SERVICIO DE MONITOREO NOC Y SOC

1. Especificaciones Técnicas

El servicio consistirá en el monitoreo externo de eventos de la Infraestructura crítica de TICs de la CAJA DE JUBILACIONES Y PENSIONES DEL PERSONAL DE LA ANDE (en adelante CAJA ANDE) mediante una conexión segura de Red Privada Virtual (VPN) entre CAJA ANDE y el Centro de Operaciones de Red (NOC) y Centro de Operaciones de Seguridad (SOC) del Oferente.

El objetivo del servicio es asegurar la operación y disponibilidad continua de los servicios de la Infraestructura crítica de TICs de la CAJA ANDE y accionar ante eventos críticos de seguridad de manera preventiva y proactiva.

En este contexto, el Oferente deberá asignar el personal idóneo para cumplir este ítem con la competencia técnica suficiente para gestionar eventos de monitoreo, que guarden relación con el servicio proveído.

El Oferente deberá proporcionar este servicio con al menos 6 (seis) Personal de Monitoreo y Seguridad asignado en forma remota. Así mismo deberá prever 1 (un) Coordinador Técnico del servicio, el cual tendrá las siguientes funciones administrativas:

- Cumplir el papel de nexo entre la CAJA ANDE y el Oferente.
- Controlar que el Personal de Monitoreo cumpla con los procedimientos de gestión de eventos de monitoreo y seguridad acordados con la CAJA ANDE.
- Presentar informes mensuales de monitoreo y cuando sea requerido por la CAJA ANDE.

Se detallan los servicios que podrán ser requeridos a este equipo de trabajo sin que ello constituya todo el universo de requerimientos posibles:

Se aceptaran condiciones de Confidencialidad y protección de los datos compartidos entre ambas partes:

Servicio Preventivo	Monitoreo de servidores físicos y virtuales, enlaces, equipos de RED y EndPoints (PCs).
	Análisis de causa de raíz de Incidentes.
	Identificar fallas y degradaciones del desempeño de la RED, los servidores y los EndPoints (PCs).
	Análisis de Rendimiento en los servicios monitoreados.
Servicio Operacionales	Reacción ágil ante la aparición de incidentes críticos para su pronta solución.
	Seguimiento del incidente con los oferentes y funcionarios involucrados para su resolución.
	Informe diario del estado de los equipos y servicios monitoreados.
	Proactividad ante anuncios de Vulnerabilidades de Ciberseguridad emitidos por la CVE.
Servicio de Mejora continua	Gestión de capacitación y concienciación en Seguridad, utilizando herramientas digitales.
	Capacitación en Seguridad para el personal de la CAJA ANDE.
	Sugerencia y acción de las mejores prácticas en Seguridad y Monitoreo en base a la experiencia.
	Consultoría para la evaluación y redacción de Políticas de Seguridad y Manual de procedimientos ante incidentes todos ajustados a normas vigentes de Seguridad Informática y documentaciones exigidas por la MITIC, aplicables a la Institución CAJA ANDE para la presentación de formalización y aprobación del Consejo Directivo de la Institución para la presentación en futuras Auditorias.
	Contrato de Confidencialidad y Responsabilidad sobre Información y datos, al cual se exponen con los diferentes niveles de acceso proveídos por CAJA ANDE

Cantidad de equipos y servicios a ser monitoreados.

EQUIPOS - NETWORKING		
ÍTEM	**EQUIPO/SERVICIOS**	**Cantidad**
1	Firewall (cisco/fortinet)	3
2	Switch (Cisco/fortinet/trendnet)	8
3	Servidores Físicos	5
4	Servidores Windows	25
5	Servidores Linux	4
6	EndPoints (PCs)	70
7	Enlaces Internet	1
8	Conexiones VPN/RMSP	4

Detalles para el servicio de Monitoreo	Indicar estado de uso de: Procesador, Memoria, Disco, CPU de cada servidor físico y virtual
	Indicar estado de uso de: Procesador, Memoria, Disco, CPU de cada equipo de Networking
	Supervisión de estado (activo, inactivo, caída) de cada Servidor y de cada equipo de Networking
	Indicar estado de las interfaces (activo, inactivo, caída) de cada Servidor y de cada equipo de Networking.
	Indicar el uso de ancho de banda de los enlaces y servicios publicados
	Remisión de reportes ante incidentes
Detalles para el servicio de Seguridad (SOC)	Identificar/Detectar posibles ataques y poner al EndPoint, al Servidor Software o archivo en cuarentena de forma automática
	Actualizaciones de Seguridad constante.
	Concienciación y/o Training en Seguridad.
	Servicios de Penetration Testing – Interno y Externo
	Implementación de nuevas funcionalidades
	Remisión de reportes ante incidentes.
	Reportes de seguridad Diarios/Semanales

Los servicios solicitados deberán cumplir con las siguientes Especificaciones Técnicas mínimas, y se deberá completar y presentar con la oferta la Planilla de Datos Garantizados

- El oferente deberá presentar en su oferta una descripción de los medios y los recursos para prestar el servicio.
- Acuerdo de Nivel de Servicio: El oferente adjudicado suscribirá un contrato por servicios del tipo SLA relacionado a :

REQUISITOS TÉCNICOS SOLICITADOS: SERVICIO DE MONITOREO NOC Y SOC	**PLANILLA DE DATOS GARANTIZADOS Además de completar (SI o NO), los oferentes deberán especificar la característica ofertada, en la columna de DETALLE**	
	Cumple con las especificaciones requeridas (SI/NO)	**DETALLE**
Tiempo del Servicio: 24/7/365		
Tiempo de notificación ante incidentes: ≤ 15 (quince) minutos.		
Tiempo de notificación al oferente de Servicios: ≤ 15 (quince) minutos.		
Asistencia in situ ante incidentes críticos: ≤ 2 (dos) horas		
ALCANCE DE SERVICIOS NOC/SOC		
El oferente deberá contar en su infraestructura herramientas para monitoreo de los diferentes equipos y servicios de la CAJA ANDE.		
El oferente deberá contar con herramientas digitales para la gestión de eventos vía sistema de ticket, mail y/o teléfono.		
El Oferente deberá asegurar que el inventario de los activos de TI de la CAJA ANDE estén actualizado y disponible.		
El oferente deberá emitir Alertas ante Bugs y vulnerabilidades de Seguridad.		
El oferente deberá notificar los ciclos de vida del equipamiento de Networking de la CAJA ANDE.		
El oferente deberá contar con un mínimo de 6 personales para monitoreo de los recursos de la CAJA ANDE.		
El oferente deberá responder ante eventos críticos hasta un máximo de 2 horas.		
El oferente deberá realizar pruebas periódicas de sistemas redundantes y disaster recovery.		
El oferente deberá realizar reportes de incidentes semanales, mensuales o cuando este fuera requerido por la CAJA ANDE.		
El oferente deberá capacitar al personal de la CAJA ANDE en las buenas prácticas de la Ciberseguridad.		
El oferente deberá contar con al menos 1 coordinador Técnico para el nexo con la CAJA ANDE.		
HERRAMIENTA DE CONCIENTIZACIÓN EN SEGURIDAD		
El oferente deberá contar con una herramienta y/o plataforma para concientizar en Seguridad al personal de la CAJA ANDE.		
La herramienta y/o plataforma deberá ser del tipo SaaS sin necesidad de instalar Software ni equipos localmente.		
La Herramienta y/o plataforma deberá contar con un Dashboard de control, programador y visor de eventos.		
La herramienta y/o plataforma deberá contar con módulos interactivos de capacitación.		
La herramienta y/o plataforma deberá simular un ataque de Phishing y Ransomware que puedan evaluar comportamientos.		
La herramienta y/o plataforma deberá gestionar reportes en tiempo real y		

REQUISITOS TÉCNICOS SOLICITADOS: SERVICIO DE MONITOREO NOC Y SOC	PLANILLA DE DATOS GARANTIZADOS Además de completar (SI o NO), los oferentes deberán especificar la característica ofertada, en la columna de DETALLE	
	Cumple con las especificaciones requeridas (SI/NO)	DETALLE
reportes automáticos vía e-mails.		
La herramienta y/o plataforma deberá poseer contenidos de capacitación, concientización y evaluación predefinidos actualizados, los cuales deben ser personalizables en su totalidad y en el idioma español.		
La herramienta y/o plataforma deberá permitir utilizar elementos de gamificación.		
La herramienta y/o plataforma deberá contar con al menos uno de estos estándares o certificaciones de seguridad: *ISO 27001. *SOC 1 and SOC 2/SSAE 16/ISAE 3402. *PCI Level 1. *FISMA Moderate. *Sarbanes-Oxley (SOX).		
La herramienta y/o plataforma deberá estar disponible por los primeros 12 meses para el personal de la CAJA ANDE. Gestionado y administrado por el oferente.		
El oferente deberá presentar la documentación correspondiente de la herramienta y/o plataforma donde indique que cumplen con los requerimientos de la CAJA ANDE.		
El oferente deberá contar con al menos 3 (tres) técnicos certificados con la marca de la herramienta y/o plataforma para el servicio de concienciación en seguridad.		
La empresa oferente deberá contar con una carta autorizada de la marca de la herramienta y/o plataforma con que cuenta para el servicio de concienciación en seguridad.		
COMPONENTES DEL SOC - CONSOLA DE ADMINISTRACION		
El oferente deberá proveer de una herramienta y/o solución para gestión de dispositivos para la CAJA ANDE.		
La herramienta y/o solución debe proveer de una consola de administración en la nube (Entregada como SaaS).		
La solución debe gestionarse en una Consola unificada basada en web.		
La consola debe soportar múltiples sitios y múltiples cuentas sin configuración adicional.		
La solución a ofertar debe tener una base de conocimiento y documentación dentro de la consola sin la necesidad de utilizar credenciales de otro sistema.		
La consola debe ser intuitiva y fácil de navegar con flujos de trabajo que permitan la respuesta ante incidentes.		
La consola de administración debe permitir el acceso granular basado en roles y por nivel de tenant (cuenta, sitio).		
La solución debe permitir el acceso vía API completo a todas las capacidades de gestión y acceso a los datos.		
La solución debe permitir el acceso vía API completo a todas las capacidades de gestión y acceso a los datos.		
La solución debe admitir 2FA y SSO (SAML 2.0) para el acceso a la consola de administración.		

REQUISITOS TÉCNICOS SOLICITADOS: SERVICIO DE MONITOREO NOC Y SOC	PLANILLA DE DATOS GARANTIZADOS Además de completar (SI o NO), los oferentes deberán especificar la característica ofertada, en la columna de DETALLE	
	Cumple con las especificaciones requeridas (SI/NO)	DETALLE
La auditoría y el registro de actividad deben mantenerse en la consola de administración. La solución debe contar con la capacidad de enviar registros a una fuente externa (como ej. SIEM).		
Los datos están cifrados tanto en el almacenamiento como en reposo.		
COMPONENTES DEL SOC – SOPORTE CON SISTEMA OPERATIVO		
La solución deberá soportar la instalación en Sistemas Operativos Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows Server 2019.		
La solución deberá soportar la instalación en Sistemas Operativos Windows 7, Windows 8, Windows 10 y Linux. Contenedores Dockers workloads, kubernetes cloud.		
La solución debe permitir la configuración en modo de detección o protección en sistemas operativos Linux.		
La solución se debe implementar como DaemonSet en plataformas Kubernetes.		
COMPONENTES DEL SOC - AGENTE		
La solución debe brindar capacidades de EPP y EDR disponibles en un solo agente sin necesidad de instalar varios paquetes de software.		
La solución debe contar con Anti-tamper.		
Capacidad para iniciar análisis bajo demanda para buscar malware o asegurarse de que se haya corregido una amenaza (desde la consola y/o el dispositivo final).		
Capacidad para programar actualizaciones de agente8s desde la consola de administración.		
Capacidad para actualizar agentes sin impacto para el usuario final.		
La herramienta y/o solución no debe dejar de funcionar si se excede la cantidad de licencias adquiridas.		
La solución debe contar con la opción de "Dar de baja automáticamente" a los agentes antiguos si no se han comunicado con la consola de administración durante un período de tiempo configurable.		
El agente debe tener un rendimiento mínimo del sistema bajo carga estándar (1-2% de CPU, <250 Mb de memoria).		
El agente no debe solicitar reinicio cuando se realice una actualización de versión.		
El agente debe permitir la comunicación a través de un proxy web.		
El agente de Windows se ejecuta en el espacio del Kernel para garantizar el nivel más alto de protección contra manipulaciones (Anti-tamper).		
La solución debe proporcionar la capacidad de enviar mensajes de notificación a la computadora del usuario final.		
El agente de Mac debe soportar arquitecturas Kextless.		
COMPONENTES SOC - PREVENCION DE AMENAZAS		
La solución debe proporcionar prevención en los Sistemas Operativos; Windows, MacOS y Linux.		

REQUISITOS TÉCNICOS SOLICITADOS: SERVICIO DE MONITOREO NOC Y SOC	PLANILLA DE DATOS GARANTIZADOS Además de completar (SI o NO), los oferentes deberán especificar la característica ofertada, en la columna de DETALLE	
	Cumple con las especificaciones requeridas (SI/NO)	DETALLE
La solución debe proporcionar protección contra malware conocido y desconocido.		
La solución debe brindar protección contra ataques de día cero, mediante el análisis de comportamiento en el punto final, sin depender de firmas.		
La solución debe proteger el endpoint contra malware, incluso cuando el sistema no esté conectado a la red.		
El agente no debe tener dependencia con la consola de administración, con la nube o cualquier recurso externo para detectar y responder adecuadamente a amenazas sofisticadas (día cero, sin archivos, basado en RAM, cero Exploits diarios, ransomware, mineros, movimiento lateral, APT) en tiempo real a medida que se detectan las amenazas.		
La solución debe permitir descargar de forma segura un archivo malicioso o archivo enviado a cuarentena desde la consola de administración.		
COMPONENTES DE SOC- CAPACIDAD DE RESPUESTA Y REMEDIACION		
La solución debe tener la capacidad de acceder remotamente al equipo.		
La solución debe tener la capacidad para remediar todos los cambios del sistema operativo con un solo clic en caso de ransomware.		
La solución debe de tener la capacidad para revertir eventos de datos destructivos que incluyen, entre otros, ransomware con un solo clic.		
La solución debe permitir tomar acciones de remediación en múltiples sistemas o eventos a la vez.		
COMPONENTES DE SOC - EXCLUSIONES		
La solución debe contar una lista predefinida de exclusiones conocidas o recomendadas.		
La solución debe permitir a los administradores de la consola realizar exclusiones mediante: Hash, Ruta, Certificado o un Signer ID, Tipo de Archivo.		
La solución debe permitir configurar las exclusiones para manejar los problemas de interoperabilidad hasta rutas específicas o ejecutables únicos reduciendo el monitoreo de los procesos principales y/o todos sus procesos secundarios generados.		
COMPONENTES DE SOC- CONTROL DE DISPOSITIVOS		
La solución debe poder controlar dispositivos USB externos.		
La solución debe poder permitir controlar dispositivos USB de manera granular teniendo como tipo de clasificación, la siguiente información del dispositivo: Clase, Número de serie específico, ID de Producto o ID de Vendor.		
La solución debe poder controlar dispositivos Bluetooth externos.		
La solución puede proporcionar un inventario de todas las aplicaciones instaladas para todos los equipos de la CAJA ANDE.		
COMPONENTES DE SOC - GENERALIDADES DE LA HERRAMIENTA Y/O SOLUCION		
El oferente deberá proveer de una herramienta para gestión de dispositivos para la CAJA ANDE.		
La herramienta deberá ser capaz de gestionar un ciclo de amenazas como; Pre-Ejecución, Ejecución y Post-Ejecución.		

REQUISITOS TÉCNICOS SOLICITADOS: SERVICIO DE MONITOREO NOC Y SOC	PLANILLA DE DATOS GARANTIZADOS Además de completar (SI o NO), los oferentes deberán especificar la característica ofertada, en la columna de DETALLE	
	Cumple con las especificaciones requeridas (SI/NO)	DETALLE
La herramienta debe contar con una única consola para la gestión de dispositivos.		
La herramienta debe ser capaz de construir una línea de tiempo ante incidentes críticos.		
La herramienta debe conservar logs de eventos hasta 365 días y estar disponible cuando la CAJA ANDE lo requiera.		
La herramienta debe ser compatible con sistemas operativos Windows, Linux, MacOs hasta incluso con sistemas operativos móviles.		
La herramienta debe ser capaz de conocer, detectar y accionar ante amenazas de ciberseguridad pudiendo bloquear o enviar a cuarentena al dispositivo o archivo en cuestión para su posterior análisis.		
El oferente deberá de disponibilizar del aplicativo o agente en caso de ser necesario para la gestión de dispositivos.		
La herramienta debe efectuar los mecanismos de protección de dispositivos en modo offline.		
La marca de la herramienta y/o plataforma para el servicio de SOC deberá formar parte del cuadrante mágico de Gartner.		
La empresa oferente deberá contar con una carta autorizada de la marca de la herramienta y/o plataforma con que cuenta para el servicio de SOC.		
El oferente deberá contar con al menos 2 (dos) personas con certificaciones de la herramienta y/o plataforma con que cuenta para el servicio de SOC. Una Certificación del tipo comercial y una Certificación del tipo técnico.		
NORMALIZACION DE PROCESOS Y POLITICAS DE SEGURIDAD		
Sugerencia y acción de las mejores prácticas en Seguridad y Monitoreo en base a la experiencia.		
Consultoría para la evaluación y redacción de Políticas de Seguridad ajustados a normas vigentes de Seguridad Informática y documentaciones exigidas por la MITIC, aplicables a la Institución CAJA ANDE para la presentación de formalización y aprobación del Consejo Directivo de la Institución para la presentación en futuras Auditorias.		
Consultoría para la evaluación y redacción de Manual de procedimientos ante incidentes todos ajustados a normas vigentes de Seguridad Informática y documentaciones exigidas por la MITIC, aplicables a la Institución CAJA ANDE para la presentación de formalización y aprobación del Consejo Directivo de la Institución para la presentación en futuras Auditorias.		
Contrato de Confidencialidad y Responsabilidad sobre Información y datos, al cual se exponen con los diferentes niveles de acceso proveídos por la Institución.		
GARANTÍA, CERTIFICACIONES Y EXPERIENCIA		
El oferente deberá contar con al menos 8 años de experiencia en el mercado de las telecomunicaciones.		
El Oferente deberá proporcionar el servicio de NOC/SOC con al menos 6 (seis) técnicos de Monitoreo y Seguridad, estos técnicos deberán ser parte de la planilla de personal del oferente. La documentación respaldatoria debe constar en la oferta con la presentación de la Planilla de IPS.		

REQUISITOS TÉCNICOS SOLICITADOS: SERVICIO DE MONITOREO NOC Y SOC	PLANILLA DE DATOS GARANTIZADOS Además de completar (SI o NO), los oferentes deberán especificar la característica ofertada, en la columna de DETALLE	
	Cumple con las especificaciones requeridas (SI/NO)	DETALLE
El oferente deberá contar con al menos 4 técnicos certificados del nivel profesional que cuenten con al menos un certificado del tipo; CISCO CCNP, FORTINET NSE7, NUTANIX NCSE-Core. Con antigüedad mínima de 1 año. Comprobada con documentación o constancia emitida por el IPS (Instituto de Previsión Social).		
El oferente deberá demostrar experiencia en provisión de servicios de Monitoreo (NOC) Presentando como mínimo 3 constancias o copia de contratos con entidades públicas y privadas.		
El oferente deberá contar con la infraestructura equipada para el servicio de Monitoreo NOC/SOC dentro del territorio de Asunción, Paraguay.		

Observación: El oferente deberá presentar todas las documentaciones respaldatorias de lo solicitado en la Planilla de Datos Garantizados que sean pertinentes.