ANEXO No. 2

ANEXO TÉCNICO ESPECIFICACIONES TECNICAS MINIMAS

El oferente se obliga a cumplir con todas y cada una de las especificaciones técnicas mínimas descritas a continuación, en compromiso y aceptación de ello suscribe el **Anexo No. 1 Carta de Presentación de la Propuesta.**

OBJETO: "Monitoreo a la infraestructura y a los elementos de seguridad implementados en las páginas web del ministerio bajo el dominio cancillería.gov.co**".**

DESCRIPCIÓN	CARACTERÍSTICA
CARACTERÍSTICAS GENERALES	1.1. El servicio ofertado para el monitoreo de actividad anómala de Phishing y Pharming en los sitios protegidos debe ser en modalidad 7x8
	1.2. El servicio debe cubrir todo el ciclo de vida de una alerta, desde que se inicia hasta que se soluciona.
	1.3. La solución debe detectar en tiempo real las conexiones de los sitios protegidos, entregando información, tal como, IP, Fechas, Horas, Información de Geolocalización, URL de conexión, URL de origen, Proxys Anónimos, etc.
	1.4. El servicio de antiphishing y antipharming deberá detectar en tiempo real ataques que pretendan enviar información crítica y/o confidencial a través de la URL (por ejemplo: inyectar código SQL)
	1.5. El servicio deberá contar con la capacidad de detectar sistemas operativos y navegadores de internet obsoletos, que por no estar soportados por sus respectivos fabricantes tengan un número importante de vulnerabilidades descubiertas.
	1.6. La solución deberá proveer detección de conexiones a través de proxies anónimos y/o cualquier otro canal de conexión que atente contra la integridad del sitio protegido
	1.7. La solución deberá proveer detección de conexiones que provengan de fuentes sospechosas en tiempo real.
	1.8. Debe tener la capacidad de analizar el origen de las conexiones, detectando, y bloqueando las que vengan de países riesgosos en cuanto a actividad maliciosa
	1.9. La solución deberá proveer la funcionalidad de recuperación forense de evidencias de ataques informáticos y credenciales robadas siempre que se encuentren disponibles
	1.10. El servicio de monitoreo debe tener la posibilidad de generar alertas personalizadas de acuerdo a las diferentes variables de conexión presente tales como IP, REFERRER, VARIABLES, etc. con el objeto de generar alertas de acuerdo a patrones específicos de interés para la organización
	1.11. El servicio de monitoreo, debe estar en la capacidad de detectar cualquier comportamiento anómalo de navegación y/o uso de los sitios web protegidos, tales como, copia del sitio protegido, redireccionamiento, etc.
	1.12. El servicio debe garantizar las desactivaciones de todos los ataques dirigidos a las páginas web, para garantizar una disponibilidad de las páginas web del 99.9%
	1.13. La solución deberá estar en la capacidad de detectar y desactivar amenazas o ataques en contra las páginas web, tales como malware, Man-in-the-Middle y Man-in-the-Browser

	1.14. El servicio deberá proveer información de los incidentes y de gestión general.
CARACTERÍSTICAS AVANZADAS	2.1. La solución debe contar con una funcionalidad de reconocimiento de ataques de Defacement contra los sitios WEB previniendo cambios en el contenido no autorizados.
	2.2. La solución debe monitorear activamente la veracidad del certificado SSL de los dominios protegidos, identificando de forma temprana posibles cambios, caducidad o riesgo con la entidad certificadora.
	2.3. El servicio debe monitorear de forma constante el tiempo de respuesta y los niveles de disponibilidad de los sitios web protegidos desde diferentes locaciones a nivel mundial identificado posibles ataques de denegación de servicio y/o disponibilidad de los sitios
	2.4. La solución debe monitorear cambios en la resolución de dominio identificando ataques de re direccionamiento de tráfico tales como DNS spoofing / DNS Poisoning
CARACTERÍSTICAS DE ADMINISTRACIÓN Y SOPORTE	3.1. El servicio ofrecido debe contar reportes, de la actividad anómala de phishing, pharming,malware, MITM, MITB, monitoreo de defacement, disponibilidad, resolución DNS, certificados SSL, estadísticas de gestión, reportes de incidentes.
	3.2. Es requerido que se incluyan detalles de los incidentes, tales como: posibles causas, fuentes de los ataques (tomando en cuenta la evidencia que esté disponible), recolección de evidencia (cuando sea posible) para análisis forense posterior.
	3.3. La solución debe generar reportes que incluyan información sobre conexiones y alertas y los requeridos por la entidad.
	3.4. El proveedor debe contar con soporte en español
	3.5. El proveedor seleccionado debe hacer un acompañamiento una vez puesta en producción la solución, de manera de poder detectar posibles mejoras, requerimiento de crecimiento, entre otros.

Atentamente,

FIRMA DEL PROPONENTE O REPRESENTANTE LEGAL O APODERADO

DATOS DEL REPRESENTANTE LEGAL		
Nombre:		
CC No.		
DATOS DEL PROPONENTE		
Nombre:		Nit:
Dirección:		
Ciudad:	Teléfono:	Fax:
Correo Electrónico:		