FICHA TÉCNICA	
FICHA TÉCNICA SOLUCION INTELIGENCIA ARTIFICIAL DE SEGURIDAD INFORMÁTICA	
1. Prestación Principal	
1.1	Solución de Cyber Defensa capaz de identificar cualquier amenaza anómala en la red en tiempo real a través del aprendizaje automático e inteligencia artificial. Cada oferente deberá proponer una solución que cumpla con las siguientes características técnicas y funcionales:
2 Sistema de Detección de Amenazas	
2.1	La solución deberá estar basada en hardware appliance, es decir, un (1) hardware de propósito específico destinado a alojar el sistema de seguridad requerido con las condiciones de endurecimiento propias de un sistema de seguridad.
2.2	La solución no debe tener ningún componente que deba instalarse en un servidor de propósito general.
2.3	La solución debe basarse en un sistema de seguridad que reciba todo el tráfico de la red desde uno o varios switches, lo analice, identifique y bloquee las amenazas o incidentes que están ocurriendo en la red.
2.4	Después del período de aprendizaje inicial, la tecnología debe proporcionar automáticamente un seguimiento de auditoría completo de todos los dispositivos en el entorno, clasificando previamente al menos el tipo de dispositivo, el nombre de host, la dirección MAC, la primera y la última vez que se vio el dispositivo en la red
2.5	Debe basarse en el análisis de comportamiento, pudiendo resaltar al menos: a. Toda conectividad inusual en la red. b. Todas las actividades inusuales en la red. c. Ser capaz de hacer un seguimiento detallado del dispositivo, indicando incluso su historial de IP, si está en un ámbito DHCP d. ser capaz de hacer un seguimiento detallado del usuario indicando incluso todos los nombres de host asociados a una determinada credencial e. Ser capaz de identificar un volumen de conexiones significativamente inusual f. identificar el nivel de rareza de un dispositivo en la red, así como el nivel de rareza de un acceso a un sitio externo.
2.6	La solución debe alertar automáticamente sobre todas las actividades inusuales y anormales en la red

2.7	Debe ser una plataforma de autoaprendizaje y tener un enfoque adaptativo, que utilice inteligencia artificial comprobada para aprender sobre el entorno en el que se encuentra, detectar y responder a las desviaciones de la actividad normal a. la línea de base de la red debe ser lo suficientemente adaptable y dinámica para adaptarse a cualquier cambio en el comportamiento del entorno b. debe funcionar completamente en función del comportamiento, donde no se permitirán las tecnologías que hacen uso de reglas y / o firmas
2.8	La herramienta debe utilizar modelos matemáticos de estimación recursiva bayesiana o similares con el fin de validar los comportamientos a normales en la red.
2.9	Debe proporcionar visibilidad completa de la red, incluidas las TI tradicionales y no tradicionales.
2.10	Debe poder identificar cualquier comportamiento anómalo en el entorno y resaltar estos comportamientos en tiempo real
2.11	Debe ser capaz de identificar cualquier dispositivo nuevo insertado en la red
2.12	Debe basarse en métodos matemáticos probabilísticos, analizando y correlacionando dimensiones distintas dentro del paquete
2.13	Debe poder realizar una captura de paquetes en tiempo real que permita un análisis exhaustivo del incidente en el momento del suceso.
2.15	Debe tener integración con LDAP.
2.16	Debe permitir la personalización avanzada de la tecnología, permitiendo considerar múltiples parámetros de datos al verificar un determinado comportamiento, entre los parámetros debería ser posible tener al menos las siguientes opciones: Conexiones, conexiones externas, conexiones internas, transferencia de datos, datos externos transferencia, conexiones SMB internas, conexiones de puerto cerrado, difusiones, dispositivos conectados, transferencia de datos (cliente), transferencia de datos (servidor), entre otras métricas relevantes.
2.17	Debe utilizar varios algoritmos de inteligencia artificial, así como varias técnicas de Machine Learning, que contienen al menos: Deep Learning , Machine Learning supervisado y Machine Learning no supervisado.
2.18	La tecnología de identificación de amenazas de la solución no debe basarse en firmas, ni reglas, ni heurística, ni sandboxing. Debe estar puramente basada en algoritmos avanzados de Machine Learning e Inteligencia Artificial.
2.19	La solución debe tener la capacidad de modelar el comportamiento normal a nivel de usuario, dispositivos y red y a partir de éste identificar de forma autónoma las anomalías que corresponden a brechas de seguridad.

2.20	La herramienta debe poder realizar un aprendizaje autónomo del comportamiento normal de la red sin requerir previo conocimiento del historial de comportamiento anómalo, con la posibilidad de identificar amenazas desde el primer día de instalada.
2.21	La tecnología debe tener la capacidad de detectar amenazas internas y externas
2.22	La tecnología debe ser auto-configurable, es decir, debe tener capacidad de adaptarse de forma automática a los cambios del entorno en tiempo real.
2.23	La solución debe tener capacidad de detectar como mínimo los siguientes tipos de brechas de seguridad: o Ataques de tipo botnet o Propagación de gusanos o Ataques de ransomware o Infiltración y exfiltración de datos o Troyanos bancarios o Credenciales comprometidas o Minería de bitcoins o Presencia de malware o Ataques DDoS a través de dispositivos IoT o Amenazas avanzadas persistentes (APT)
2.24	Los dispositivos propios de la herramienta deben estár en sitio, no se aceptan soluciones que necesiten de la nube para hacer los análisis de la información, cualquier configuración remota debe ser consultada y autorizada con la entidad
2.25	La herramienta debe ser tipo appliance no se aceptarán equipos que involucren la instalación de agentes en los dispositivos a monitorear.
2.26	La solución debe poder reconocer nuevas amenazas que no hayan sido advertidas previamente.
2.27	La solución no debe ser Firewalls, NGFW, SIEM o Sandboxing
3. Visualización de red	
3.1	La solución debe poseer una interfaz de visualización amigable, que debe ser accesible vía web https.
3.2	La interfaz de visualización debe permitir tener visibilidad gráfica de cualquier elemento de la red con gran profundidad en el detalle. Debe poder llegarse a ver gráficamente hasta el nivel de dispositivo y sus conexiones en tiempo real. No deberá necesitar compartir datos con una nube de seguridad global para obtener su inteligencia de seguridad

3.3	La visualización de cualquier elemento en la red debe ser en tiempo real y también debe haber posibilidad de visualizar actividad histórica de manera gráfica. La solución debe permitir la búsqueda en la hora exacta que se desea ver la actividad histórica, con un nivel de exactitud de minutos.
3.4	Debe ser capaz de agrupar automáticamente los dispositivos en grupos y grupos por su similitud de comportamiento
3.5	Debe tener una sección de búsqueda que permita buscar inmediatamente un dispositivo, IP, subred o host de red
3.6	Debe tener una interfaz de usuario donde se pueda consultar el estado completo del sistema, incluyendo al menos: a. La versión del software, el espacio en disco utilizado, el consumo de CPU y el consumo de memoria. b. El detalle de todas las interfaces activas y el tráfico respectivo recibido a través de cada una de ellas c. El ancho de banda total procesado actualmente, el ancho de banda promedio procesado hasta la fecha, el ancho de banda registrado en los últimos 7 días y 2 semanas anteriores d. Un análisis detallado de todo el tráfico recibido en el dispositivo y la última vez que se vieron los protocolos principales, entre ellos HTTP, HTTPS, FTP, LDAP, SMTP, SSH, SMB, SSDP, POP3, NTLM, IMAP, Kerberos, entre otros
3.7	La solución nos debe dar visibilidad en tiempo real de los siguientes datos correspondientes a la red: o Cantidad de servidores o Cantidad de estaciones cliente o Cantidad de credenciales de usuario o Tráfico de red
3.8	La interfaz de visualización debe poseer una barra de búsqueda que permita encontrar de manera rápida cualquier elemento de la red bajo los siguientes criterios: o Dirección IP o Tipo de dispositivo o Función o protocolo conocido tal como DNS o Active Directory o Móviles por tipo de dispositivo o Nombre del dispositivo
3.9	Cuando se hace búsqueda de un dispositivo, la interfaz debe poder mostrar la información de éste en detalle incluyendo: dirección IP, MAC, sistema operativo, logs de eventos, logs de brechas de seguridad identificadas, historial de conexiones, lista de dispositivos similares

3.10	La interfaz debe permitir la visualización de todas las subredes, así como todos los dispositivos que las conforman. Debe permitir la visualización de la subred de manera gráfica en tiempo real, mostrando el esquema de conexiones entre los dispositivos que la conforman.
3.11	Las subredes deben poder visualizarse en un mapa global que permita conocer la ubicación real de cada subred.
4. Visibilidad de amenazas	
4.1	La interfaz debe mostrar las amenazas que se van identificando en la red en tiempo real, con el detalle de logs de cada amenaza generados por la herramienta, así como vistas gráficas que permitan ver el comportamiento de la amenaza en el tiempo.
4.2	Debe proporcionar filtros simples y rápidos para permitir el análisis de violaciones por parte de Usuarios, Dispositivos y tipo de violación, como mínimo
4.3	La interfaz debe poder mostrar la amenaza y o violación de manera gráfica y en tiempo real, donde se permita reproducir de manera gráfica los dispositivos/credenciales que intervienen en determinado ataque, sus distintas conexiones a nivel de red en la línea de tiempo del comportamiento investigado.
4.4	Las amenazas identificadas deben tener un nivel de clasificación según su criticidad y debe contar con un código de colores asociado a cada nivel.
4.5	La interfaz nos debe brindar la posibilidad de investigación de alertas en profundidad en tiempo real, de manera gráfica y mediante eventos.
4.6	Debe tener una función que permita el análisis retrospectivo de los registros del incidente, devolviendo la conexión en segundos, minutos, horas o días antes de que se haya identificado una cierta anomalía
4.7	La interfaz debe poseer herramientas o funcionalidades que permitan la investigación forense al mayor nivel de detalle de cualquier amenaza identificada, sin necesidad de uso de herramientas externas.
4.8	Debe ser capaz de agrupar las anomalías de manera inteligente y por nivel de criticidad.
4.9	Debe contar dentro la su propia interface con herramientas tipo Punycode Convertor ,RegEx Tester ,Base64 Convertor ,JS Beautifie ,Epoch Converter , Facilitando el análisis de los incidentes.
4.10	La interfaz de visualización debe permitir tener visibilidad gráfica en 3D de cualquier elemento de la red con gran profundidad en el detalle. Debe poder llegarse a ver gráficamente hasta el nivel de dispositivo y sus conexiones en tiempo real.

4.11	La visualización de cualquier elemento en la red debe ser en tiempo real y también debe haber posibilidad de visualizar actividad histórica de manera gráfica. La solución debe permitir la búsqueda en la hora exacta que se desea ver la actividad histórica, con un nivel de exactitud de minutos. La solución debe contar con al menos 500 modelos de comportamiento predefinidos de fábrica y poder realizar la creación de modelos personalizados.
5. Arquitectura de la Solución	
5.1	La solución debe ser centralizada, es decir, debe contar con una única interfaz de administración y visualización, desde la cual se pueda gobernar toda la solución y monitorear todo el entorno.
5.2	El análisis del tráfico mediante los algoritmos de Machine Learning e Inteligencia Artificial debe realizarse de manera centralizada a la totalidad del tráfico proveniente del datacenter Principal
5.3	El equipo que conforma la solución debe ser instalado fuera de línea, es decir, la recepción del tráfico de red debe hacerse a través de puertos pasivos, de tal manera de no causar retardos en el desempeño de la red.
5.4	Debe realizar un análisis completo del tráfico (No análisis parciales de los paquetes p.e: sflow, jflow, netflow, Syslog.
5.5	Se debe considerar los siguientes datos para el dimensionamiento de la solución a ofertar: • Cantidad de appliance (Mínimo uno (1)), doble fuente de suministro • Marca: Especificar • Conexiones por minuto 50.000 • Troughput: hasta 2 Gbps • Cantidad de dispositivos a analizar minimo535 • Tipo de interfaz Deben tener mínimo: • 2-puertos 1G/10G SFP+ • 2-puertos 10G RJ45 10000 BASE-T • 2-puertos 1G RJ45 1000 BASE-T • 4-puertos 1G RJ45 1000 BASE-T
5.6	La herramienta debe soportar los siguientes modos de implementación: Port mirror (SPAN) TAP Externo
6. Notificaciones	
6.1	La solución debe contar con la capacidad de poder notificar las amenazas a través de correos electrónicos, asi como las amenazas de red.

7. Administración	
7.1	La herramienta debe ser capaz de realizar backup y restore de la configuración, permitiendo al administrador programar la realización de los backups en el momento deseado.
7.2	Los backups deben poder ser transferidos a un repositorio vía SFTP o alguna tecnología de transferencia equivalente, es decir, que considere las medidas de seguridad bajo protocolos aceptados por la industria
7.3	La tecnología debe tener su propia aplicación móvil disponible tanto en GooglePlay como en AppleStore para permitir la gestión remota de incidentes.
8. Bloqueo de Amenazas y Respuesta Autonoma	
8.1	Generación de respuestas autónomas y quirúrgicas de manera inteligente cuando surge un incidente altamente anómalo. El sistema interrumpe la actividad maliciosa mientras mantiene las operaciones normales del dispositivo.
8.2	Puede configurarse de modo pasivo o de modo activo según la configuracion predeterminada por el administrador de la herramienta
8.3	Puede detener la anomalia o amenaza hasta en un plazo de 24 horas recurrentes de ser necesario.
9. Deteccion y bloqueo de anomalias a nivel correo	
9.1	La solucion tambien debe contar con una consola que sea capaz de detectar cualquier tipo de ciberamenazas a nivel de buzones de correo para un total mínimo de 180 Buzones.
9.2	Esta solucion debe ser capaz de integrarse con la solucion principal de deteccion de amenazas a nivel de red, con el fin de mostrar una deteccion global de anomalias a nivel de trafico de red y correo
9.3	Debe poder integrarse con O365
9.4	Debe poder dar respuesta autonoma ante cualquier correo malicioso que contenga ciberamenazas tipo malware, spear phishing avanzado, intentos de suplantacion de identidad, secuestro de cuentas, ingenieria social, entre otros.
9.5	La solucion no debe estar en linea y debe poder identificar correos maliciosos en tiempo real.
9.6	Debe utilizar inteligencia artificial, machine learning supervisado y no supervisado para poder detectar anomalias y detenerlas
9.7	La solucion debe ser capaz de tomar multiples acciones de bloqueo como: bloquear el enlace, mover el correo a la carpeta de junk, eliminar el enlace, convertir el archivo sospechoso, entre otros
9.8	La solucion debe poder mostrar al menos el detalle de los correo accionados, tipo de campañas de ciberamenazas que han llegado, correos leidos y no leidos que contenian este tipo de campañas, tipo de respuestas tomadas para cada campaña

9.9	La solucion debe ser capaz de mostrar graficamente quienes son las personas en la organización a la que les llegan mas campañas de ciberamenazas y hacer un perfilamiento de cada una de ellas que al menos muestre su nivel de expocision, tipo de campañas que le llegan y momento en que estas campañas suelen llegar
9.10	La solucion no debe hacer uso de reglas ni firmas para su deteccion de anomalias
10. Deteccion y bloqueo de anomalias a nivel de red	
10.1	Debe inlcuir respuesta automatica que realiza acciones dentro de la red (Consola dentro del appliance), incluso en entornos virtuales. El cual no requiera hardware adicional y permita personalizarse en minimo los sigientes opciones: a.)Modo para establecer confianza: Confirmación humana por parte de los funcionarios, genera respuestas que deben ser validadas por el equipo de seguridad antes de tomar medidas a nivel de red. b) Modo activo: Negocio digital de autodefensa: este modo es totalmente autónomo, lo que significa que una amenaza grave puede ser contenida instantáneamente sin que un analista de seguridad necesite iniciar sesión en la red.
10.2	La solucion debe poder dar respuesta autónoma ante cualquier evento malicioso a nivel de red que contenga ciberamenazas tipo malware, intentos de suplantación de identidad o IP, secuestro de sesiones, o accesos no autorizados, entre otros.
10.3	La solución debe ser capaz de tomar multiples acciones de bloqueo a nivel de red desde la consola centralizada como: bloquear la dirección IP, dispositivos o conexiones a nivel de red, entre otros.
11. Detección y bloqueo de anomalias a nivel de aplicaciones SaaS	
11.1	La solución debe ser capaz proposionar visibilidad e eventos de los productos de Microsoft 365 como Sharepoint/OneDrive (OneDrive for Business), Dynamics y Teams.
11.2	Dependiendo del servicio configurado la solución debe ser capaz de visualizar actividades del usuario, administración de usuarios, creación e intercambio de archivos y eventos administrativos.
11.3	La solución debe ser capaz de recuperar la actividad de Microsoft Teams, incluidos inicios de sesión y cambios en la membresía del equipo. También se recuperan acciones administrativas como la creación de equipos y canales y la adición o eliminación de aplicaciones, conectores y bots de los canales.
11.4	La solución debe ser capaz de proporcionar acceso a una consola SaaS, una interfaz especializada para investigar la actividad de SaaS y la nube. La consola SaaS proporciona acceso a mapas globales de actividad, registros detallados de la actividad del usuario y visualización de cadenas de comportamiento anómalas.

11.5	La solucion tambien debe contar con una consola que sea capaz de detectar cualquier tipo de ciberamenazas a nivel de aplicaciones SaaS para un total mínimo de 180 Buzones.
11.6	Debe poder integrarse con O365
11.7	Debe utilizar inteligencia artificial, machine learning supervisado y no supervisado para poder detectar anomalias y detenerlas
11.8	La solución debe ser capaz de tomar multiples acciones de bloqueo como: Bloquear todas las conexiones de instancia, Bloquear rangos de IP no especificados, bloquear IP fuera de la subred, desasociar perfil de instancia, bloquear acceso público a buckets de S3, deshabilitar rol, deshabilitar usuario, deshabilitar función Lambda, desactivar clave de acceso de usuario, bloquear acción de usuario y bloquear acción de rol.
12. Periodo de vigencia	
12.1	La solución deberá ser licenciada y entregada por un periodo de 12 meses, a partir de la instalación y puesta en marcha.
13. Soporte y servicios del Fabricante	
13.1	El horario de cobertura debe ser 7x24 por 12 meses en el cual se recibira asistencia telefonica y el servicio sera brindado remotamente o en sitio según aplique.
13.2	El fabricante deberá brindar las actualizaciones de software sin costo adicional durante el periodo de vigencia del la suscripción de la solucion.
13.3	En caso de falla del equipo, el fabricante deberá proporcionar los materiales y/o piezas para su reparación o en todo caso un equipo nuevo para el reemplazo.
14. Acceso al Portal de Capacitación	
14.1	Usuario de acceso del portal de capacitación del fabricante