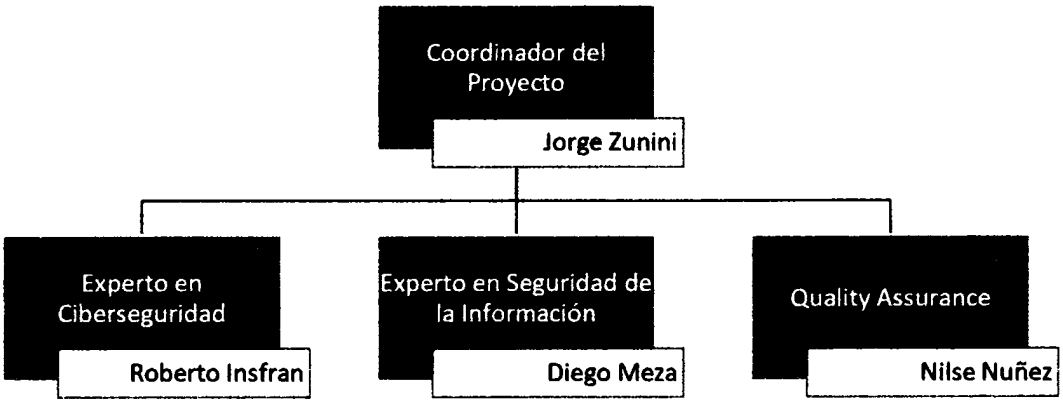
A continuación, se listan los requisitos funcionales.

Diagnóstico Y Evaluación De La Seguridad De Los Sistemas Transaccionales Del MEC	RF1. Definición del alcance del proyecto. • Controles Críticos de Ciberseguridad – CIS Controls – Gáp Análisis compatible con la metodología "Controles críticos de Ciberseguridad" aprobado por RESOLUCIÓN MITICNº277- 2020)

GRUPO HORUS
GRUPO HORUS S.A.
GEORGE TEMPERLEY

	• Cantidad de endpoint externos • Cantidad de dispositivos internos

3 Equipo De Proyecto



4 Plan De Comunicación Del Proyecto

A continuación, se detalla el plan de comunicación a ser utilizado en el transcurso del proyecto:

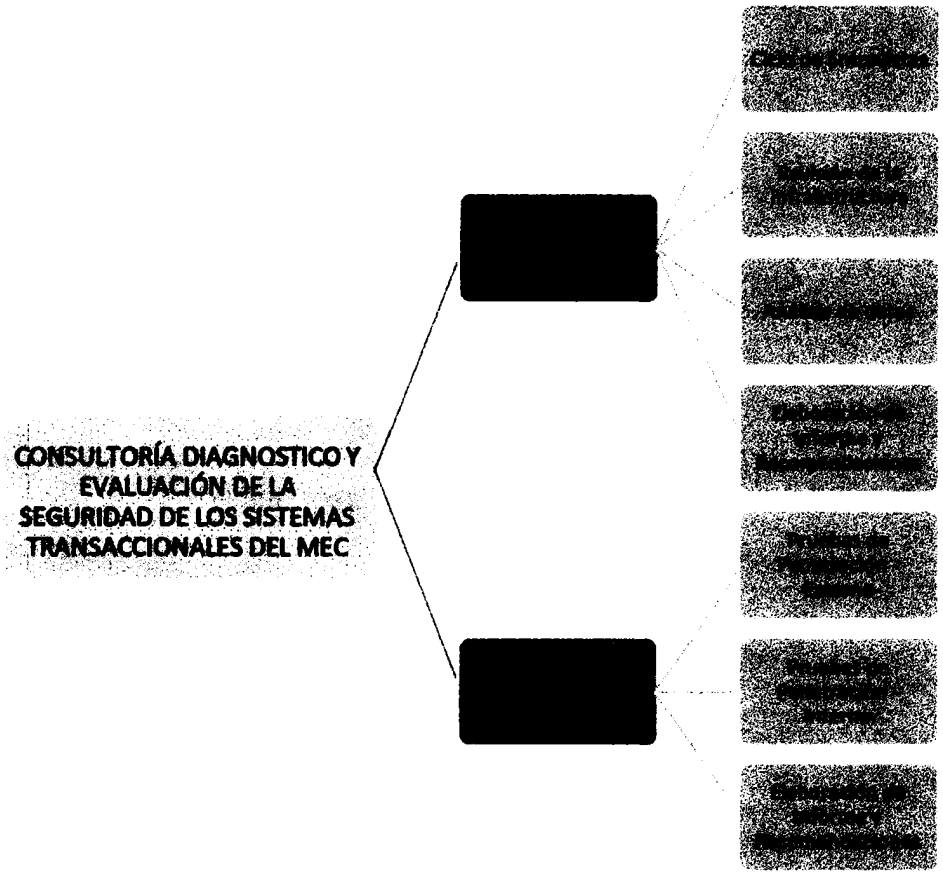
Actividad	Quien Participa / Recibe	Periodicidad	Responsable
Reunión Revisión Progreso Dia/Hora a convenir (Virtual)	Administrador de Contrato, Líder Técnico, Gerente del Proyecto, Personal técnico.	Semanal	Coordinador de Proyecto Proveedor

GRUPO HORUS
GRUPO HORUS S.A.
GEORGE TEMPERLEY

Reporte de Progreso del Proyecto (vía correo)	Administrador de Contrato, Líder Técnico.	Quincenal	Coordinador de Proyecto Proveedor

5 Enfoque Técnico y Metodología

La consultoría tendrá como actividades principales:



1. Informe del estado de madurez con respecto a la ciberseguridad **"GAP ANALISIS CIS CONTROL"** de los sistemas transaccionales de gestión e información del MEC.

GRUPO HORUS
Grupo Horus S.A.
GEORGE TEMPERLEY

Evaluar el estado de implementación de los **18 Controles Críticos de Seguridad**. El énfasis en los Controles de Higiene se debe a que varios estudios muestran que la implementación de los controles de higiene proporciona una defensa eficaz contra los ciberataques más comunes (~ 80% de los ataques). Constará de 3 etapas: Etapa de Relevamiento y Colecta de Información, Análisis de Datos Colectados y Presentación de Informe Final.

2. **Diagnóstico de seguridad y vulnerabilidad** de los Sistemas transaccionales de gestión e información del MEC.

   Análisis de Vulnerabilidades internas y externas, se simulan pruebas bajo el rol de atacante externo para poder identificar qué vulnerabilidades tiene el aplicativo, brechas de seguridad existentes, por dónde puede un atacante acceder a información o poner en riesgo datos; el objetivo es identificarlos para poder mitigarlos, controlarlos y no dejarlos visibles a los ciberdelincuentes.

6 Metodología

1. **GAP ANÁLISIS**

   Realizar una revisión exhaustiva de la Infraestructura de TI para verificar y proponer mejoras en cuanto a la seguridad informática conforme a los **Controles Críticos de Ciberseguridad** indicados en la **"Guía de Controles Críticos de Ciberseguridad"** establecido según resolución del "Ministerio de Tecnologías de la Información y Comunicación - MITIC N° 277/20 POR LA CUAL SE ACTUALIZA LA GUÍA DE CONTROLES CRÍTICOS DE CIBERSEGURIDAD".

   Durante el desarrollo de esta etapa el equipo de trabajo realizará las entrevistas y cuestionarios relativos a los diferentes ejercicios de evaluación, atendiendo los criterios de prioridad y criticidad que manifiesten. Según **modelo NIST en los Controles Críticos de Ciberseguridad**

2. **OFFENSIVE SECURITY**

   Metodología líder a nivel mundial para el desarrollo de pruebas de penetración y estudios de seguridad, la metodología contempla principalmente los métodos para el desarrollo de estudios de seguridad enfocados en seguridad ofensiva y teniendo como marco la posibilidad real de explotación independientemente de los indicadores de riesgos y vulnerabilidades, las principales ventajas de adoptar este marco metodológico son:

   - Enfoque sobre la explotación real de las plataformas.
   - Enfoque altamente intrusivo.

GRUPO HORUS
Grupo Horus S.A.
GEORGE TEMPERLEY

- Enfoque orientado a resultados tangibles y no a estadísticas generadas por herramientas.

Actividades de la Etapa

- Reconocimiento
- Preparación
- Distribución
- Explotación
- Instalación
- Comando y control
- Informe

7 Cronograma De Actividades

#	Actividad	Destinado	M1	M2	M3	M4	M5	M6
0	Kickoff Meeting - Equipo	Gerencia						
E1	**Plan de Trabajo**							
A	Ajuste de Calendario para entrevistas	Gerencia						
	Controles Criticos de Ciberseguridad v8							
	Control 1: Inventario y control de los activos empresariales	Infraestructura						
	Control 2: Inventario y control de activos de software	Sistemas						
	Control 3: Protección de datos	Sistemas						
	Control 4: Configuración segura de activos y software	Infraestructura/Sistemas						
	Control 5: Gestión de cuentas	Infraestructura/Sistemas						
	Control 6: Gestión del control de acceso	Infraestructura						
	Control 7: Gestión continua de vulnerabilidades	Infraestructura						
	Control 8: Gestión de registros de auditoría	Infraestructura						
	Control 9: Protecciones de correo electrónico y navegador web	Infraestructura						
	Control 10: Defensas contra el malware	Infraestructura						
	Control 11: Recuperación de datos	Infraestructura						
	Control 12: Gestión de la infraestructura de red	Infraestructura						
	Control 13: Supervisión y defensa de la red	Infraestructura						

GRUPO HORUS
GRUPO HORUS S.A.
GEORGE TEMPERLEY

	Control 14: Concientización y capacitación en materia de seguridad	Infraestructura						
	Control 15: Gestión de proveedores de servicios	Infraestructura						
	Control 16: Seguridad del software de aplicación	Infraestructura/Sistemas						
	Control 17: Gestión de respuesta a incidentes	Infraestructura/Sistemas						
	Control 18: Pruebas de penetración	Infraestructura/Sistemas						
B	OFFENSIVE SECURITY EXTERNA							
	Calendarizacion de actividades	Infraestructura/Sistemas						
	Solicitud de autorizacion para actividades	Infraestructura/Sistemas						
	Paso 1: Reconocimiento	Infraestructura/Sistemas						
	Paso 2: Preparación	Infraestructura/Sistemas						
	Paso 3: Distribución	Infraestructura/Sistemas						
	Paso 4: Explotación	Infraestructura/Sistemas						
	Paso 5: Instalación	Infraestructura/Sistemas						
	Paso 6: Comando y control	Infraestructura/Sistemas						
	Paso 7: Informe	Infraestructura/Sistemas						
C	OFFENSIVE SECURITY INTERNA							
	Calendarizacion de actividades	Infraestructura/Sistemas						
	Solicitud de autorizacion para actividades	Infraestructura/Sistemas						
	Paso 1: Reconocimiento	Infraestructura/Sistemas						
	Paso 2: Preparación	Infraestructura/Sistemas						
	Paso 3: Distribución	Infraestructura/Sistemas						
	Paso 4: Explotación	Infraestructura/Sistemas						
	Paso 5: Instalación	Infraestructura/Sistemas						
	Paso 6: Comando y control	Infraestructura/Sistemas						
	Paso 7: Informe	Infraestructura/Sistemas						
E2	* Informe del estado de madurez con respecto a la ciberseguridad "GAP ANALISIS CIS CONTROL" de los sistemas transaccionales de gestión e información del MEC, actividades descriptas en el apartado "Actividades Principales". * Diagnóstico de seguridad y vulnerabilidad de los Sistemas transaccionales de gestión e información del MEC (actividades 1 al 4)							

GRUPO HORUS
Grupo Horus S.A.
GEORGE TEMPERLEY

E3	Informe de Seguridad, hallazgos y evidencias de las vulnerabilidades de los sistemas transaccionales de gestión e informacióndel MEC, incluyendo recomendaciones concretas que permitan corregir los problemas y brechas de seguridad detectados y mitigar los riesgos asociados.						■	
E4	Informe Final de la consultoría de síntesis de recomendaciones y entrega técnica							■

8 Aceptación y Entregables

Los siguientes entregables están definidos como entregables y formarán parte del criterio de aceptación:

Entregable	Plazo Máximo a partir de OIS	Descripción
Producto 1: Plan de Trabajo	10 Dias	Documento que contiene el desarrollo de las actividades.
Producto 2: Informe Intermedio	120 Dias	Documento que contiene los detalles gerenciales de los trabajos realizados. - Informe del estado de madurez con respecto a la ciberseguridad "GAP ANALISIS CIS CONTROL"de los sistemas transaccionales de gestión e información del MEC, actividades descriptas en el apartado "Actividades Principales" - - Diagnóstico de seguridad y vulnerabilidad de los Sistemas transaccionales de gestión e información del MEC
Producto 3: Informe	160 Dias	Documento con los detalles técnicos contemplados en la Orden de Servicio, la misma servirá de base para la elaboración del informe final. Contenido del Informe - informe de Seguridad, hallazgos y evidencias de las vulnerabilidades de los sistemas transaccionales de gestión e información del MEC,

GRUPO HORUS
Grupo Horus S.A.
GEORGE TEMPERLEY

		- recomendaciones concretas que permitan corregir los problemas y brechas de seguridad detectados - Propuesta de acciones de mitigación de los riesgos asociados
Producto 4: Informe Final	180 Dias	Informe que resume la ejecución de la Orden de Servicio, así como los entregables y observaciones recolectadas al final de la misma. Informe Final de la consultoría de síntesis de recomendaciones y entrega técnica

George Temperley

Representante Legal

GRUPO HORUS

GRUPO HORUS S.A.