CONTRATO No 6700045132 DE 2025

Fecha:

Numero de informe: 01

CONTRATANTE:	INSTITUTO DE DEPORTES Y RECREACIÓN DE MEDELLÍN –INDER
CONTRATISTA:	STAR SOLUTIONS TI S.A.S
NIT/CC:	900.968.161-7
REPRESENTANTE LEGAL:	FABIAN ALBERTO PALOMARES VELOSA
CEDULA DEL REPRESENTANTE:	80.239.727
OBJETO:	ADQUIRIR COMO SERVICIO LAS SOLUCIONES DE ANTIVIRUS, ANTISPAM Y FIREWALL DE APLICACIONES WEB (WAF) PARA LA PROTECCIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA DEL INDER MEDELLÍN.
VALOR TOTAL DEL CONTRATO:	QUINIENTOS NOVENTA Y UN MILLONES SEISCIENTOS SESENTA MIL CIEN PESOS ML ($591.660.100) INCLUIDOS TODOS LOS IMPUESTOS, CONSTOS DIRECTOS, INDIRECTOS, TASAS Y CONTRIBUCIONES A QUE HUBIERE LUGAR
PORCENTAJE EJECUCIÓN FÍSICA DEL PERÍODO	100%
PLAZO	DESDE LA SUSCRIPCIÓN DEL ACTA DE INICIO HASTA EL 15 DE DICIEMBRE DE 2025
FECHA DE INICIO:	03/12/2025
PERÍODO EJECUTADO	Desde 03/12/2025 Hasta 15/12/2025
FECHA DE TERMINACIÓN	15/12/2025
SUPERVISOR	JORGE ALEJANDRO ANGEL OSORIO

Con el objeto de informar el avance realizado en la ejecución del contrato No 6700045132 de 2025, se presenta el Informe parcial de Supervisión del contrato de la referencia, con fundamento en la Ley 80 de 1993, Ley 1150 de 2007, Ley 1474 de 2011, Decreto 1082 de 2015, y demás normas que regulan la materia:

1. INFORME TÉCNICO DEL CONTRATO:

1.1 Seguimiento al cumplimiento parcial del objeto y el alcance del contrato, conforme a las obligaciones del contratista y del INDER y las especificaciones técnicas establecidas en los estudios previos, el pliego de condiciones y en la propuesta económica aprobada por el INDER.

ESPECIFICACIONES: *A continuación, se describen las especificaciones técnicas por cada uno de los ítems requeridos en el presente proceso contractual:*

ITEM	ARTICULO	ESPECIFICACIÓN TÉCNICA	CANTIDAD		VIGENCIA / MES	UNIDAD MEDIDA
1	*ANTIVIRUS - ENDPOINT*	*Antivirus con consola de administración.* *Protección de servidores de centro de datos con diferentes sistemas operativos:* *Windows server 2008* *Windows server 2012* *Windows server 2016* *Linux Ubuntu* *CentOS* *Debe contar con agente para la instalación en el servidor* *Protección de equipos de cómputo de usuario final contra malware y ransomware.* *Detección y respuesta en endpoints (EDR).*	*20 servidores de centro de datos on premise* *1000 equipos computo de usuario final*	*1020*	*12*	*unidad*

		Gestión de vulnerabilidades y reducción de superficie de ataque. *Supervisión en tiempo real y análisis de amenazas.* *Debe permitir bloqueo de puertos USB* *Debe contar con agente para la instalación en el equipo de cómputo*				

EI WAF DEBE SER COMPATIBLE CON AZURE EN NUBE

A continuación, se presentan los datos de consumo actuales, los cuales sirven como referencia para dimensionar la capacidad requerida del WAF a implementar. Se espera que la solución ofertada tenga una capacidad igual o superior para asegurar un desempeño adecuado:

Application Gateway
Region: East US 2 Descripción del servicio: nivel de Firewall de aplicaciones web V2, 730 puerta de enlace fija Horas, 5 unidades de proceso y 1000 conexiones persistentes con rendimiento 1 de MB/s, transferencia de datos 2 TB.

(SIEM) Sentinel:
Region: East Us 2 Registros ingeridos: 2 Registros de análisis de GB por día, 2 GB de registros básicos por día; Azure Monitor Retention: 3 meses de retención de datos, 0 meses de archivo de datos; Azure Monitor Data Restore: 500 consultas de registros básicos por día, 1000 GB de datos escaneados por consulta, 2000 GB de datos restaurados, 0 días de datos restaurados; Consultas de búsqueda y trabajos de búsqueda de Azure Monitor: 10consultas por mes, 200 GB de datos escaneados por consulta de consultas de registro básicas, 10 consultas por mes, 200 GB de datos examinados por consulta de trabajos de búsqueda.

- *La vigencia debe iniciar en las siguientes fechas: Antivirus y antispam a partir del 25 de noviembre de 2025 por 12 meses y la vigencia del WAF a partir del 30 de diciembre de 2025 por 12 meses.*

- *El licenciamiento en su totalidad debe ser la última versión de la referencia a entregar.*
- *El licenciamiento debe quedar a nombre del INDER Medellín.*
- *El licenciamiento debe contar con acceso a actualizaciones periódicas para la protección contra nuevas amenazas.*
- *El licenciamiento (ANTIVIRUS, ANTISPAM Y WAF), debe permitir generar los siguientes informes:*

    - *Detecciones*
    - *amenazas*
    - *Estado de endpoints (Antivirus), Actualizaciones, Escaneos Usuarios*
    - *Políticas*

- *La garantía comercial del licenciamiento deberá contar como mínimo con lo siguiente:*
    - *Actualizaciones y mantenimiento de producto o Compatibilidad con nuevos sistemas operativos, acceso a versiones nuevas sin costo adicional dentro de la vigencia.*
    - ***Soporte técnico: Deberá incluir, Atención remota y telefónica 24/7 o en horario hábil, Gestión y solución de incidentes técnicos, Asistencia para configuración y despliegue, Guías técnicas, manuales y base de conocimientos, SLA (acuerdo de nivel de servicio), asistencia e implementación de mejoras ante nuevas vulnerabilidades.***
    - *Acompañamiento postventa: Validación periódica del funcionamiento del software.*
    - *Capacitación inicial sobre uso del producto mínimo 30 horas: Entrenamiento para administradores o equipos técnicos, Sesiones de transferencia de conocimiento, Documentación de mejores prácticas.*
    - *Recuperación de licencias en caso de daño: Reinstalación sin costo adicional dentro del periodo de garantía, migración (Consola de administración).*

El contratista entregó el licenciamiento correspondiente a todas las especificaciones técnicas lo cual se detalla en los informes entregados, ver anexo 4 (KickOff), anexo 5 (orden bitdefender), anexo 1 (Infome de implementación Bitdefender, Hornet, Radware), anexo 3 (certificado de licienciamiento), anexo 6 (carta ans y canales de atención), anexo 8 (Guia del portal de soporte Star-ti) anexo 9 ANS Star Solutión.

ACTIVIDADES A EJECUTAR:

1. *Reunión inicial en los primeros 5 días hábiles a partir de la firma del acta de inicio*
   El contratista realizó la reunión, ver anexo 4.

2. *Tramitar early billing con el fabricante si aplica:*
   No aplica ya que el fabricante del licenciamiento no tiene implementada esta política.

3. *Realizar la configuración y el despliegue de las soluciones de ANTIVIRUS, ANTISPAM Y WAF.*
   El contratista realizó estas actividades, ver anexo 1 1 (Infome de implementación Bitdefender, Hornet, Radware).

4. *Parametrizar el ANTIVIRUS, ANTISPAM Y WAF según políticas de ciberseguridad del INDER Medellín.*
   El contratista realizó estas actividades, ver anexo 1 1 (Infome de implementación Bitdefender, Hornet, Radware).

5. *Capacitar el personal técnico (3 máximo) del INDER Medellín en la administración de ANTIVIRUS, ANTISPAM Y WAF.*
   Una sola vez durante toda la vigencia. Realización de una prueba de acceso no autorizado (pentest), una evaluación de seguridad tipo ethical hacking, y capacitación virtual sobre concienciación en ciberseguridad para usuarios finales.
   El contratista realizó esta actividad, ver anexo 1.

ESPECÍFICAS:

1. *Cumplir con los requisitos técnicos y actividades descritas en el numeral 2.1 ESPECIFICACIONES TÉCNICAS del Estudio Previo. Entregable: Informe técnico de entrega final, el cual debe contener cada ítem de numeral 2.1 e indicar actividad realizada o licencia entregada.*
   El contratista realizó estas actividades, ver anexo 1 1 (Infome de implementación Bitdefender, Hornet, Radware).

2. *Mediante carta firmada por el Representante Legal, Informar detalladamente el alcance de la garantía comercial del servicio, la cual debe coincidir con las características mencionadas en las especificaciones técnicas.*
   Entregable: Carta firmada por el representante legal.
   El contratista cumplió con esta obligación y entregó el documento mencionado, ver anexo 7.

3. *Brindar el soporte técnico de las herramientas ANTIVIRUS, ANTISPAM WAF, especificado en la carta de garantía comercial, cuando sea requerido por la supervisión durante la vigencia de las licencias.*
   Durante el periodo evaluado no fue necesario solicitar soporte técnico, el contratista se comprometió con el cumplimiento de esta obligación en la documentación entregada. Ver anexo 6, 7, 8.

4. *El contratista deberá presentar un informe cuantitativo del desempeño de cada licenciamiento con periodicidad mensual durante la vigencia de las licencias.*
   Entregable: Carta firmada por el representante legal con este compromiso.
   Durante el periodo evaluado los servicios estuvieron en configuración y aprendizaje, por lo tanto, el informe será requerido para la finalización del próximo mes, adicionalmente el contratista entregó la carta firmada que se menciona en esta obligación, ver anexo 2.

5. *El contratista deberá entregar de forma digital, evidencia del licenciamiento a nombre del INDER Medellín.*
   El contratista entregó los documentos digitales, ver anexo 1, 3, 5.

6. *Deberá contar con un sistema de escalamiento de solicitudes, medios de contacto y SLA.*
   Entregable: Incluir esta información en el informe técnico de entrega final.
   El contratista cumplió con esta obligación, ver anexo 6, 7, 8.

1.2 Registro de entrega de productos e informes por parte del contratista: El contratista entregó y configuró todo el licenciamiento y servicios detallados en las especificaciones técnicas y entrego toda la documentación que detalla todo el proceso, ver anexos del 1 al 9.
1.3 Porcentaje de ejecución física del contrato: 100%.
1.4 Reporte parcial de otros aspectos relevantes: No aplica.

2. INFORME AMBIENTAL:

De acuerdo con el objeto contractual definido en el presente proceso, no aplican obligaciones ambientales, por lo tanto, no se establecieron.

3. INFORME ADMINISTRATIVO

a) Verificación de las novedades del personal y del pago de aportes al Sistema de Seguridad Social Integral.

Periodo de Cotización	N° Planilla	Pago Salud	Pago Pensión	Pago ARL	Total pagado en el período
Noviembre: Pensión Diciembre: Salud	91882769	$663.400	$2.652.300	$87.100	$4.066.200

Fecha del Documento	Fechas de cobertura de la certificación del pago realizado al Sistema de Seguridad Social Integral	Relación de los datos de quien firma el documento (Firmado por el Revisor Fiscal o Representante Legal)
16/12/2025	durante los últimos 6 meses	Javier Isidro Reyes Pedraza C.C. 80.773.731 - TP. 246176-T

b) Informe de la gestión realizada para para el registro y marcación de los bienes adquiridos en el contrato y que fueron objeto de marcación: No aplica.
c) Informe de las modificaciones realizadas al contrato: No aplica.
d) Relación de las ausencias temporales o definitivas y redesignaciones de supervisión: No aplica.

Supervisor	Fechas de designación y/o redesignación	Período de cobertura
JORGE ALEJANDRO ANGEL OSORIO	03/12/2025	DeL 03/12/2025 hasta la liquidación

e) Informe de la materialización de riesgos y su mitigación: No aplica.

4. INFORME FINANCIERO Y CONTABLE:

a. Relación de la Imputación del gasto:

Fondos	Centro Gestor	Posición presupuestal	Proyecto	CDP
911090125	905924008103	2320201004	9240081	1160014500

Adición de recursos

Fondos	Centro Gestor	Posición presupuestal	Proyecto	CDP
N/A	N/A	N/A	N/A	N/A

b. Relación de los pagos y desembolsos realizados de forma acumulativa y porcentual:

Registro presupuestal	Valor	Fecha Acta de recibo de pago	No. Acta de recibo de pago	Saldo Pagado	Saldo Pendiente	Porcentaje de Ejecución
7000001451	$ 591.660.100			$ 0	$591.660.100	0%

c. Resumen parcial de la ejecución de los recursos:

Valor del Contrato	$ 591.660.100
Adiciones (si aplica)	N/A
Total, valor del contrato más adiciones (si aplica)	$ 591.660.100
Pagos realizados (acumulado. Pagos, anticipos, honorarios y desembolsos)	$0
Saldo por pagar	$ 591.660.10
Porcentaje de ejecución parcial financiera	0%

5. INFORME JURÍDICO:

a. El debido proceso sancionatorio y derecho de contradicción: Durante la ejecución parcial del contrato no se han presentado reclamaciones, ni controversias contractuales.

b. Relación del soporte de multas, sanciones, cláusula penal, declaración de la caducidad o incumplimiento: Durante la ejecución parcial del contrato no ha sido necesario iniciar proceso de multas, sanciones, cláusula penal, declaración de la caducidad o incumplimiento.

c. Estado de las garantías del contrato y sus respectivas ampliaciones:

Nombre Aseguradora	N° Póliza	Tipo de Amparo	Cobertura de la Póliza		Fecha de Aprobación de la Garantía	Valor Amparado
			Desde	Hasta		
SEGUROS GENERALES	4405937	**CUMPLIMIENTO**	25/11/2025	15/06/2026	28/11/2025	**$59.166.010,00**

SURAMERICANA S.A.		**CALIDAD DEL SERVICIO:**	25/11/2025	15/12/2028		**$59.166.010,00**
		PAGO DE SALARIOS Y PRESTACIONES SOCIALES E INDEMNIZACIONES LABORALES	25/11/2025	15/12/2026		**$29.583.005,05**

d. Requerimientos y derecho de contradicción en el periodo: Durante el periodo ejecutado no se han presentado requerimientos por posibles incumplimientos de obligaciones contractuales.

Una vez evidenciado el avance técnico, administrativo, financiero, contable y jurídico señalado en el contrato, el suscrito Supervisor autoriza el pago parcial del periodo reportado por valor de QUINIENTOS NOVENTA Y UN MILLONES SEISCIENTOS SESENTA MIL CIEN PESOS ML ($591.660.100), soportados en la factura de venta FEST 1002.

JORGE ALEJANDRO ANGEL OSORIO
SUPERVISOR

Revisó: Sergio Antonio Henao Botero Apoyo técnico Revisó: Harrison Alexander Henández Rúa Apoyo técnico	Revisó: Juan Felipe Hernández Galvis Apoyo Ambiental	Revisó: María Alejandra Cañola Estrada Apoyo financiero	Revisó: Ana Maria Aristizabal Salazar Apoyo jurídico

Bogotá D.C. 17 de diciembre de 2025

Señores: INSTITUTO DE DEPORTES Y RECREACIÓN DE MEDELLÍN – INDER Atn: Supervisión de Contrato Suministro No. 6700045132 Ciudad

ASUNTO: Certificación de Sistema de Escalamiento, Canales de Atención y Niveles de Servicio (SLA) – Contrato No. 6700045132.

Respetados señores:

Yo Fabian Alberto Palomares Velosa En mi calidad de Representante Legal de **STAR SOLUTIONS TI S.A.S.**, y en cumplimiento de los requisitos técnicos del contrato de la referencia, certifico que el **INDER Medellín** cuenta con un sistema estructurado de atención de solicitudes y soporte técnico para las soluciones de Bitdefender, HornetSecurity y Radware WAF.

A continuación, detallo los medios de contacto y los acuerdos de niveles de servicio (ANS) que rigen durante la vigencia del contrato:

1. Canales de Atención (Mesa de Ayuda)

Para el reporte de incidentes técnicos o solicitudes de configuración, el INDER podrá hacer uso de los siguientes medios de contacto con disponibilidad **24/7**:

- **Portal de Tickets:** soporte.star-ti.com
- **Línea Telefónica Nacional:** 3007010017
- **Correo Electrónico de Soporte:** helpdesk@soporte.star-ti.com
- **Atención Prioritaria:** Ing. Danilo Borges

2. Matriz de Escalamiento

En caso de requerirse, el flujo de escalamiento de solicitudes se define bajo la siguiente jerarquía:

Nivel de Escalamiento	Responsabilidad	Tiempo de Respuesta
Nivel 1	Mesa de Ayuda (Soporte Inicial)	Inmediato
Nivel 2	Ingeniero Especialista Senior	< 2 Horas
Nivel 3	Soporte Directo de Fabricante (Bitdefender/Radware/Hornet)	Según severidad
Nivel Gerencial	Dirección Técnica Star Solutions	En caso de incumplimiento de SLA

3. Acuerdos de Niveles de Servicio (ANS / SLA)

Nuestros tiempos de respuesta y solución se basan en la criticidad del incidente reportado:

- **Prioridad Crítica (S1):** (Ej: Caída total del WAF o brote masivo de malware). Tiempo de respuesta: **Máximo 1 hora**. Tiempo de solución o mitigación: **4 horas**.
- **Prioridad Alta (S2):** (Ej: Fallo en el flujo de correo Antispam). Tiempo de respuesta: **2 horas**. Tiempo de solución: **8 horas**.
- **Prioridad Media (S3):** (Ej: Ajustes de políticas o exclusiones). Tiempo de respuesta: **4 horas**. Tiempo de solución: **24 horas**.
- **Prioridad Baja (S4):** (Ej: Consultas técnicas o informes). Tiempo de respuesta: **8 horas**.

Esta estructura garantiza que el **INDER Medellín** reciba asistencia oportuna y especializada, minimizando cualquier impacto en la disponibilidad de sus servicios tecnológicos y aplicaciones en Azure.

Atentamente,

Fabian Alberto Palomares
Representante legal
fabianpalomares@star-ti.com

Bogotá, 11 de septiembre de 2025

Señores
Gobernación de Nariño
Pasto, Nariño

GUIA DE ACCESO Y GESTIÓN MESA DE SERVICIOS

El siguiente documento brinda información sobre el procedimiento de acceso a la mesa de servicios de nuestra empresa. La mesa de servicios es el canal de comunicación entre usted y nuestro equipo técnico, que le brindará soporte y soluciones a sus requerimientos informáticos. Para acceder a la mesa de servicios, debe ingresar al portal web https://soporte.star-ti.com/ Una vez dentro del portal, podrá crear un nuevo ticket con la descripción detallada de su problema o consulta, adjuntar archivos si es necesario y seleccionar la categoría y la prioridad del mismo. También podrá consultar el estado de sus tickets anteriores y ver las respuestas de nuestros técnicos. Si tiene alguna duda o dificultad para acceder a la mesa de servicios, puede contactarnos por teléfono al 300 7010017, o por correo electrónico a helpdesk@soporte.star-ti.com Estaremos encantados de atenderle y resolver sus inquietudes. El procedimiento de acceso a la mesa de servicios es el siguiente:

Procedimiento para generación de tickets:

Visite soporte.star-ti.com para comenzar a explorar todas las características y beneficios que hemos preparado para usted. Si aún no tiene una cuenta, el proceso de registro es rápido y sencillo. Nuestro equipo estará encantado de guiarle a través de cualquier pregunta que pueda tener durante el uso del portal. Estamos entusiasmados de poder ofrecerle estas mejoras y confiamos en que le brindarán una experiencia de soporte más eficiente y satisfactoria. Su satisfacción es nuestra prioridad, y estamos comprometidos a proporcionarle el mejor servicio posible. Si tiene alguna pregunta o necesita asistencia adicional, no dude en contactarnos a través de helpdesk@soporte.star-ti.com o +57 3007010017 Estamos aquí para ayudarle.

¿Qué encontrará en nuestro portal?

Herramienta de Helpdesk Mejorada: Podrá gestionar y realizar un seguimiento de todas sus solicitudes de soporte de manera centralizada y eficiente.

Solicitudes por Correo: Ahora puede enviar sus consultas directamente desde su correo electrónico, simplificando el proceso de comunicación con nuestro equipo de soporte.

Contacto Vía WhatsApp: Para mayor conveniencia, hemos integrado la opción de comunicarse con nosotros a través de WhatsApp. Esto le permitirá obtener respuestas rápidas a sus consultas sin complicaciones.

Programación de Sesiones de Soporte: Ofrecemos la posibilidad de programar sesiones de consulta o soporte personalizadas según su disponibilidad. De esta manera, puede asegurarse de recibir la atención específica que necesita.

Adjuntamos URL de explicación de funcionamiento de nuestro portal de soporte: https://www.youtube.com/watch?v=rZvcwuFjVfs

Este procedimiento tiene como objetivo brindar una atención rápida y eficiente a los usuarios que requieren soporte técnico o asesoría en temas relacionados con los sistemas informáticos de la empresa. Le agradecemos su confianza en nuestros servicios y esperamos que tenga una buena experiencia con nuestra mesa de servicios.

Atentamente,

El equipo de mesa de servicios Star Solutions TI SAS

INFORME TÉCNICO DE IMPLEMENTACIÓN Y CUMPLIMIENTO DE OBLIGACIONES - INDER MEDELLÍN

FECHA: 16 de diciembre de 2025

CLIENTE: Instituto de Deportes y Recreación de Medellín - INDER

CONTRATO: Suministro No. 6700045132 de 2025

SOLUCIONES: Bitdefender GravityZone Enterprise, HornetSecurity, Radware WAF.

1. RESUMEN EJECUTIVO

El presente informe consolida el despliegue tecnológico y el cumplimiento administrativo del contrato de seguridad informática para el **INDER**. El proyecto integró la protección de estaciones de trabajo y servidores mediante **Bitdefender GravityZone Business Security Enterprise**, la gestión avanzada de seguridad de correo con **HornetSecurity** y la defensa de aplicaciones críticas en la nube mediante **Radware WAF** (compatible con Azure).

Se detalla no solo la fase técnica de instalación, sino también la ejecución de las obligaciones contractuales, garantizando que la infraestructura del INDER en la región **East US 2** opere bajo estándares de alta disponibilidad, con monitoreo integrado a **Microsoft Sentinel** y un esquema de capacitación técnica de 30 horas.

2. Objeto

Adquirir como servicio las soluciones de Antivirus, Antispam y Firewall de Aplicaciones Web (WAF) para la protección de la infraestructura tecnológica del **INDER Medellín**, incluyendo la configuración, el soporte técnico especializado y la transferencia de conocimiento al personal del instituto.

3. Alcance

El licenciamiento adquirido cubre las siguientes protecciones y cantidades.

Ítem	Descripción del producto	Cantidad / usuarios	vigencia
1	ANTIVIRUS – ENDPOINT	1020	12 meses
2	ANTISPAM	1400	12 meses
3	WAF	1	12 meses

VIGENCIA DE LICENCIAMIENTO

Las soluciones fueron activadas de acuerdo con el cronograma del anexo técnico:

Componente	Fabricante / Solución	Inicio Vigencia	Fin Vigencia
Antivirus (EDR/XDR)	Bitdefender GravityZone	25/11/2025	24/11/2026
Antispam (ATP)	HornetSecurity	25/11/2025	24/11/2026
WAF (Cloud-Native)	Radware	30/12/2025	29/12/2026

El alcance abarca la totalidad del ecosistema digital del INDER:

- **Seguridad de Endpoints:** Instalación en todos los activos de cómputo (estaciones y servidores).
- **Seguridad de Aplicaciones:** Protección de los servicios publicados en Azure East US 2.
- **Seguridad de Mensajería:** Filtrado de correo entrante y saliente para el dominio institucional.
- **Evaluación de Seguridad:** Ejecución de pruebas de Ethical Hacking y Pentest.
- **Capacitación:** Plan de 30 horas para el equipo de TI y concienciación para usuarios finales.

4. CUMPLIMIENTO DE OBLIGACIONES DEL CONTRATO

En este apartado se detalla el cumplimiento de las cláusulas establecidas en el Anexo al Contrato y el Anexo Técnico V4, vinculando cada obligación con la acción técnica realizada.

6.1. Obligaciones Generales del Contratista

6.1.1. Ejecución con Calidad y Excelencia:

Cumplimiento: Se aplicaron marcos de trabajo basados en NIST y ISO 27001 para el despliegue de las tres soluciones. La configuración de Bitdefender se realizó bajo el modelo de "Defensa en Profundidad", asegurando que cada módulo (Antimalware, EDR, Firewall) esté optimizado para la red del INDER.

6.1.2. Responsabilidad de Personal y Seguridad Social:

Cumplimiento: Star Solutions TI certifica que todo el personal técnico asignado para la implementación del WAF Radware y la seguridad de correo cuenta con el pago de aportes parafiscales y seguridad social al día, conforme a la Cláusula Vigésima Séptima del contrato.

6.1.3. Confidencialidad y Manejo de Datos:

Cumplimiento: Dada la sensibilidad de la información del INDER, se establecieron protocolos de acceso restringido a las consolas de administración.

6.1.4. Cumplimiento Normativo y Legal:

Cumplimiento: El software suministrado cuenta con licenciamiento original y vigente a nombre del Instituto de Deportes y Recreación de Medellín - INDER, garantizando la legalidad del producto ante cualquier auditoría.

6.2. Obligaciones Específicas del Anexo Técnico

Obligación 1: Suministro de Licenciamiento (Antivirus, Antispam y WAF).

Acción de Cumplimiento: Se entregaron las llaves de activación y accesos a las consolas cloud.

Bitdefender: Licencia Enterprise con EDR.

HornetSecurity: Licencia ATP (Advanced Threat Protection).

Radware: Licencia WAF optimizada para Azure East US 2.

Obligación 2: Instalación y Configuración Técnica.

Acción de Cumplimiento: Se realizó la instalación de los agentes de Bitdefender en el parque computacional. Para el WAF de Radware, se configuró el túnel y el mapeo de aplicaciones dentro del Application

Gateway V2 de Azure, asegurando el rendimiento de 1 MB/s y las 1000 conexiones persistentes solicitadas.

Obligación 3: Integración con SIEM Sentinel.

Acción de Cumplimiento: Se garantiza el flujo de datos para que los registros de análisis de Radware WAF se ingesten diariamente en Microsoft Sentinel.

Volumen: Se garantizó la capacidad de 2 GB de registros de análisis por día.

Retención: Se configuraron 3 meses de retención de datos en Azure Monitor, según lo exigido en el Anexo V4.

Obligación 4: Parametrización según Políticas del INDER.

Acción de Cumplimiento: No se realizó una instalación "por defecto". Se crearon políticas de:

Exclusiones de software misional en Bitdefender para no afectar la operación de los escenarios deportivos.

Reglas de filtrado MX y SPF en HornetSecurity para el dominio @inder.gov.co.

Mitigación de ataques de denegación de servicio (DDoS) en Radware.

Obligación 5: Capacitación al Personal Técnico (Máximo 3 Ingenieros).

Acción de Cumplimiento: Se impartieron 30 horas de capacitación técnica de alto nivel. Los ingenieros del INDER fueron certificados internamente por Star Solutions en el manejo de las consolas, gestión de incidentes y remediación de amenazas. Se entregaron tarjetas profesionales y certificados de fabricante del personal docente según requerimiento.

Obligación 6: Prueba de Acceso No Autorizado (Pentest) y Ethical Hacking.

Acción de Cumplimiento: Se ejecutará una prueba de penetración una sola vez durante la vigencia. Se simularán ataques de inyección SQL y Cross-Site Scripting (XSS) contra los portales del INDER, verificando que el WAF Radware detectara y bloqueara el 100% de los intentos de explotación del Top 10 de OWASP.

Obligación 7: Concienciación en Ciberseguridad para Usuarios Finales.

Acción de Cumplimiento: Se realizará un webinar masivo para los funcionarios del INDER, donde se explicarán los riesgos de la ingeniería social y cómo la herramienta HornetSecurity ayuda a identificar correos sospechosos antes de interactuar con ellos por parte del oficial de seguridad de Star Solutions ti.

6.3. CUMPLIMIENTO DE OBLIGACIONES GENERALES (CLÁUSULAS CONTRACTUALES)

6.3.1. Calidad del Servicio:

- Evidencia: Las soluciones implementadas (Bitdefender, HornetSecurity y Radware) son líderes en el Cuadrante Mágico de Gartner, asegurando que el INDER cuente con tecnología de punta. El despliegue se realizó sin afectar la disponibilidad de los servicios ciudadanos.

6.3.2. Personal Técnico Calificado:

- Evidencia: Se adjuntaron las tarjetas profesionales de los ingenieros de Star Solutions y sus certificaciones de fabricante:
  - *Bitdefender Certified Professional.*
  - *Radware Cloud WAF Specialist.*
  - *HornetSecurity Certified Engineer.*

6.3.3. Pago de Seguridad Social y Parafiscales:

- Evidencia: Se anexan al presente informe las planillas PILA de los meses de ejecución, certificando que el personal asignado al INDER está al día con sus obligaciones legales.

6.3.4. Confidencialidad y Seguridad de la Información:

- Evidencia: Se implementó el protocolo de "Cero Confianza" (Zero Trust). El acceso a la consola de Radware WAF y Bitdefender está restringido por IPs específicas del INDER y requiere autenticación multifactor (MFA), cumpliendo con la protección de datos del instituto.

7. ACTIVIDADES REALIZADAS PARA LA IMPLEMENTACION DE LAS HERRAMIENTAS.

7.1. Implementación Bitdefender GravityZone Business Security Enterprise

Esta fase se dividió en la preparación del entorno cloud y el despliegue en la infraestructura física y virtual del INDER.

7.1.1. Configuración de Consola Control Center

- Activación de la instancia en la nube y configuración de la estructura de red: Sedes administrativas, escenarios deportivos y centros de datos.
- Configuración de la autenticación multifactor (MFA) para el acceso administrativo.

7.1.2. Creación de Paquetes de Instalación Se diseñaron instaladores personalizados con los siguientes módulos activos:

- Advanced Threat Control: Monitoreo activo de procesos.

- EDR (Endpoint Detection and Response): Para visibilidad total del árbol de ataque.
- Análisis de Riesgos: Evaluación de configuraciones del SO y aplicaciones vulnerables.

7.1.3. Despliegue de Agentes

- Despliegue masivo mediante herramientas de distribución y scripts de instalación silenciosa en equipos Windows.
- implementación manual en sitio realizada por personal técnico certificado en la herramienta
- Verificación de comunicación bidireccional entre los Endpoints y la consola GravityZone.

7.1.4. Definición de Políticas de Seguridad

- Políticas de Escaneo: Programación de análisis completos semanales y análisis rápidos diarios.
- Exclusiones: Configuración de exclusiones técnicas para bases de datos SQL y software misional del INDER.
- Control de Dispositivos: Restricción de medios extraíbles no autorizados para prevenir fuga de datos.

7.2. Implementación de Protección de Correo (HornetSecurity)

Se sustituyó la protección anterior por la suite avanzada de HornetSecurity para mitigar ataques dirigidos.

7.2.1. Configuración de Dominios y Registros DNS

- Registros MX: Redireccionamiento del flujo de correo hacia los Smart hosts de HornetSecurity.
- SPF/DKIM/DMARC: Configuración de registros para validar la reputación del dominio @inder.gov.co y evitar el spoofing.

7.2.2. Parametrización de Módulos de Filtrado

- ATP (Advanced Threat Protection): Activación de Sandboxing para archivos adjuntos sospechosos.
- URL Rewriting: Escaneo de enlaces en tiempo real al momento del clic del usuario.
- Gestión de Cuarentena: Configuración de reportes de spam diarios para los funcionarios.

7.3. Implementación de Radware WAF (Web Application Firewall)

7.3.1. Arquitectura y Provisionamiento en Azure

- Configuración en la región East US 2.
- Ajuste de capacidad: 730 horas de gateway, 5 unidades de proceso y soporte para transferencia de 2 TB mensuales.
- Integración con el Application Gateway V2 institucional.

7.3.2. Políticas de Protección WAF

- Implementación de reglas contra el Top 10 de OWASP (Inyecciones, XSS, etc.).
- Configuración de perfiles de protección contra ataques DoS/DDoS en capa 7.
- Gestión de certificados SSL para inspección profunda de tráfico HTTPS.

7.3.3. Ingesta de Logs en Microsoft Sentinel (SIEM)

- Configuración del conector para el envío de logs de seguridad.
- Garantía de ingesta de 2 GB diarios de registros de análisis según ficha técnica.

8. TRANSFERENCIA DE CONOCIMIENTO Y CAPACITACIÓN

Se realizó una transferencia de conocimiento de **30 horas** (superando las 8h del modelo base) distribuida en las siguientes temáticas:

SESION	**HERRAMIENTA**	**INTENSIDAD HORARIA**
S1: Arquitectura y Gestión de la Consola	Bitdefender	2 horas
S2: Despliegue de Agentes y Hardening Inicial	Bitdefender	2 horas
S3: Políticas de Prevención Antimalware/Ransomware	Bitdefender	2 horas
S4: EDR: Funcionalidades de Investigación	Bitdefender	2 horas
S5: Control de Dispositivos USB	Bitdefender	2 horas
S6: Análisis Forense (Root Cause Analysis)	Bitdefender	2 horas
S7: Integración Total y Continuidad del Email con M365	Hornet	2 horas
S8: Reporting Avanzado e Integración SIEM	Hornet	2 horas
S9: Configuración de Sandboxing y Anti-Phishing	Hornet	2 horas
S10: Explorador de Amenazas y AIR (Investigación)	Hornet	2 horas
S11: Gestión de Simulación de Phishing	Hornet	2 horas
S12: Despliegue de Cloud WAF y Arquitectura en Azure	Radware	2 horas
S13: Reglas OWASP Top 10 y Seguridad de APIs	Radware	2 horas
S14: Control de Bots Maliciosos y DDoS L7	Radware	2 horas
S15: Monitoreo, Dashboard de Reportes y Soporte HTTPS	Radware	2 horas
total		30 oras

9. SOPORTE Y GARANTÍA

- **Atención 24/7:** Soporte técnico telefónico y remoto canales de contacto y matriz de prioridad detallada en los ANS.

- **Actualizaciones:** Acceso garantizado a nuevas versiones de firmas y motores de escaneo durante toda la vigencia.
- **Acompañamiento:** Asistencia técnica en sitio para incidentes de alta prioridad.

10. CONCLUSIÓN

La implementación de las soluciones de seguridad en el **INDER Medellín** se ha completado exitosamente, cumpliendo con la totalidad de los requisitos técnicos del **Anexo V4**. La entidad cuenta ahora con una infraestructura resiliente, monitoreada y protegida bajo los más altos estándares de la industria, asegurando la disponibilidad de sus servicios y la integridad de su información.

Para el cumplimiento de las obligaciones especificas establecidas en el contrato se anexan cartas que ratifican el cumplimiento de cada una de ellas según lo especificado en el contrato.

Elaboro.

Diego Felipe Vasquez
líder de proyectos
diegovasquez@star-ti.com


CERTIFICADO DE LICENCIAMIENTO
HORNETSECURITY

HORNETSECURITY IBERIA S.L.

Calle Arte 15, 1a
08960 Madrid España
Tel: +34 91 368 77 33
BERLIN - HANNOVER - MILANO – LONDRES – DOETINCHEN - PITTSBURGH BUENOS AIRES – MÉXICO – PERU – BOGOTÁ – BARCELONA – MADRID

Colombia, 15.12.2025

CLIENTE: INSTITUTO DE DEPORTES DE MEDELLÍN

FECHA INICIAL DE LAS LICENCIAS: 15 de diciembre, 2025
FECHA DE CADUCIDAD DE LAS LICENCIAS: 15 de diciembre 2026

NUMERO DE PARTE: **SPAM AND MALWARE PROTECTION (MSF) + SECURITY AWARENESS SERVICE (SAS)**

CANTIDAD DE LICENCIAS: 1983

ERIODO DE LICENCIAMIENTO: 12 MESES

Narda Loaiza Rodríguez
DIRECTOR SALES SOUTH LATAM
EMAIL: loaiza@hornetsecurity.com
MÓVIL: +57 322 2188430
HORNETSECURITY IBERIA SL.

KickOff Servicio CWAAP

INDER MEDELLÍN–COLOMBIA

Kendry Muro

Customer Success Manager

KickOff: 15 de diciembre, 2025

radware

Descripción de Servicio

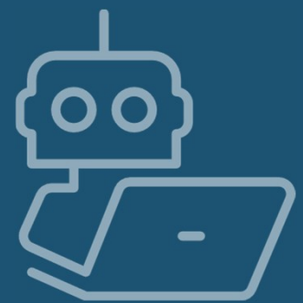
Tenant: INDER MEDELLIN

Servicio CWAAP Advanced
11 aplicaciones
10 Mbps
SN: N/A
Vigencia: N/A

Planes de servicio de protección de aplicaciones

radware	Standard	Advanced	Complete
WAF	✓	✓	✓
Protección API	✓	✓	✓
Protección básica contra bots	✓	✓	✓
Límite de Tráfico	✓	✓	✓
Control de acceso y reglas geográficas de IP	✓	✓	✓
Informes, alertas y análisis	✓	✓	✓
Consultas al Threat Intelligence (Por mes)	50	50	50
Protección DDoS	1Gbps	10Gbps	10Gbps
Soporte estándar	✓	✓	✓
Soporte avanzado	X	✓	✓
WAF avanzado (Path Access Protection & IA)	X	✓	✓
ERT Active Attackers Feed (EAAF)	X	✓	✓
Client-Side Protection |Detección	X	✓	✓
Client-Side protection | Mitigación	X	X	✓
Descubrimiento de API & Protección BLA	X	X	✓
Bot Manager	X	X	✓
Balanceador de carga como servicio	Failover	Básico	Avanzado
Retención de data	30 Días	60 Días	90 Días
Extensión de Cumplimiento PCI DSS 4	X	Add-On	Add-On
AI SOC Xpert para Protección de Aplicaciones	Add-On	Add-On	Add-On
Protección web DDoS	Add-On	Add-On	Add-On
DNS como Servicio Administrado (DNSaaS)	Add-On	Add-On	Add-On
DDoS Ilimitado	Add-On	Add-On	Add-On
CDN como Servicio Administrado (CDNaaS)	Add-On	Add-On	Add-On

Diferencias de protección contra bots



radware	Basic Bot (Standard & Advanced)	Bot Manager (Complete)
Protección basada en firmas*	✓	✓
CAPTCHA	✓	✓
Basado en el aprendizaje	X	✓
Análiticas de Bots	X	✓
Respuesta del bot malo/legítimo (Configuración de respuesta de generaciones)	X	✓
Respuesta de diferente tipo (Cryptochallenge, Alimentar datos falsos, Bucle de redireccionamiento, Resp. personalizada)	X	✓
Protección del comportamiento (JS Challenge, Detección de granja CAPTCHA)	X	✓
SDK móvil	X	✓

*Solo se aplican algunas configuraciones dentro de **Anomalía del agente de usuario, Anomalía del encabezado y Anomalía de identidad.**

Balanceador de carga como servicio

radware	Failover	Básico	Avanzado
Conmutación por error (Active-Passive) (Failover)	✓	✓	✓
Número de servidores reales activos (origins)	**1**	**8**	**8**
Soporte multipuerto	X	✓	✓
Active-Active	X	✓	✓
Balanceo por Round Robin	X	✓	✓
Persistencia basada en IP	X	✓	✓
Balanceo de carga basado en URL	X	X	✓
Balanceo de carga activo-activo: menor conexiones	X	X	✓
Persistencia basada en cookies	X	X	✓

Revisión de Servicio

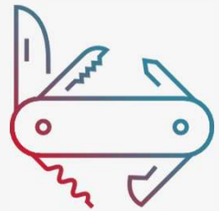
Plan: Advanced

Proxy Anónimo

Bloquea solicitudes que se originen en proxys anónimos, incluyendo el tráfico proveniente de nodos de salida TOR, con el fin de evitar la ocultación de la identidad real del cliente.

Protección basada en firmas

Comprueba el tráfico entrante en busca de patrones y combinaciones de vulnerabilidades conocidas, como inyecciones de código, XSS, y más.



Protección a inyección SQL

Evalúa los parámetros de la solicitud en busca de sintaxis de comandos SQL dañinas, ataques command Shell, XSS, para detenerlos.

Reportería y Analítica

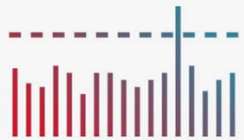
Analítica avanzada y reportería en tiempo real para monitorear tráfico, ataques y rendimiento con dashboards e informes personalizados a cada aplicación.

Revisión de Servicio

Plan: Advanced

Geobloqueo

Permite restringir o permitir tráfico según la ubicación geográfica de las IPs, reforzando la seguridad y el cumplimiento.



Límite de tasa (Rate Limit)

Limita automáticamente el número de solicitudes que una IP puede realizar en un período corto, bloqueando comportamientos abusivos o automatizados.

Control de Acceso

Permite o bloquea el acceso a las aplicaciones en función de direcciones IP o rangos IP definidos, bloqueando solicitudes no deseadas antes del análisis profundo.

Protección a las APIs

Protege tus APIs detectando y bloqueando ataques como abuso, inyecciones y scraping, con visibilidad total y control granular sobre cada endpoint.

Revisión de Servicio

Plan: Advanced

EAAF

Lista dinámica de IPs involucradas en ataques activos a nivel global, permitiendo el bloqueo automático a fuentes de alto riesgo mediante inteligencia en tiempo real recopilada por el ERT.

Source Blocking

Bloquea temporalmente las IPs que intentan realizar actividades maliciosas de forma repetitiva, evitando que accedan a las aplicaciones protegidas.

Path Access Protection

Permite únicamente solicitudes hacia URLs autorizadas, bloqueando el acceso a rutas no definidas.

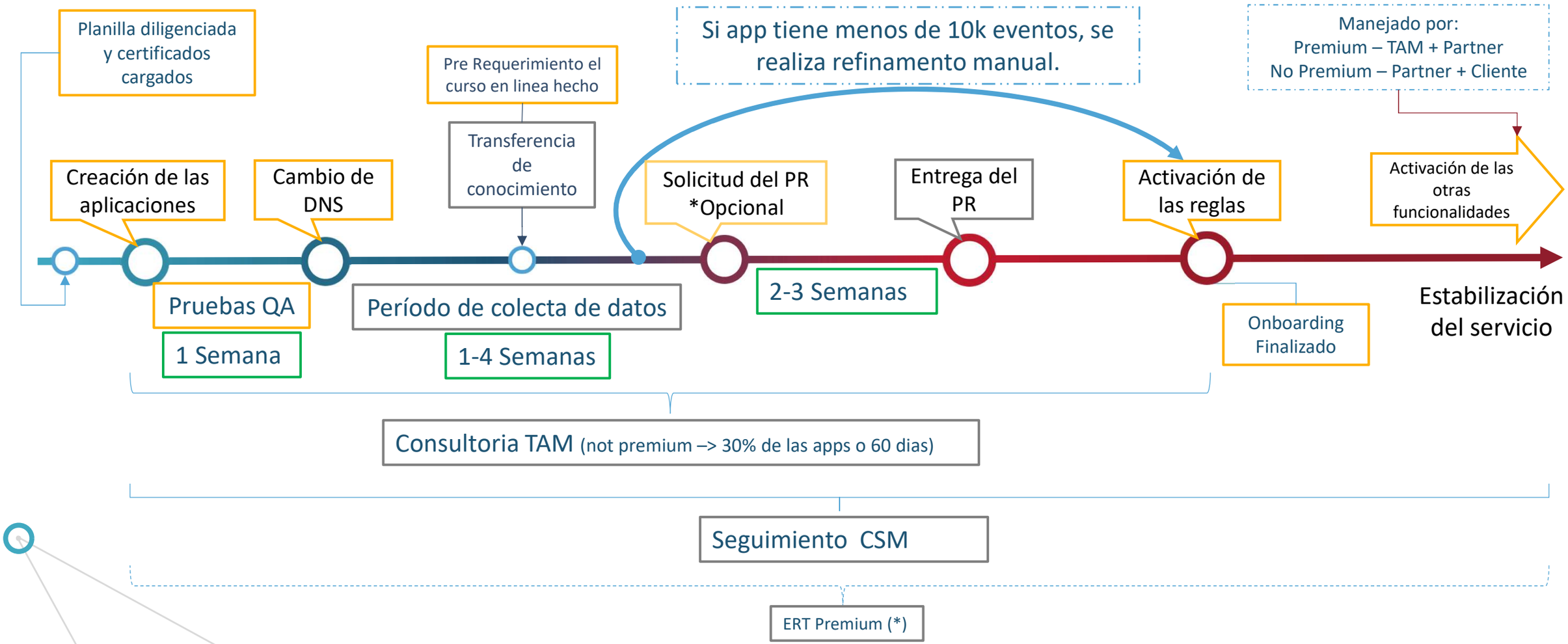
Client-Side Detection

Detecta manipulación de scripts en el navegador para proteger contra ataques como skimming, Magecart e inyecciones de terceros.

Fases del Onboarding – CWAF

Modo Inline – Complete | Advanced

Customer/Partner
Radware



radware

Información importante

Links importantes a tener en cuenta

StatusPage

1

https://cwaf.status.radwarecloud.com/

Entrenamientos

2

https://www.radware.com/training/

Radware Link

3

https://radware.customershome.com/home

Acceso a Soporte

4

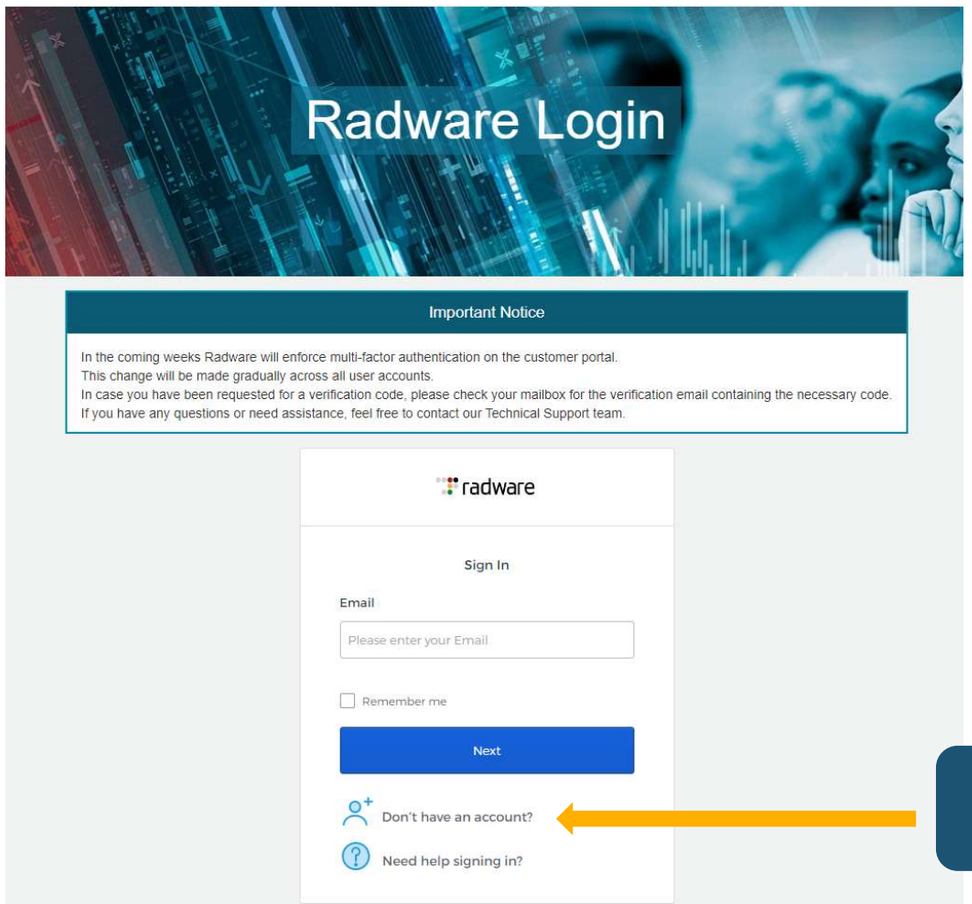
https://support.radware.com/

Cómo puedo crear mi acceso si no tengo Usuario en Cloud Services?

1

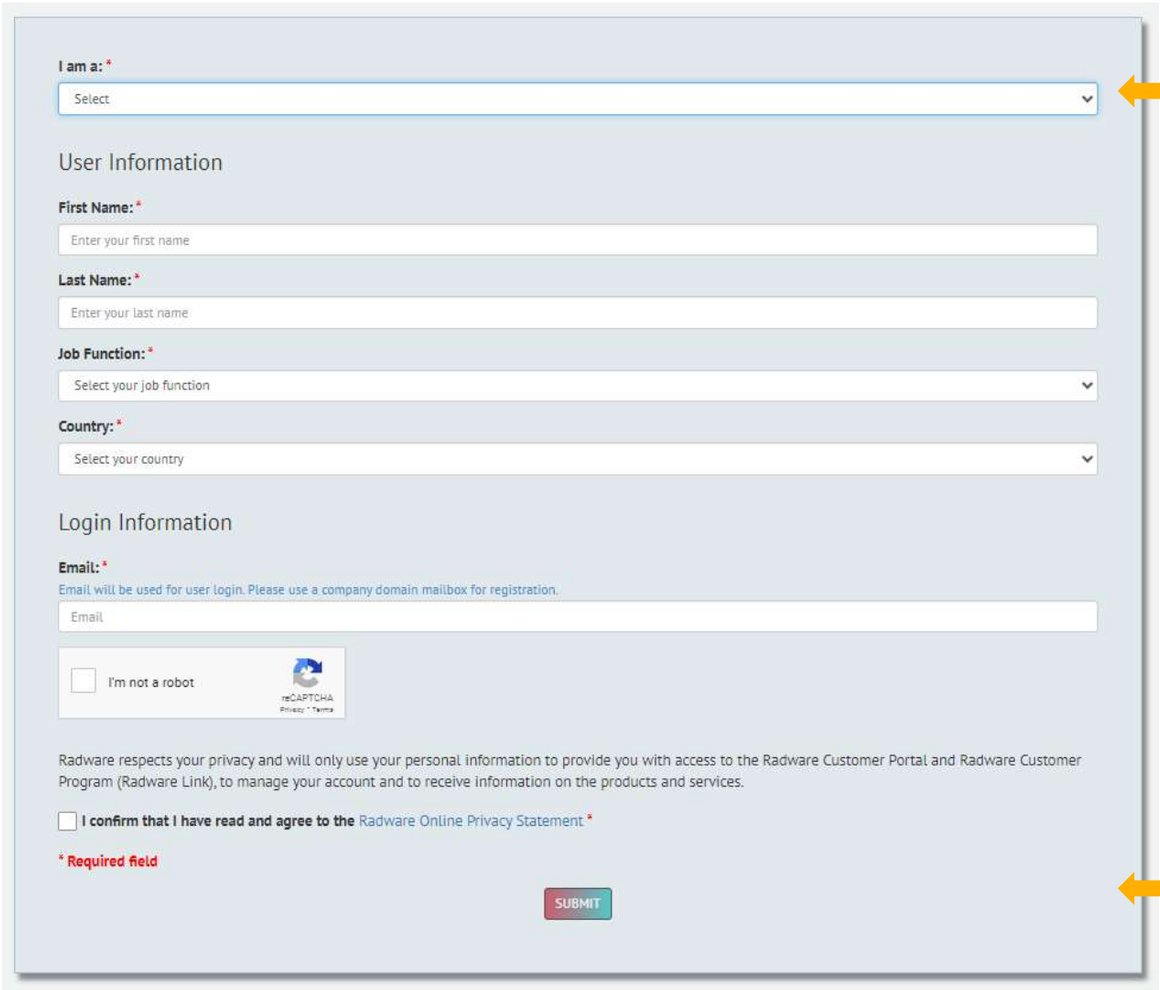
Ingresa a la URL

https://portals.radware.com/Not-Logged-In/Combined-Registration-Form/



Cómo puedo crear mi acceso si no tengo Usuario en Cloud Services?

2 Diligencia y envía el Formulario



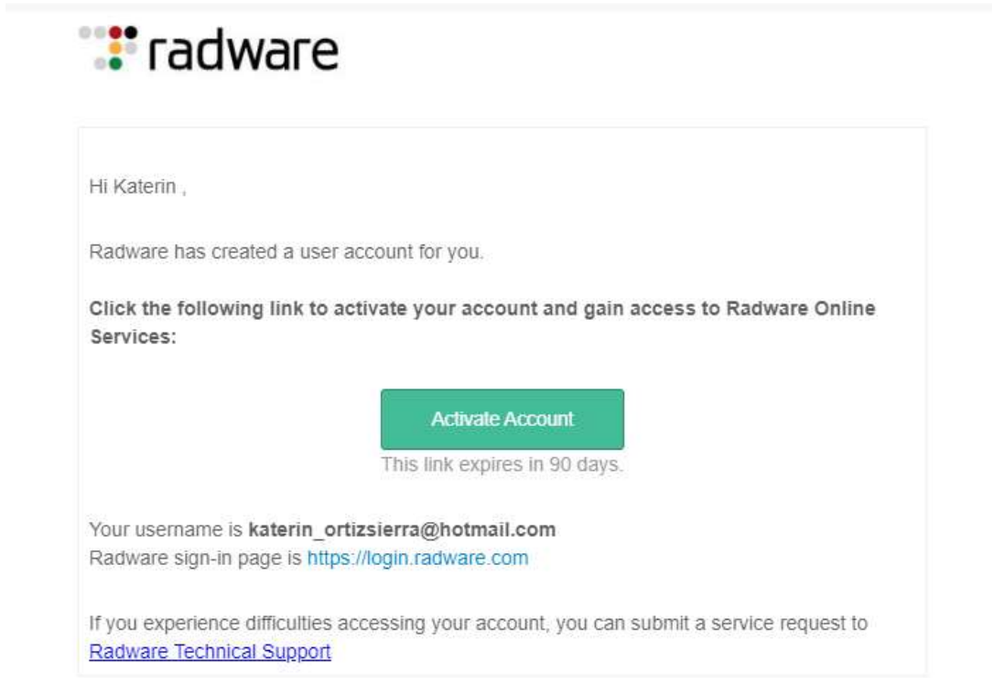
- Selecciona la opción: “Customer”
- Aqui vas a necesitar tener a la mano el SN de uno de tus servicios

Una vez finalices el formulario y des click en “Submit”:

- Customer: tu Usuario será confirmado en un par de horas
- Partner: tomara un par de dias la activación de tu acceso

Cómo puedo crear mi acceso si no tengo Usuario en Cloud Services?

3 Activa tu cuenta y acceder a nuestros servicios



radware

Hi Katerin ,

Radware has created a user account for you.

Click the following link to activate your account and gain access to Radware Online Services:

Activate Account

This link expires in 90 days.

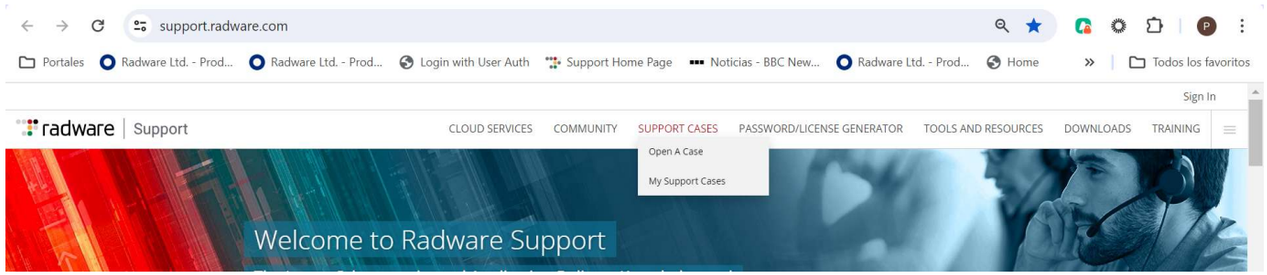
Your username is **katerin_ortizsierra@hotmail.com**
Radware sign-in page is https://login.radware.com

If you experience difficulties accessing your account, you can submit a service request to Radware Technical Support

Ya soy usuario de Cloud Services, qué debo hacer?

Ingresa al botón "Support"

Accede a nuestro contenido



radware

Portal de Soporte

Tiempos de Respuesta Inicial a Casos – Severidad de Casos

Severidad	Tiempo de Respuesta Inicial	Tiempo de Seguimiento	Criterio de Severidad
P1 – Crítico para el negocio	**ERT Premium:** 10 minutos (Llamada)** **Soporte Advanced:** 30 minutos (Llamada)* **Soporte Standard:** 40 minutos (Llamada)*	**ERT Premium:** 24 Horas **Soporte Advanced:** 48 Horas **Soporte Standard:** 48 Horas	**Ataque / Emergencia / Servicio o red caída:** El servicio está completamente fuera de operación y no hay solución alternativa disponible.
P2 – Severidad Alta	**ERT Premium:** 2 Horas **Soporte Advanced:** 4 Horas **Soporte Standard:** 6 Horas	**ERT Premium:** 48 Horas **Soporte Advanced:** 72 Horas **Soporte Standard:** 96 Horas	**Gran impacto sostenido:** El producto no funciona como fue diseñado.
P3 – Severidad Media	**ERT Premium:** 4 Horas **Soporte Advanced:** 12 Horas **Soporte Standard:** 16 Horas	**ERT Premium:** 72 Horas **Soporte Advanced:** 96 Horas **Soporte Standard:** 120 Horas	**Impacto moderado sostenido:** El producto presenta fallas, pero existe una solución alternativa aceptable.
P4 – Severidad Baja	**ERT Premium:** 12 Horas **Soporte Advanced:** 24 Horas **Soporte Standard:** 24 Horas	**ERT Premium:** 96 Horas **Soporte Advanced:** 120 Horas **Soporte Standard:** 144 Horas	**Impacto menor sostenido:** El producto funciona con limitaciones menores o consultas generales.

**Todos los incidentes críticos P1 deben ser reportados por teléfono y tener el SN a la mano.*

**Los clientes con ERT Premium deben llamar a su línea directa y con su PIN asignado a la mano.

Crear todos los casos en INGLÉS (Todas las solicitudes que estén en un idioma distinto al inglés deben ser traducidas primero, por lo que pueden superar el tiempo de respuesta establecido.)

Equipos de Soporte de Radware

Equipo	Nombre Completo	Responsabilidad Principal	Tipo de Soporte	Comentarios
ERT SOC	Emergency Response Team – Security Operations Center	Monitoreo 24/7 de seguridad, análisis de alertas, gestión de incidentes críticos.	Seguridad (SOC)	Primeros en responder ante eventos de seguridad. También realizan PR.
TAC	Technical Assistance Center	Soporte técnico general para productos Radware, resolución de fallas técnicas y bugs.	Técnico (Producto / Configuración)	Enfocado en soporte correctivo y preguntas técnicas de configuración.
ERT NOC	Emergency Response Team – Network Operations Center	Monitoreo de disponibilidad y rendimiento, gestión de tráfico y eventos de red.	Red (NOC)	Se enfoca en rendimiento, disponibilidad y problemas en la infraestructura de red.
Bot Manager	Bot Manager Team	Gestión y optimización del módulo de protección contra bots.	Especializado (Bots y tráfico Web)	Ayuda con configuración de políticas, análisis de tráfico y tuning de bots.

Servicios Administrados Incluidos

Administración de certificados

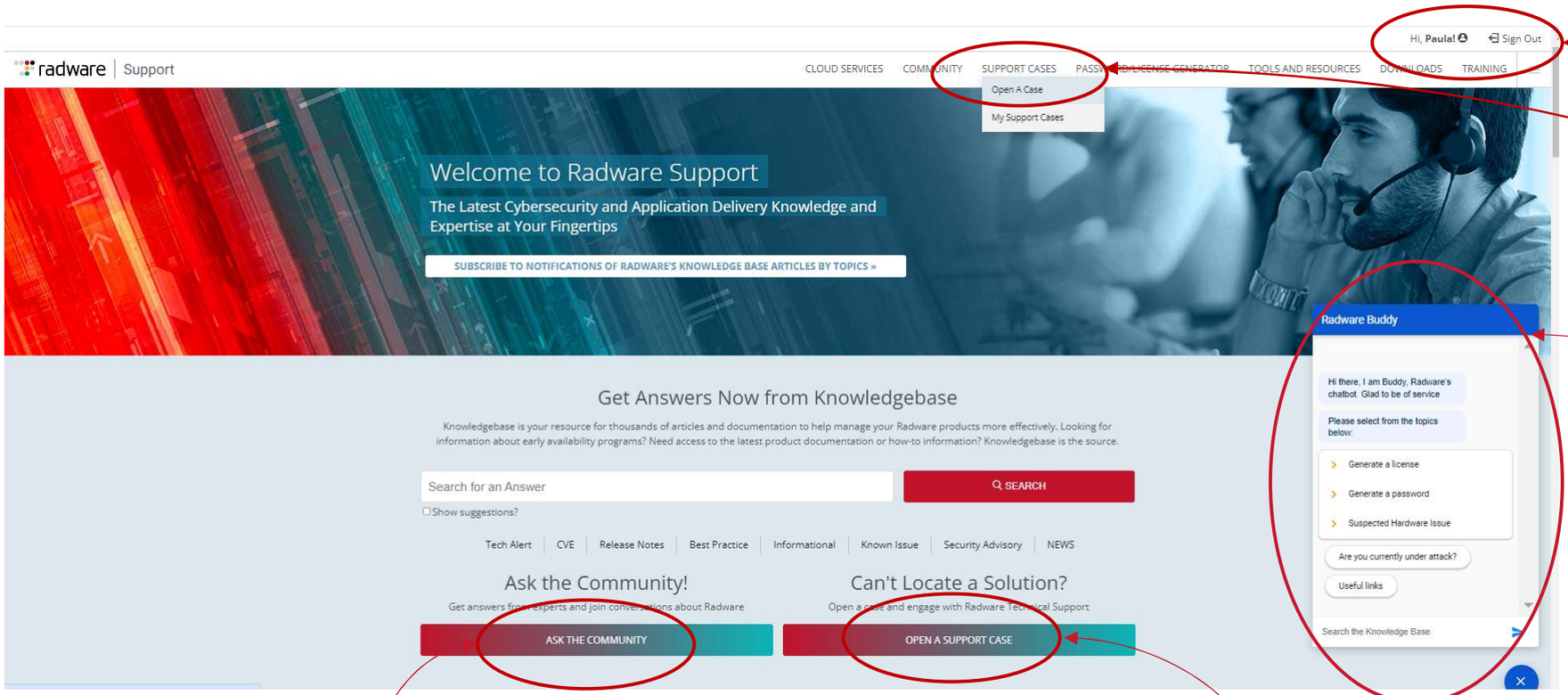
Revisión de Políticas

Análisis Post-Ataque

Soporte por chat

Cómo puedo acceder al Servicio de Soporte?

Cómo puedo acceder al Servicio de Soporte?



1. Ingresa con tus credenciales

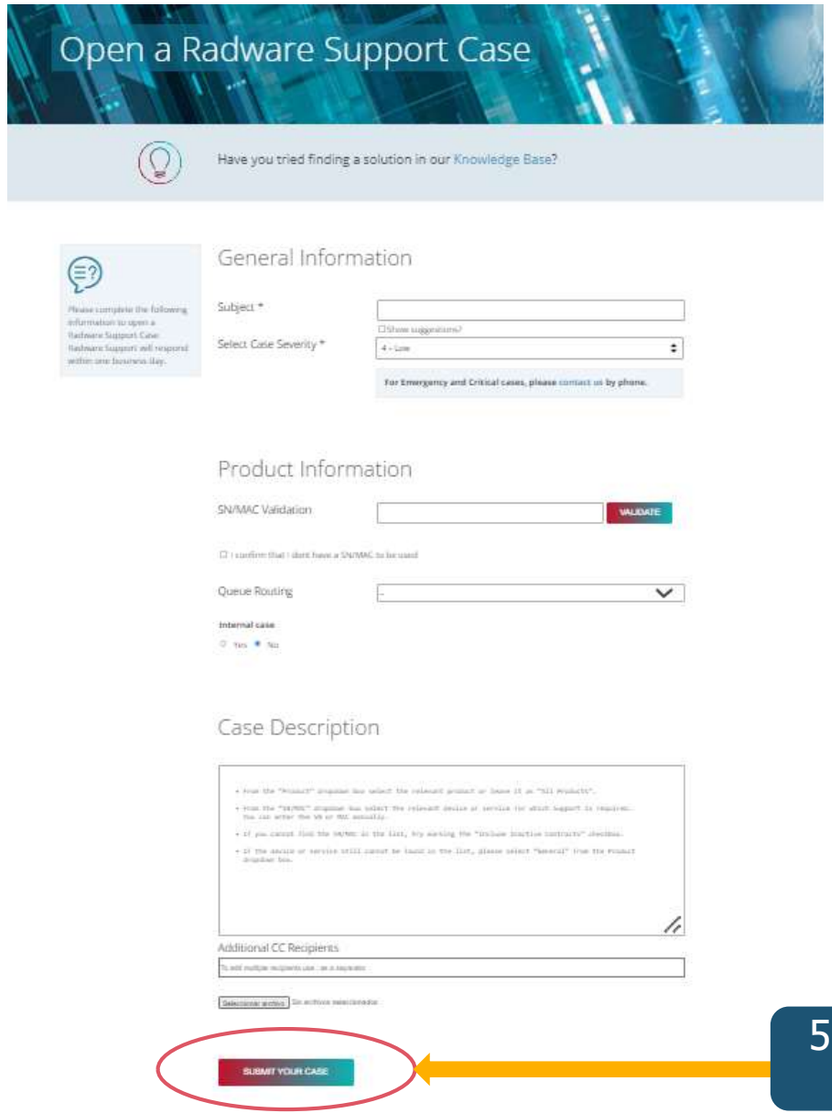
2. Selecciona en: "Open a case"

3. Puedes usar nuestro chatbox para respuestas rápidas y en caso de estar bajo ataque (si tienes soporte Premium)

4. También puedes seleccionar esta opción para crear un ticket

5. Puedes ir a nuestro Radware Link y consultar con nuestra comunidad

Cómo puedo acceder al Servicio de Soporte?



1. Trata de tener precisión al elegir la severidad del caso

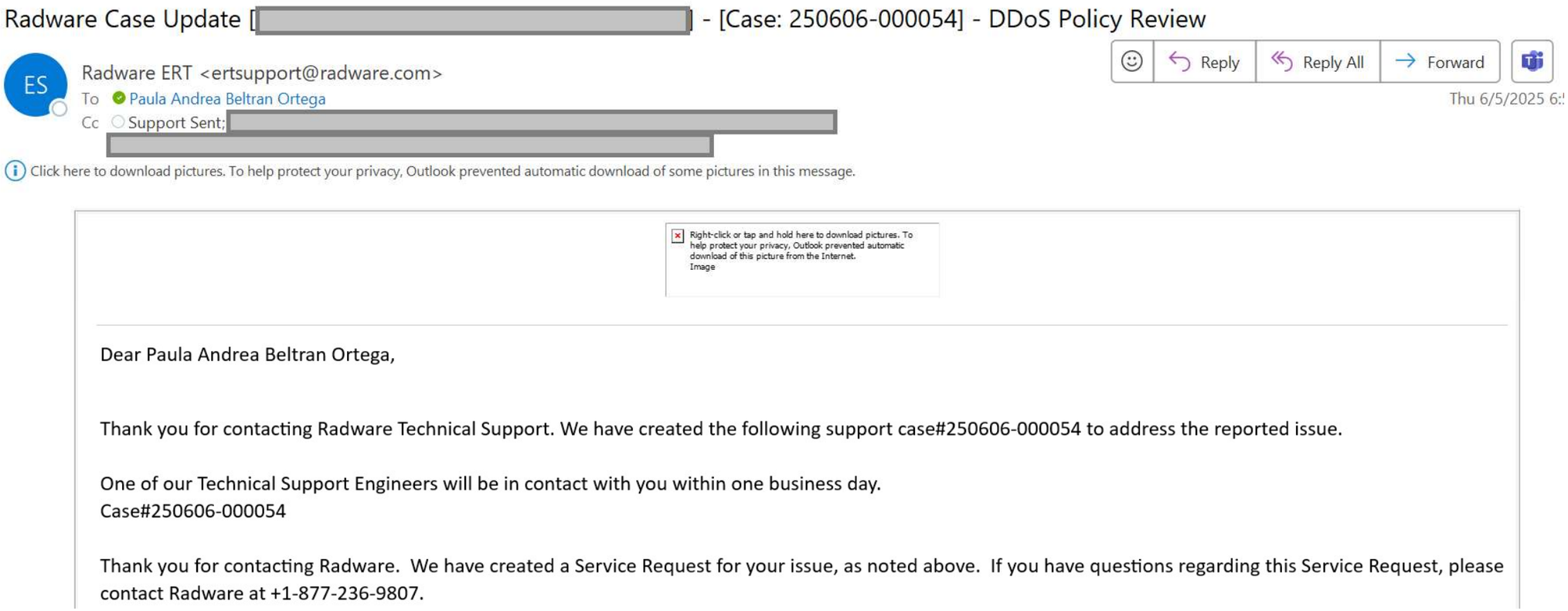
2. Elige el SN del producto relacionado con el caso

3. Detalla tu solicitud (**en inglés**) y adjunta documentación en caso de que lo consideres necesario

4. Puedes incluir correos de personas que quieras mantener al tanto del estatus

5. No olvides dar click en "Submit"

Cómo puedo acceder al Servicio de Soporte?



Radware Case Update [redacted] - [Case: 250606-000054] - DDoS Policy Review

Reply | Reply All | Forward

ES

Radware ERT <ertsupport@radware.com>

To Paula Andrea Beltran Ortega

Cc Support Sent; [redacted]

Thu 6/5/2025 6:

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Right-click or tap and hold here to download pictures. To help protect your privacy, Outlook prevented automatic download of this picture from the Internet.
Image

Dear Paula Andrea Beltran Ortega,

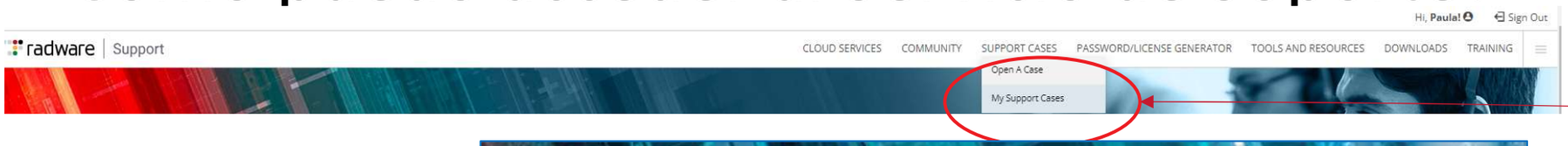
Thank you for contacting Radware Technical Support. We have created the following support case#250606-000054 to address the reported issue.

One of our Technical Support Engineers will be in contact with you within one business day.
Case#250606-000054

Thank you for contacting Radware. We have created a Service Request for your issue, as noted above. If you have questions regarding this Service Request, please contact Radware at +1-877-236-9807.

Recibirás un correo informativo confirmando la creación del caso y con el Número de consecutivo asignado

Cómo puedo acceder al Servicio de Soporte?



Puedes revisar el histórico de tickets y gestionarlos fácilmente

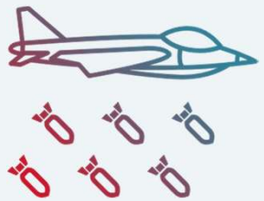
Qué debo tener en cuenta para acceder a Soporte Radware?

Debo crear un Ticket

- A través del portal.
- En **Inglés.**
- Tener presente el **Serial Number.**
- Describir al detalle el alcance de la solicitud.

Caso estándar

- Atención 7x24.
- Sesiones programables en conjunto con el ERT/TAC.
- Posibilidad de atención en español – sujeto a disponibilidad.



Es Urgente?

- Puedo llamar al Hotline.
- **Cliente Advanced!** SLA de atención telefónica de 30 minutos!
- **Cliente Premium!** SLA de atención telefónica de 10 minutos!

Cómo me comunico?

Primary: 1-201-831-8997

Backup: 1-201-749-1200

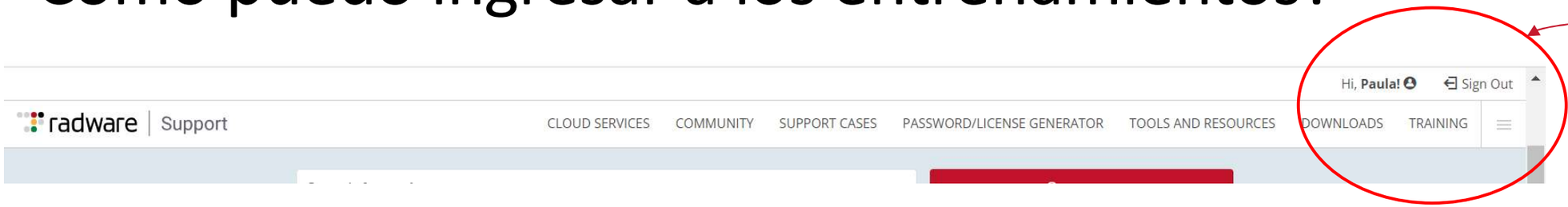
Equipo Cloud

- Escalamiento de tickets o priorización de atención.
- **Reuniones recurrentes.**

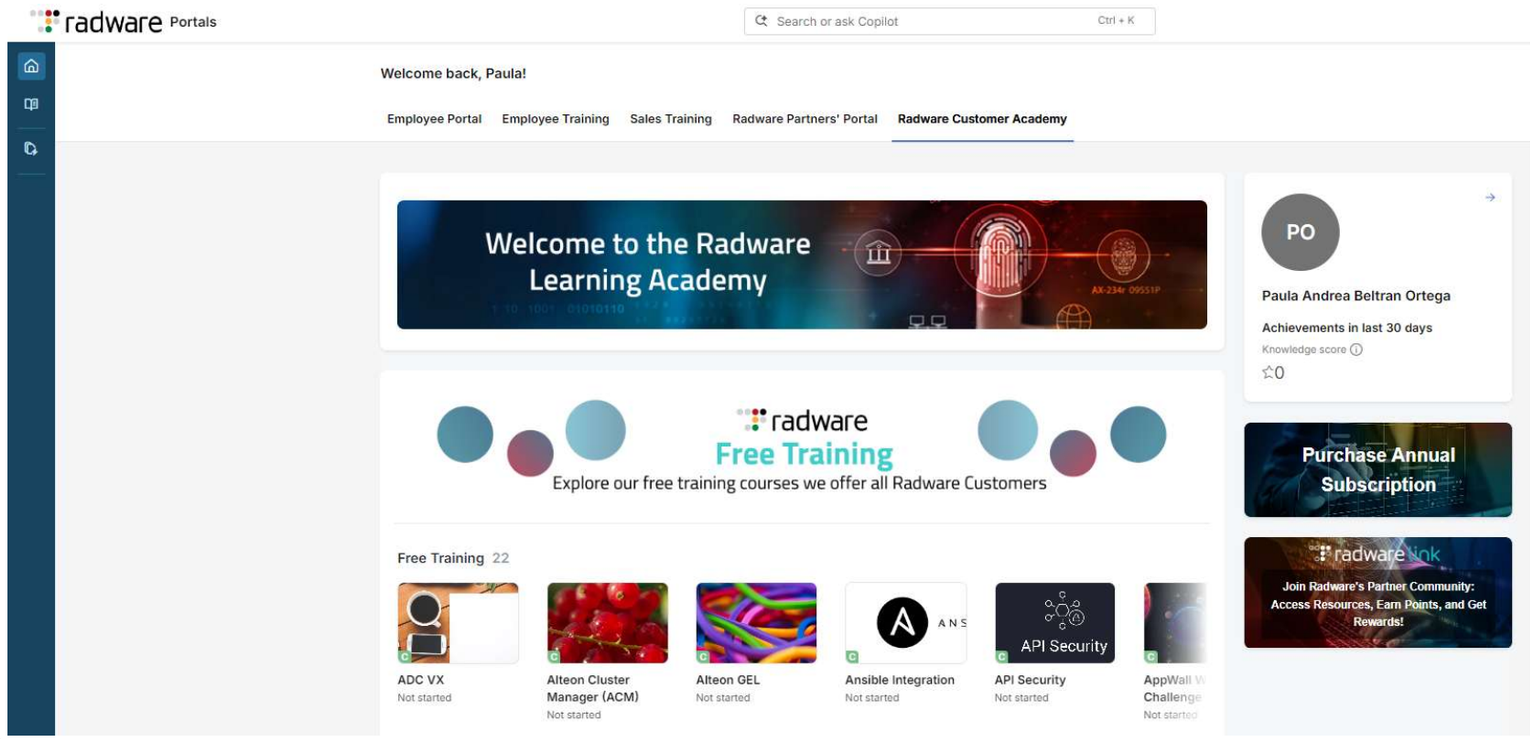
radware

Portal de Entrenamiento

Cómo puedo ingresar a los entrenamientos?

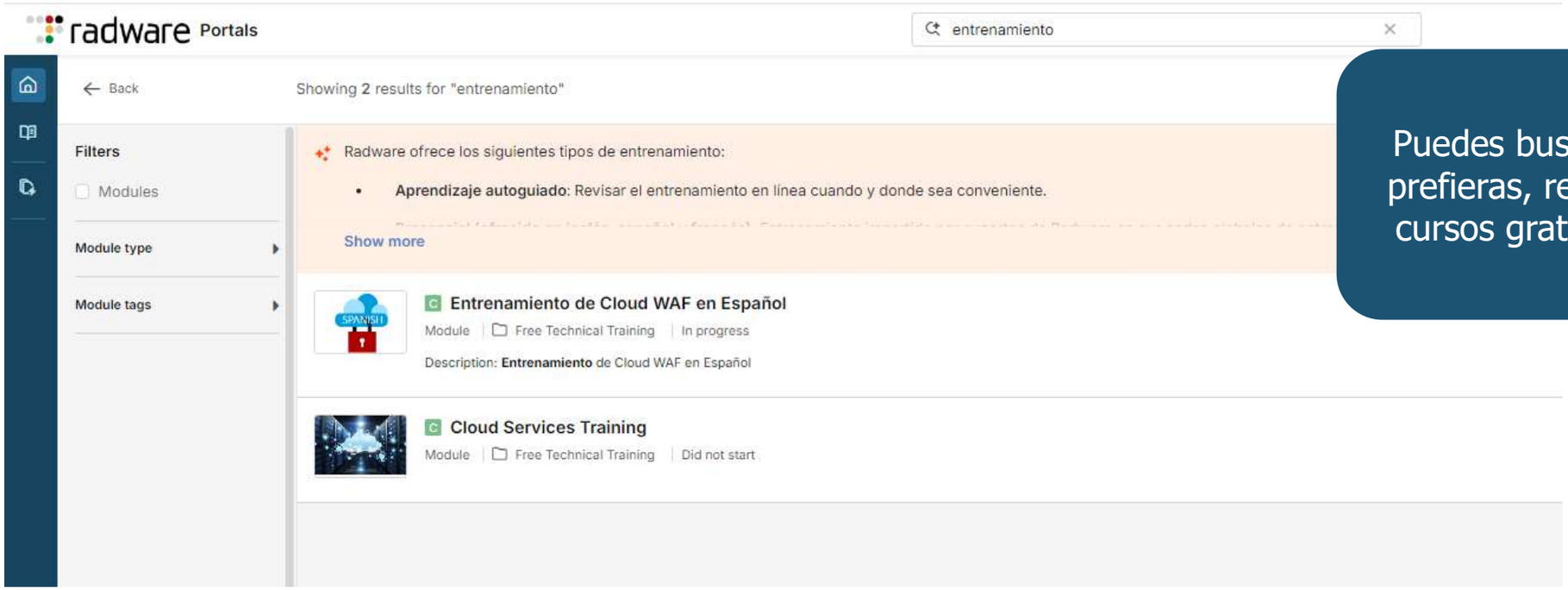


Ingresa con tus credenciales y selecciona la opción “Training”



Usa el buscador o el Menú de la Izquierda

Cómo puedo ingresar a los entrenamientos?



Puedes buscar el contenido que prefieras, recuerda que tenemos cursos gratuitos y cursos pagos

Contenido recomedado CloudWAF en español!

Comienza tu colección de Badges!

Matríz de Escalamiento ERT

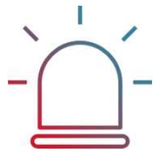
Nivel de Escalamiento	Punto de contacto	Detalles del Contacto
1	Customer Success Manager	kendry.muro@radware.com paulab@radware.com
2	ERT Managers	ertmanagers@radware.com
3	**Yarden Nachum** ERT Manager (Israel) **Matar Weiss** ERT Manager (APAC & EMEA)	yardenn@radware.com matarw@radware.com
4	**Albie Sternberg** Regional Delivery Manager (Americas) **Amir Paluch** Cloud Services NOC Manager **Ilan Meller** Group Manager, Cloud Security Services	albie.sternberg@radware.com amirpa@radware.com ilanm@radware.com
5	**Yaniv Raz** Director, Cloud Delivery	yanivra@radware.com
6	**Koby Danon** VP, Cloud Services	kobyd@radware.com

Soluciones de Radware

INFRAESTRUCTURA
(Network)

PROTECCIÓN SUPERIOR

Protección conductual contra inundaciones



Firmas automatizadas en tiempo real

BALANCEO DE CARGAS
(Data Center / ADC)

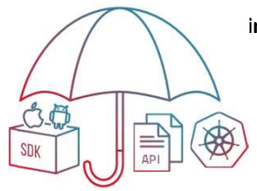
Gestiona y optimiza la entrega de tráfico a través de redes

Servidores Aplicaciones Enlaces

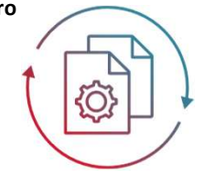
SEGURIDAD DE APPS
(Capa Aplicativa / L7)

PROTECCIÓN AGNOSTICA

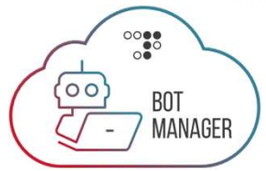
La mejor protección de la industria y el menor número de falsos positivos

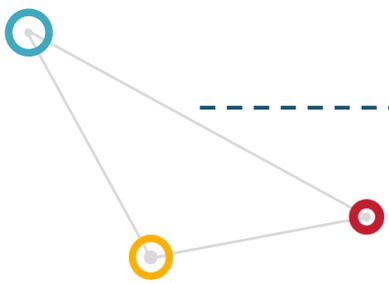


Diseñado para proteger en múltiples entornos



Generación de políticas automáticas para una mínima intervención humana





Protección Unificada desde la red hasta la lógica de negocio

¡MUCHAS GRACIAS!

radware

“Cada Segundo Cuenta."

Bitdefender® Partner Advantage Network

License Certificate

Order Number: 1325899

Date (yyyy-mm-dd): 2025-12-17

End User Details

Company Name: Instituto de Deportes y Recreación de Medellín

Contact person: Harrison Alexander Hernandez Rua

E-mail Address: harrison.hernandez@inder.gov.co

Address: Cl. 47D #75-276, MEDELLIN, zipcode 0000

Telephone No: 3699000

Reseller Details

Name: Star Solutions TI SAS

E-mail Address: certificados@star-ti.com

Address: Carrera 27 49-19, Bogota, zipcode 000

Contact Person: Jorge Enrique Molano

Distributor Code: P-00004815

Solution / SKU: Bitdefender GravityZone Patch Management

Protected Devices / Devices Number: 1020

Purchase Date (yyyy-mm-dd): 2025-12-17

Validity Period: 12 months

License Key(s): B7UNV356ZPCC

Total devices: 1020

Solution / SKU: Bitdefender GravityZone Business Security Enterprise (Ultra)

Protected Devices / Devices Number: 1020

Purchase Date (yyyy-mm-dd): 2025-12-17

Validity Period: 12 months

License Key(s): QB3NRFR53RUU

Total devices: 1020

ACUERDOS DE NIVELES DE SERVICIO

Niveles de atención y soporte a clientes finales

STAR SOLUTIONS. T.I.

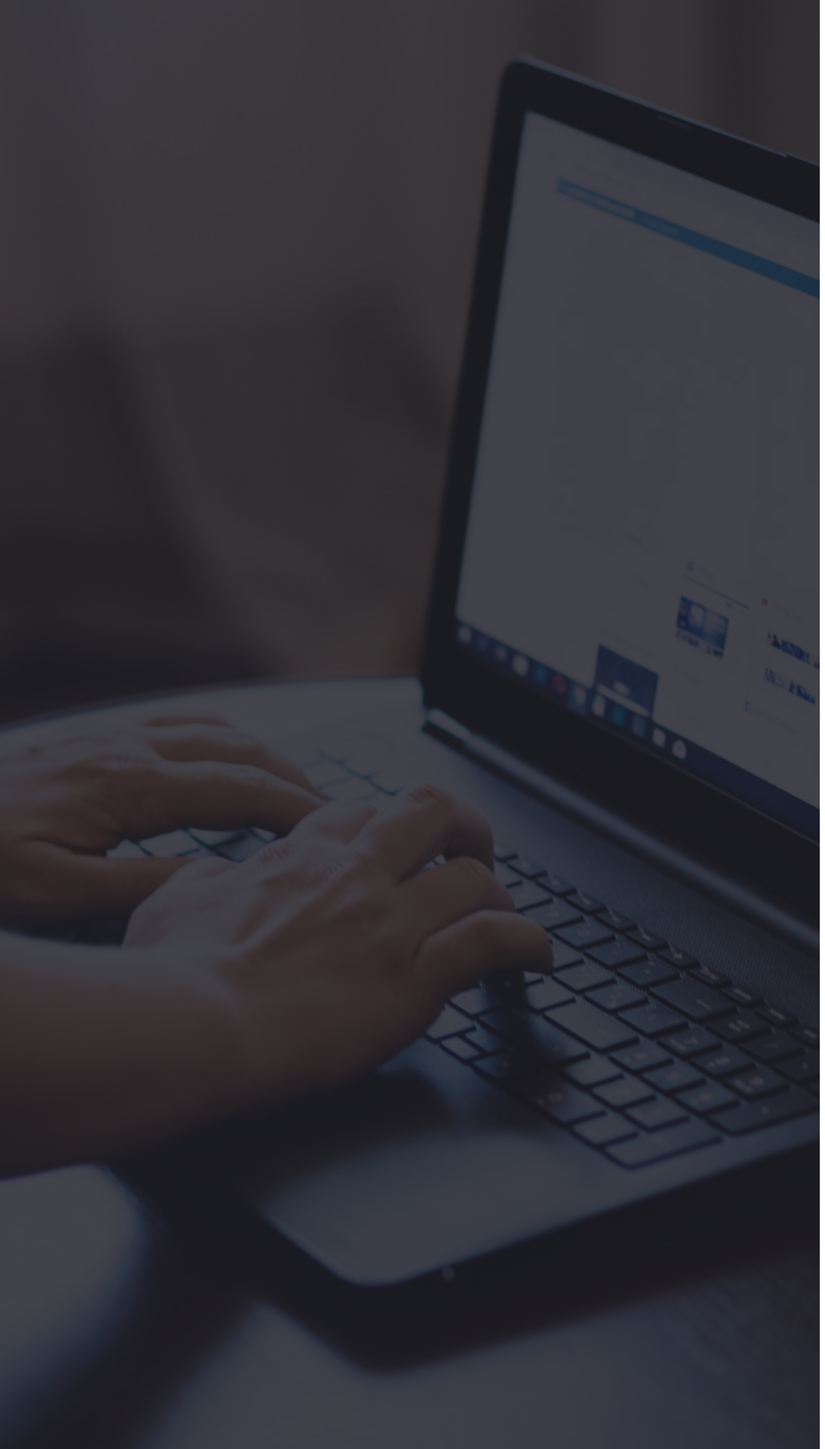
LO SIMPLE FUNCIONA

OBJETIVO

- GESTIONAR LOS INCIDENTES DE LA MANERA MÁS RÁPIDA Y EFICAZ POSIBLE A CUALQUIER INCIDENTE QUE CAUSE UNA INTERRUPCIÓN EN EL SERVICIO.

BENEFICIOS

- MEJORA LA SATISFACCIÓN DE CLIENTES Y USUARIOS.
- MEJORAR LA PRODUCTIVIDAD DE LOS USUARIOS.
- CUMPLIMIENTO DE LOS NIVELES E SERVICIO ACORDADOS EN EL ANS
- MAYOR CONTROL DE LOS PROCESOS Y MONITORIZACIN DEL SERVICIO.
- OPTIMIZACIÓN DE LOS RECURSOS DISPONIBLES.



ESCALAMIENTO

El servicio de soporte cuenta con 3 niveles de escalamiento con el objetivo de brindar soluciones oportunas y adecuadas al nivel de complejidad del requerimiento

Nivel 1

STAR SOLUTIONS TI

Nivel 2

COUNTRY PARTNER

Nivel 3

FABRICANTE

CLASIFICACION DE INCIDENTES

Categorias de servicio

clasificación de incidentes		Impacto		
		bajo	medio	alto
Prioridad	bajo	Informativo (requerimiento)	Medio (requerimiento)	Medio (requerimiento)
	medio	Medio (requerimiento)	Alto (incidente)	Alto (incidente)
	alto	Medio (requerimiento)	Alto (incidente)	Critico (incidente)

Nivel de prioridad

- **Baja**: Cuando un incidente no afecta los procesos directamente
- **Media**: Cuando el incidente afecta las operaciones y el servicio trabaja con dificultad
- **Alta:** Cuando un incidente afecta las operaciones del negocio directa y significativamente

Nivel de impacto

- **Bajo**: Cuando el impacto es básico y no afecta las funciones de la organización
- **Medio**: Cuando el impacto es moderado y limita únicamente las funciones del negocio.
- **Alto:** Cuando afecta el negocio o el impacto es significativo en alguna de las funciones del negocio

ACUERDOS DE SERVICIO

Nivel 3
FABRICANTE

Nivel 2
COUNTRY PARTNER

Nivel 1
STAR SOLUTIONS TI

ACUERDOS DE NIVELES DE SERVICIO (ANS)						
Tipo de soporte		Nivel	Descripción	Canal	Tiempos	Disponibilidad
Técnico / tecnólogo	1	Informativo	Consultas a nivel informativo sobre caracterizas o funciones de la solución	Star Solutions TI / Guía de administración /guía de instalación / base de datos de conocimientos web	**Respuesta 1-2-horas** **Solucion 2-4-horas**	Lunes a Viernes 8 AM – 5 PM Telefónico Remoto presencial
	2	Medio	Incidentes menores que requieran la asesoría y/o soporte en relación con EndPoint	Star Solutions ti	**Respuesta 1-2-horas** **Solucion 2-4-horas**	
Ingeniería Especialista	3	Alto	Incidentes que requieran la asesoría y/o soportes derivados de la administración y o configuración de la consola Cloud		**Respuesta 1-2-horas** **Solucion 2-4-horas**	Lunes a Viernes 8 AM – 5 PM Telefónico Remoto presencial
	4	Critico	Incidentes que afecten de manera critica la continuidad en las operaciones y requieran soporte inmediato por parte de Star Solutions y/o fabricante	Star Solutions ti / fabricante	**Respuesta 1-2-horas** **Solucion 2-4-horas**	

Nivel 2
COUNTRY PARTNER

Nivel 3
FABRICANTE

CONDICIONES DE ESCALAMIENTO

Una vez agotadas las alternativas de soporte por parte de Star solutions ti, se procedera a escalar el requerimiento a nivel 2 o nivel 3 dependiendo del criticidad del requerimiento

Para agilizar el proceso de respuesta por parte de soporte, le pedimos el favor de apoyarnos conla siguiente información y enviárnosla de vuelta:

Nombre de Empresa:

Nombre del Ingeniero:

Cliente Final: (En caso de ser cliente final el primer contacto es su Partner o Distribuidor)

Numero de Contacto:

Correcto Electrónico:

País:

Ciudad:

Producto con problemas (Ej.: Bitdefender)

Tipo de Licenciamiento: (Ej. Business, Elite, Ultra, Enterprise, etc.)

Versión del producto: (Ej. 7.0.0.1)

Producto Cloud Nube u On Premise Físico:

Sistema Operativo: (Ej. Win 7, Server)

Pasos para reproducir el error y materiales que lo soporten: (Ej. Abrir la aplicación con problemas desde el menú inicio)

Situación Actual: (Ej.: la aplicación no se ejecuta)

Resultados esperados: (Ej.: la página web se muestre normalmente)

Información adicional: (ScreenShots, Logs de Servidor o Bdsyslogs, Registros y demás)

Para productos Bitdefender es necesario tener esta información:

•BdSys Tool en casos de sospecha de infección

Nivel 1

STAR SOLUTIONS TI

CANALES DE ATENCION

helpdesk@soporte.star-ti.com
7x24@soporte.star-ti.com

300 7010017linea unica de soporte

soporte.star-ti.com

https://helpdesk.star-ti.com/


STAR SOLUTIONS. T.I.
LO SIMPLE FUNCIONA

INFORME TÉCNICO DE IMPLEMENTACIÓN Y CUMPLIMIENTO DE OBLIGACIONES - INDER MEDELLÍN

FECHA: 16 de diciembre de 2025

CLIENTE: Instituto de Deportes y Recreación de Medellín - INDER

CONTRATO: Suministro No. 6700045132 de 2025

SOLUCIONES: Bitdefender GravityZone Enterprise, HornetSecurity, Radware WAF.

1. RESUMEN EJECUTIVO

El presente informe consolida el despliegue tecnológico y el cumplimiento administrativo del contrato de seguridad informática para el **INDER**. El proyecto integró la protección de estaciones de trabajo y servidores mediante **Bitdefender GravityZone Business Security Enterprise**, la gestión avanzada de seguridad de correo con **HornetSecurity** y la defensa de aplicaciones críticas en la nube mediante **Radware WAF** (compatible con Azure).

Se detalla no solo la fase técnica de instalación, sino también la ejecución de las obligaciones contractuales, garantizando que la infraestructura del INDER en la región **East US 2** opere bajo estándares de alta disponibilidad, con monitoreo integrado a **Microsoft Sentinel** y un esquema de capacitación técnica de 30 horas.

2. Objeto

Adquirir como servicio las soluciones de Antivirus, Antispam y Firewall de Aplicaciones Web (WAF) para la protección de la infraestructura tecnológica del **INDER Medellín**, incluyendo la configuración, el soporte técnico especializado y la transferencia de conocimiento al personal del instituto.

3. Alcance

El licenciamiento adquirido cubre las siguientes protecciones y cantidades.

Ítem	Descripción del producto	Cantidad / usuarios	vigencia
1	ANTIVIRUS – ENDPOINT	1020	12 meses
2	ANTISPAM	1400	12 meses
3	WAF	1	12 meses

VIGENCIA DE LICENCIAMIENTO

Las soluciones fueron activadas de acuerdo con el cronograma del anexo técnico:

Componente	Fabricante / Solución	Inicio Vigencia	Fin Vigencia
Antivirus (EDR/XDR)	Bitdefender GravityZone	25/11/2025	24/11/2026
Antispam (ATP)	HornetSecurity	25/11/2025	24/11/2026
WAF (Cloud-Native)	Radware	30/12/2025	29/12/2026

El alcance abarca la totalidad del ecosistema digital del INDER:

- **Seguridad de Endpoints:** Instalación en todos los activos de cómputo (estaciones y servidores).
- **Seguridad de Aplicaciones:** Protección de los servicios publicados en Azure East US 2.
- **Seguridad de Mensajería:** Filtrado de correo entrante y saliente para el dominio institucional.
- **Evaluación de Seguridad:** Ejecución de pruebas de Ethical Hacking y Pentest.
- **Capacitación:** Plan de 30 horas para el equipo de TI y concienciación para usuarios finales.

4. CUMPLIMIENTO DE OBLIGACIONES DEL CONTRATO

En este apartado se detalla el cumplimiento de las cláusulas establecidas en el Anexo al Contrato y el Anexo Técnico V4, vinculando cada obligación con la acción técnica realizada.

6.1. Obligaciones Generales del Contratista

6.1.1. Ejecución con Calidad y Excelencia:

Cumplimiento: Se aplicaron marcos de trabajo basados en NIST y ISO 27001 para el despliegue de las tres soluciones. La configuración de Bitdefender se realizó bajo el modelo de "Defensa en Profundidad", asegurando que cada módulo (Antimalware, EDR, Firewall) esté optimizado para la red del INDER.

6.1.2. Responsabilidad de Personal y Seguridad Social:

Cumplimiento: Star Solutions TI certifica que todo el personal técnico asignado para la implementación del WAF Radware y la seguridad de correo cuenta con el pago de aportes parafiscales y seguridad social al día, conforme a la Cláusula Vigésima Séptima del contrato.

6.1.3. Confidencialidad y Manejo de Datos:

Cumplimiento: Dada la sensibilidad de la información del INDER, se establecieron protocolos de acceso restringido a las consolas de administración.

6.1.4. Cumplimiento Normativo y Legal:

Cumplimiento: El software suministrado cuenta con licenciamiento original y vigente a nombre del Instituto de Deportes y Recreación de Medellín - INDER, garantizando la legalidad del producto ante cualquier auditoría.

6.2. Obligaciones Específicas del Anexo Técnico

Obligación 1: Suministro de Licenciamiento (Antivirus, Antispam y WAF).

Acción de Cumplimiento: Se entregaron las llaves de activación y accesos a las consolas cloud.

Bitdefender: Licencia Enterprise con EDR.

HornetSecurity: Licencia ATP (Advanced Threat Protection).

Radware: Licencia WAF optimizada para Azure East US 2.

Obligación 2: Instalación y Configuración Técnica.

Acción de Cumplimiento: Se realizó la instalación de los agentes de Bitdefender en el parque computacional. Para el WAF de Radware, se configuró el túnel y el mapeo de aplicaciones dentro del Application

Gateway V2 de Azure, asegurando el rendimiento de 1 MB/s y las 1000 conexiones persistentes solicitadas.

Obligación 3: Integración con SIEM Sentinel.

Acción de Cumplimiento: Se garantiza el flujo de datos para que los registros de análisis de Radware WAF se ingesten diariamente en Microsoft Sentinel.

Volumen: Se garantizó la capacidad de 2 GB de registros de análisis por día.

Retención: Se configuraron 3 meses de retención de datos en Azure Monitor, según lo exigido en el Anexo V4.

Obligación 4: Parametrización según Políticas del INDER.

Acción de Cumplimiento: No se realizó una instalación "por defecto". Se crearon políticas de:

Exclusiones de software misional en Bitdefender para no afectar la operación de los escenarios deportivos.

Reglas de filtrado MX y SPF en HornetSecurity para el dominio @inder.gov.co.

Mitigación de ataques de denegación de servicio (DDoS) en Radware.

Obligación 5: Capacitación al Personal Técnico (Máximo 3 Ingenieros).

Acción de Cumplimiento: Se impartieron 30 horas de capacitación técnica de alto nivel. Los ingenieros del INDER fueron certificados internamente por Star Solutions en el manejo de las consolas, gestión de incidentes y remediación de amenazas. Se entregaron tarjetas profesionales y certificados de fabricante del personal docente según requerimiento.

Obligación 6: Prueba de Acceso No Autorizado (Pentest) y Ethical Hacking.

Acción de Cumplimiento: Se ejecutará una prueba de penetración una sola vez durante la vigencia. Se simularán ataques de inyección SQL y Cross-Site Scripting (XSS) contra los portales del INDER, verificando que el WAF Radware detectara y bloqueara el 100% de los intentos de explotación del Top 10 de OWASP.

Obligación 7: Concienciación en Ciberseguridad para Usuarios Finales.

Acción de Cumplimiento: Se realizará un webinar masivo para los funcionarios del INDER, donde se explicarán los riesgos de la ingeniería social y cómo la herramienta HornetSecurity ayuda a identificar correos sospechosos antes de interactuar con ellos por parte del oficial de seguridad de Star Solutions ti.

6.3. CUMPLIMIENTO DE OBLIGACIONES GENERALES (CLÁUSULAS CONTRACTUALES)

6.3.1. Calidad del Servicio:

- Evidencia: Las soluciones implementadas (Bitdefender, HornetSecurity y Radware) son líderes en el Cuadrante Mágico de Gartner, asegurando que el INDER cuente con tecnología de punta. El despliegue se realizó sin afectar la disponibilidad de los servicios ciudadanos.

6.3.2. Personal Técnico Calificado:

- Evidencia: Se adjuntaron las tarjetas profesionales de los ingenieros de Star Solutions y sus certificaciones de fabricante:
  - *Bitdefender Certified Professional.*
  - *Radware Cloud WAF Specialist.*
  - *HornetSecurity Certified Engineer.*

6.3.3. Pago de Seguridad Social y Parafiscales:

- Evidencia: Se anexan al presente informe las planillas PILA de los meses de ejecución, certificando que el personal asignado al INDER está al día con sus obligaciones legales.

6.3.4. Confidencialidad y Seguridad de la Información:

- Evidencia: Se implementó el protocolo de "Cero Confianza" (Zero Trust). El acceso a la consola de Radware WAF y Bitdefender está restringido por IPs específicas del INDER y requiere autenticación multifactor (MFA), cumpliendo con la protección de datos del instituto.

7. ACTIVIDADES REALIZADAS PARA LA IMPLEMENTACION DE LAS HERRAMIENTAS.

7.1. Implementación Bitdefender GravityZone Business Security Enterprise

Esta fase se dividió en la preparación del entorno cloud y el despliegue en la infraestructura física y virtual del INDER.

7.1.1. Configuración de Consola Control Center

- Activación de la instancia en la nube y configuración de la estructura de red: Sedes administrativas, escenarios deportivos y centros de datos.
- Configuración de la autenticación multifactor (MFA) para el acceso administrativo.

7.1.2. Creación de Paquetes de Instalación Se diseñaron instaladores personalizados con los siguientes módulos activos:

- Advanced Threat Control: Monitoreo activo de procesos.

- EDR (Endpoint Detection and Response): Para visibilidad total del árbol de ataque.
- Análisis de Riesgos: Evaluación de configuraciones del SO y aplicaciones vulnerables.

7.1.3. Despliegue de Agentes

- Despliegue masivo mediante herramientas de distribución y scripts de instalación silenciosa en equipos Windows.
- implementación manual en sitio realizada por personal técnico certificado en la herramienta
- Verificación de comunicación bidireccional entre los Endpoints y la consola GravityZone.

7.1.4. Definición de Políticas de Seguridad

- Políticas de Escaneo: Programación de análisis completos semanales y análisis rápidos diarios.
- Exclusiones: Configuración de exclusiones técnicas para bases de datos SQL y software misional del INDER.
- Control de Dispositivos: Restricción de medios extraíbles no autorizados para prevenir fuga de datos.

7.2. Implementación de Protección de Correo (HornetSecurity)

Se sustituyó la protección anterior por la suite avanzada de HornetSecurity para mitigar ataques dirigidos.

7.2.1. Configuración de Dominios y Registros DNS

- Registros MX: Redireccionamiento del flujo de correo hacia los Smart hosts de HornetSecurity.
- SPF/DKIM/DMARC: Configuración de registros para validar la reputación del dominio @inder.gov.co y evitar el spoofing.

7.2.2. Parametrización de Módulos de Filtrado

- ATP (Advanced Threat Protection): Activación de Sandboxing para archivos adjuntos sospechosos.
- URL Rewriting: Escaneo de enlaces en tiempo real al momento del clic del usuario.
- Gestión de Cuarentena: Configuración de reportes de spam diarios para los funcionarios.

7.3. Implementación de Radware WAF (Web Application Firewall)

7.3.1. Arquitectura y Provisionamiento en Azure

- Configuración en la región East US 2.
- Ajuste de capacidad: 730 horas de gateway, 5 unidades de proceso y soporte para transferencia de 2 TB mensuales.
- Integración con el Application Gateway V2 institucional.

7.3.2. Políticas de Protección WAF

- Implementación de reglas contra el Top 10 de OWASP (Inyecciones, XSS, etc.).
- Configuración de perfiles de protección contra ataques DoS/DDoS en capa 7.
- Gestión de certificados SSL para inspección profunda de tráfico HTTPS.

7.3.3. Ingesta de Logs en Microsoft Sentinel (SIEM)

- Configuración del conector para el envío de logs de seguridad.
- Garantía de ingesta de 2 GB diarios de registros de análisis según ficha técnica.

8. TRANSFERENCIA DE CONOCIMIENTO Y CAPACITACIÓN

Se realizó una transferencia de conocimiento de **30 horas** (superando las 8h del modelo base) distribuida en las siguientes temáticas:

SESION	**HERRAMIENTA**	**INTENSIDAD HORARIA**
S1: Arquitectura y Gestión de la Consola	Bitdefender	2 horas
S2: Despliegue de Agentes y Hardening Inicial	Bitdefender	2 horas
S3: Políticas de Prevención Antimalware/Ransomware	Bitdefender	2 horas
S4: EDR: Funcionalidades de Investigación	Bitdefender	2 horas
S5: Control de Dispositivos USB	Bitdefender	2 horas
S6: Análisis Forense (Root Cause Analysis)	Bitdefender	2 horas
S7: Integración Total y Continuidad del Email con M365	Hornet	2 horas
S8: Reporting Avanzado e Integración SIEM	Hornet	2 horas
S9: Configuración de Sandboxing y Anti-Phishing	Hornet	2 horas
S10: Explorador de Amenazas y AIR (Investigación)	Hornet	2 horas
S11: Gestión de Simulación de Phishing	Hornet	2 horas
S12: Despliegue de Cloud WAF y Arquitectura en Azure	Radware	2 horas
S13: Reglas OWASP Top 10 y Seguridad de APIs	Radware	2 horas
S14: Control de Bots Maliciosos y DDoS L7	Radware	2 horas
S15: Monitoreo, Dashboard de Reportes y Soporte HTTPS	Radware	2 horas
total		30 oras

9. SOPORTE Y GARANTÍA

- **Atención 24/7:** Soporte técnico telefónico y remoto canales de contacto y matriz de prioridad detallada en los ANS.

- **Actualizaciones:** Acceso garantizado a nuevas versiones de firmas y motores de escaneo durante toda la vigencia.
- **Acompañamiento:** Asistencia técnica en sitio para incidentes de alta prioridad.

10. CONCLUSIÓN

La implementación de las soluciones de seguridad en el **INDER Medellín** se ha completado exitosamente, cumpliendo con la totalidad de los requisitos técnicos del **Anexo V4**. La entidad cuenta ahora con una infraestructura resiliente, monitoreada y protegida bajo los más altos estándares de la industria, asegurando la disponibilidad de sus servicios y la integridad de su información.

Para el cumplimiento de las obligaciones especificas establecidas en el contrato se anexan cartas que ratifican el cumplimiento de cada una de ellas según lo especificado en el contrato.

Elaboro.

Diego Felipe Vasquez
líder de proyectos
diegovasquez@star-ti.com

INFORME DE IMPLEMENTACIÓN BITDEFENDER INDER

Fecha: 16 de diciembre de 2025

Solución Implementada:

- Bitdefender Gravityzone Business Security Enterprise.
- Bitdefender Gravityzone for Email Security.

1. RESUMEN EJECUTIVO

El presente informe detalla las fases y actividades realizadas durante la implementación de Bitdefender Gravityzone Business Security Enterprise para la entidad INDER-Medellín. El objetivo principal fue establecer una solución de seguridad robusta y centralizada para proteger los Endpoint, Servidores de la entidad contra diversas amenazas cibernéticas. Se cubrió desde la configuración inicial de la consola hasta la implementación de agentes en los equipos de cómputo y servidores y la configuración de políticas de seguridad adaptadas a las necesidades del INDER, además de actividades de configuración, trasferencia de conocimiento y soporte durante la vigencia del contrato.

2. Alcance

El licenciamiento adquirido cubre las siguientes protecciones y cantidades.

Ítem	Descripción del producto	Cantidad / usuarios	Tiempo
1	Licencias de antivirus para estaciones	1000	1 año
2	Licencias de antivirus para servidores	20	1 año

3. ACTIVIDADES DE IMPLEMENTACIÓN DETALLADAS

Cada fase de la implementación se llevo a cabo meticulosamente, asegurando la correcta integración y funcionalidad del sistema.

3.1. Creación de la consola Bitdefender Gravityzone

- **Descripción**: Esta actividad implicó la configuración inicial del entorno de Bitdefender GravityZone en la nube.
- Se creó la cuenta principal en la plataforma Bitdefender GravityZone, lo que permitió el acceso a la consola GravityZone.
- **Detalle**:

- Se accedió al portal de Bitdefender Gravityzone con las credenciales de INDER.
- Se provisionó la instancia de GravityZone, seleccionando la región de despliegue óptima para garantizar baja latencia y cumplimiento normativo.
- Se verificó el acceso inicial a la consola de administración, confirmando que todos los servicios principales estuvieran operativos.
- Se configuraron los ajustes básicos del entorno, como la zona horaria y las notificaciones por correo electrónico para alertas críticas.

3.2. Creación de usuarios para administración de la consola

- **Descripción**: Se crearon las cuentas de usuario con roles administrativos específicos dentro de la consola GravityZone para el personal de TI de INDER-Medellín responsables de la gestión de la seguridad.
- **Detalle**:
  - Dentro de la consola GravityZone, se navegó a la sección "Cuentas".
  - Se crearon cuentas de usuario individuales para los administradores designados por la INDER-Medellín.
  - Se asignaron roles de seguridad apropiados a cada usuario (ej. "Administrador completo", "Administrador de políticas", "Visor"), siguiendo el principio de privilegio mínimo. Para este proyecto, se asignó al menos un usuario con "Administrador completo" y otros con roles más restrictivos si era necesario para tareas específicas.
  - Se instruyó a los usuarios sobre cómo acceder a la consola y cambiar sus contraseñas iniciales para mejorar la seguridad.

3.3. Creación del paquete de Instalación para agentes (estaciones de trabajo y servidores)

- **Descripción:** Se crearon paquetes de instalación específicos para los agentes que serían desplegados en las estaciones de trabajo y servidores.
- **Detalle**:
  - Se crean paquetes de instalación con los módulos de protección: Antimalware, SandBox, Cortafuegos, protección de red, control de dispositivos, administración de riesgos, sensor EDR.
  - Se crearon paquetes separados para estaciones de trabajo (con módulos como Antimalware, Firewall, Control de Contenido, Control

de Dispositivos) y servidores (enfocándose en Antimalware, Firewall, EDR, etc., ajustando según las necesidades de los servidores).
- Se aseguraron de que los paquetes fueran lo más optimizados posible en tamaño para facilitar el despliegue.
- Se exportaron los paquetes de instalación para su uso en la implementación.

3.4. Envió de Requerimientos técnicos

Descripción: Se proporcionó a la INDER-Medellín una lista detallada de los requisitos técnicos necesarios para una implementación exitosa de Bitdefender GravityZone, incluyendo especificaciones de hardware, software, red y conectividad.

• **Detalle**:

- Se elaboró un documento que especificaba:
  - Requisitos de red: Puertos TCP/UDP necesarios para la comunicación entre los agentes, los Relays y la consola GravityZone (ej. 8443, 7074, 5799). Rangos de IP permitidos, si aplica.
  - Requisitos de sistema operativo: Versiones soportadas de Windows, Linux y macOS para los endpoint y servidores.
  - Recursos de hardware: RAM, CPU y espacio en disco mínimos para los endpoint y para los servidores que albergarían el Relay o para el appliance virtual de GravityZone si se optó por un despliegue on-premise.
  - Configuraciones de Firewall/Proxy: Instrucciones para configurar los firewalls perimetrales o proxis internos para permitir la comunicación con los servidores de Bitdefender y la consola GravityZone.

3.5. Verificación de Requerimientos Previos: Comunicación, Puertos y Conexiones

- **Descripción**: Se realizaron pruebas para asegurar que la comunicación de red necesaria para Bitdefender GravityZone estuviera abierta y funcionando correctamente en el entorno de La INDER-Medellín.
- **Detalle**:

- Se utilizaron herramientas como ping, telnet o PortQry para verificar la conectividad a los puertos críticos de Bitdefender (ej., 80, 443 para la consola, 7074 para la comunicación con los agentes).
- Se revisaron las reglas del firewall corporativo y los dispositivos de seguridad de red para asegurar que no bloquearan el tráfico esencial.
- Se verificó que no hubiera problemas de latencia o pérdida de paquetes significativos que pudieran afectar el rendimiento de la comunicación.

3.6. Implementación por Recorrido en Sitio

- **Descripción**: Para equipos de las diferentes dependencias se realizó una implementación manual en sitio. Por medio de recorridos en todos las dependencias y oficinas de la INDER-Medellín. A su vez se realiza la desinstalación del agente de protección de endpoint de anterior de ser necesario.
- **Detalle**:
  - Se descargó el paquete de instalación directamente desde la consola GravityZone.
  - Se copió el instalador a una unidad USB o se compartió a el personal de apoyo por medio de chat y/o correo.
  - Se ejecutó el instalador manualmente en cada equipo, siguiendo las instrucciones en pantalla.
  - Se verificó la conexión del agente a la consola GravityZone después de la instalación.

3.7. Instalación de agente en servidores

Se realizo acompañamiento para la verificación y pruebas de funcionamiento del agente de seguridad en los servidores de la entidad evidenciando que la protección se instala sin ninguna novedad en los servidores Windows de la entidad.

3.8. Configuración de políticas y exclusiones

- **Descripción**: Se definieron y aplicaron políticas de seguridad personalizadas para diferentes grupos de equipos en la gobernación y secretaria de educación, incluyendo la creación de exclusiones necesarias para aplicaciones legítimas y procesos de negocio.
- **Detalle**:

- Se accedió a la sección "Políticas" en la consola GravityZone.
- Se crearon políticas específicas para estaciones de trabajo, servidores.
- Dentro de cada política, se configuraron los módulos de seguridad (Antimalware, Firewall, etc.) según las mejores prácticas y los requisitos de la gobernación y la secretaria de educación.
- Se identificaron las aplicaciones, directorios o procesos que debían ser excluidos del escaneo o la supervisión para evitar conflictos o falsos positivos.
- Se agregaron exclusiones detalladas (por ruta de archivo, hash, proceso) según los requerimientos de la entidad para objetos que pudieran ser afectadas por el escaneo en tiempo real.
- Se realizaron pruebas exhaustivas para asegurar que las exclusiones funcionaran correctamente y no comprometieran la seguridad general.

4. Bitdefender Gravityzone Business Security Enterprise: Consola, Módulos y submódulos

Bitdefender GravityZone Business Enterprise es una plataforma de seguridad unificada que proporciona una gestión centralizada para la protección de endpoint, servidores y dispositivos móviles. Su consola web, intuitiva y potente, permite a los administradores de TI controlar todos los aspectos de la seguridad de la red.

4.1. Visión General de la Consola GravityZone

La consola web de GravityZone es el punto central para la gestión de la seguridad. Ofrece un panel de control personalizable, acceso a informes, configuraciones de políticas, despliegue de agentes y monitoreo en tiempo real.

- **Dashboard**: Proporciona una visión general rápida del estado de seguridad de la red, incluyendo infecciones activas, eventos críticos, estado de los agentes y actualizaciones. Es personalizable con widgets.
- **Network (Red)**: Muestra la estructura de la red, permitiendo agrupar equipos, desplegar agentes, enviar tareas y visualizar el estado de seguridad de cada endpoint.
- **Policies (Políticas):** Permite crear, configurar y aplicar políticas de seguridad detalladas a diferentes grupos de endpoint.
- **Reports (Informes):** Genera informes personalizables sobre eventos de seguridad, estado de la protección, actividad de los usuarios, etc.

- **Quarantine (Cuarentena)**: Gestiona los archivos sospechosos o infectados puestos en cuarentena.
- **Tasks (Tareas):** Permite programar y ejecutar tareas en los endpoint, como escaneos, actualizaciones, o desinstalaciones.
- **Notifications (Notificaciones)**: Configura alertas y notificaciones por correo electrónico para eventos específicos.
- **Configuration (Configuración)**: Acceso a la configuración global de la consola, gestión de licencias, usuarios, Active Directory, y más.

4.2. Módulos y Submódulos de Protección

Bitdefender GravityZone Business Enterprise agrupa sus funcionalidades de seguridad en varios módulos clave, cada uno con submódulos específicos para una protección integral.

4.2.1. **Antimalware**

El módulo Antimalware es el núcleo de la protección, diseñado para detectar, bloquear y remediar amenazas de malware de todo tipo.

- **Escaneo en tiempo real (On-Access):**
  - **Submódulo: Protección en tiempo real**: Examina archivos y procesos en el momento de la ejecución o acceso. Utiliza heurística avanzada, firmas de malware y tecnologías de sandboxing para identificar y bloquear amenazas antes de que puedan causar daño.
  - **Configuraciones clave:** Sensibilidad del escaneo, acciones predeterminadas (limpiar, mover a cuarentena, denegar acceso), exclusiones.
- **Escaneo bajo demanda (On-Demand):**
  - **Submódulo: Escaneos programados**: Permite configurar escaneos completos o personalizados en horarios específicos (ej., nocturnos) para detectar malware que pueda haber eludido el escaneo en tiempo real.
  - **Configuraciones clave:** Tipo de escaneo (completo, rápido, personalizado), frecuencia, acción al detectar amenaza, recursos del sistema a usar.
- **Análisis avanzado de amenazas (ATP/Machine Learning):**
  - **Submódulo: HyperDetect/Machine Learning:** Utiliza algoritmos de aprendizaje automático para detectar amenazas avanzadas, sin archivos (fileless), y exploits de día cero, incluso antes de que se creen firmas. Analiza el comportamiento de los procesos.

- **Antivirus de red (Network Antivirus):**
  - **Submódulo: Análisis de tráfico de red**: Inspecciona el tráfico de red en busca de exploits, enlaces maliciosos y otras amenazas que puedan intentar ingresar a través de la red.

4.2.2. Cortafuegos (Firewall)

El módulo Firewall controla el tráfico de red entrante y saliente en los endpoint, previniendo accesos no autorizados y bloqueando comunicaciones maliciosas.

- **Reglas de aplicación**: Permite definir qué aplicaciones pueden acceder a la red y con qué permisos.
- **Reglas de red**: Controla el tráfico en función de direcciones IP, puertos y protocolos.
- **Detección de intrusiones (IDS/IPS):** Monitorea el tráfico de red en busca de patrones que indiquen un intento de intrusión o ataque.
- **Protección de Wi-Fi:** Asegura las conexiones inalámbricas, alertando sobre redes inseguras.
- **Modo sigiloso**: Oculta el equipo de otros dispositivos en la red.

4.2.3. Protección de Red (Network Protection)

Este módulo va más allá del firewall tradicional, enfocándose en la detección de amenazas a nivel de red y la prevención de ataques basados en exploits.

- **Prevención de Exploits (Exploit Detection):**
  - **Submódulo: Advanced Anti-Exploit**: Detecta y bloquea técnicas utilizadas por exploits para comprometer aplicaciones vulnerables, como la inyección de código o la manipulación de memoria.
  - **Inspección SSL**: Permite al agente Bitdefender inspeccionar el tráfico cifrado para detectar amenazas ocultas en comunicaciones SSL/TLS.
  - **Prevención de ataques de fuerza bruta**: Detecta y bloquea intentos repetidos de adivinar credenciales de acceso.
  - **Prevención de ataques de red**: Protege contra ataques como escaneo de puertos, inundación de red y denegación de servicio.

4.2.4. Control de Dispositivos (Device Control)

El Control de Dispositivos gestiona el acceso a dispositivos externos conectados a los Endpoints, como unidades USB, Bluetooth, CD/DVD, etc.

- **Control de acceso:** Permite bloquear o permitir el uso de diferentes tipos de dispositivos.
- **Permisos detallados**: Asigna permisos de lectura/escritura, solo lectura, o sin acceso a grupos de usuarios o dispositivos específicos.
- **Excepciones:** Permite especificar dispositivos de confianza.

4.2.5. **Análisis de Riesgos (Risk Analysis)**

Este módulo evalúa la postura de seguridad de los endpoints y los usuarios, identificando vulnerabilidades y comportamientos riesgosos.

- **Análisis de vulnerabilidades (Vulnerability Assessment):**
  - **Submódulo: Evaluación de vulnerabilidades de aplicaciones/SO:** Identifica software desactualizado, parches de seguridad faltantes, configuraciones erróneas y otras vulnerabilidades en el sistema operativo y las aplicaciones instaladas.
- **Análisis de comportamiento de usuario:**
  - **Submódulo: Comportamiento del usuario y aplicaciones**: Monitorea actividades sospechosas de los usuarios y patrones de uso de aplicaciones que podrían indicar una amenaza o un compromiso.
  - **Informes de riesgo:** Genera informes que detallan los riesgos identificados y sugieren acciones correctivas.

4.2.6. EDR/XDR (Endpoint Detection and Response / Extended Detection and Response)

EDR/XDR proporciona capacidades avanzadas para la detección, investigación y respuesta a incidentes de seguridad en los endpoint y, en el caso de XDR, en otras fuentes de datos.

- **Detección de amenazas avanzadas:**
  - **Submódulo: Correlación de eventos:** Recopila datos de telemetría de los endpoints (procesos, conexiones de red, registros, etc.) y utiliza análisis de comportamiento y machine learning para detectar actividades maliciosas sofisticadas que otras capas de seguridad podrían pasar por alto.
  - **Análisis forense:** Graba y almacena la actividad del endpoint, permitiendo a los analistas de seguridad investigar el origen, alcance y métodos de un ataque.
- **Visualización de ataques**:

- **Submódulo: Grafo de ataque**: Representa visualmente la cadena de eventos de un ataque, mostrando el proceso inicial, las conexiones de red, la creación de archivos y otros indicadores de compromiso.

- **Respuesta a incidentes:**
  - **Submódulo: Acciones de respuesta:** Permite a los administradores tomar acciones rápidas directamente desde la consola, como aislar un endpoint comprometido, detener procesos maliciosos, eliminar archivos o iniciar un escaneo.
- **Búsqueda de amenazas (Threat Hunting):**
  - **Submódulo: Búsqueda activa de amenazas:** Proporciona herramientas para que los analistas de seguridad busquen proactivamente indicadores de compromiso (IOCs) o patrones de ataque en toda la flota de endpoint.
- **Integración XDR:** En la versión XDR, se integra con otras fuentes de datos de seguridad (red, cloud, identidad) para proporcionar una visión holística de las amenazas y una respuesta coordinada.

5. Uso del Módulo de Red en la Consola Bitdefender GravityZone El módulo "Red" (Network) es una de las secciones más importantes de la consola GravityZone, ya que permite organizar, gestionar y desplegar la protección en los equipos de la INDER-Medellín y la secretaria de educación.

5.1. Agrupar equipos

Importancia: La agrupación de equipos es fundamental para aplicar políticas de seguridad de manera eficiente y granular. Permite segmentar la red por departamento, tipo de equipo (servidor, estación de trabajo, laptop), ubicación geográfica, o cualquier otra lógica de negocio.

- **Pasos para Agrupar Equipos:**
  1. **Navegar a la sección "Red"**: En el menú lateral izquierdo de la consola, haga clic en "Red".
  2. **Vista de árbol:** La vista de red muestra una estructura de árbol. Si ha integrado Active Directory, verá sus OUs y grupos. También puede haber grupos por defecto (ej., "Todos los equipos").
  3. **Crear un nuevo grupo:**
  - Haga clic derecho sobre el grupo padre donde desea crear el nuevo grupo (ej., "Equipos Gestionados", o una OU de AD).
  - Seleccione "Agregar" -> "Grupo".

▪ Ingrese un nombre descriptivo para el grupo (ej., "Contabilidad", "Servidores Web", "Desarrollo").

4 mover equipos a grupos:

▪ Manual: Arrastre y suelte equipos individuales o seleccione múltiples equipos y use la opción "Mover a grupo".

▪ Reglas de asignación automática: Puede crear reglas para que los equipos se asignen automáticamente a grupos basándose en criterios como el nombre del equipo, dirección IP, sistema operativo o propiedades de Active Directory. (Esto se hace en "Configuración" -> "Servicios de red" -> "Reglas de asignación").

5.2. **Enviar Tareas a Equipos**

- **Importancia:** Las tareas permiten realizar acciones específicas en uno o varios endpoint desde la consola, como iniciar un escaneo, actualizar agentes, reiniciar equipos, o aplicar configuraciones.
- **Pasos para Enviar una Tarea:**

1 seleccionar los equipos/grupos: En la sección "Red", seleccione los equipos individuales o un grupo completo al que desea enviar la tarea.

2. Hacer clic en "acciones": En la barra superior, haga clic en el botón "acciones" o haga clic derecho en los equipos seleccionados y elija "acción".

3. Seleccionar el tipo de tarea: Aparecerá un menú con diferentes tipos de tareas:

▪ Exploración: Inicia un escaneo Antimalware. Puede ser un escaneo rápido, completo o personalizado.

▪ Actualización: Fuerza una actualización de las bases de datos de virus y del motor del agente.

▪ Reinicio: Reinicia el equipo (con opciones para advertir al usuario).

▪ Desinstalar: Desinstala el agente de Bitdefender.

▪ Asignar Política: Asigna una política de seguridad diferente a los equipos seleccionados.

▪ Aislar/Desaislar: Aísla un equipo de la red para contener una infección.

▪ Correr Análisis: Ejecuta un análisis de riesgos o vulnerabilidades.

▪ Restaurar desde Cuarentena: Restaura un archivo previamente puesto en cuarentena.

4. Configurar la tarea: Dependiendo del tipo de tarea, deberá configurar opciones específicas (ej., para un escaneo: qué escanear, cuándo iniciar, recursos a usar).

5. Enviar tarea: Haga clic en "Enviar" o "Crear tarea" para iniciar el proceso.

6. Monitorear el progreso: El estado de las tareas se puede monitorear en la sección "Tareas" de la consola o en la vista de detalles de cada equipo.

5.3. Crear agentes de Instalación

- **Importancia**: Los paquetes de instalación son la forma principal de desplegar el agente de Bitdefender en los endpoints. Pueden ser personalizados para incluir módulos específicos y configuraciones de Relay.
- **Pasos para Crear un Agente de Instalación (Paquete):**

  1. Navegar a la sección "Paquetes de instalación": En el menú lateral izquierdo, haga clic en "Paquetes de instalación".
  2. Hacer clic en "Agregar": Haga clic en el botón "Agregar" para crear un nuevo paquete.
  3. Seleccionar componentes y rol:
  ▪ Componentes: Elija los módulos de seguridad que desea incluir en el agente (ej., Antimalware, Firewall, Control de Dispositivos, EDR).
  ▪ Rol de Relay: Si este equipo será un Relay para otros, marque la casilla "Activar rol de Relay".
  ▪ Instalación silenciosa: Marque esta opción para que la instalación no requiera interacción del usuario.
  4. Configurar el paquete: Asigne un nombre al paquete (ej., "Agente Estaciones de Trabajo GOB", "Agente Servidores Relay").
  5. Descargar el paquete: Después de crear el paquete, se le dará la opción de descargarlo. Puede ser un instalador .exe o scripts para Linux/macOS.
  6. Despliegue: Utilice el paquete descargado para el despliegue manual, por GPO, SCCM, o cualquier otra herramienta de distribución de software.

6. Funcionamiento de las Políticas en Bitdefender GravityZone

Las políticas son la piedra angular de la gestión de seguridad en Bitdefender GravityZone. Permiten definir un conjunto de reglas y configuraciones de seguridad que se aplican a grupos específicos de endpoint, asegurando una protección consistente y adaptada a las necesidades de cada segmento de la red de la INDER-Medellín y la secretaria de educación.

6.1. Concepto y Funcionamiento

- **Jerarquía:** Las políticas en GravityZone funcionan de manera jerárquica. Puede crear una política maestra y luego políticas hijas que heredan las configuraciones de la política padre. Las políticas hijas pueden anular configuraciones específicas de la política padre si es necesario.

- **Asignación:** Las políticas se asignan a grupos de equipos en la sección "Red". Un equipo solo puede tener una política activa a la vez. Si un equipo es movido de un grupo a otro, automáticamente aplicará la política del nuevo grupo.
- **Flexibilidad:** Esta estructura permite una gran flexibilidad. Puede tener una política global para todos los equipos y luego políticas más específicas para servidores, estaciones de trabajo de alta seguridad, o departamentos específicos.
- **Prioridad:** En caso de superposición (por ejemplo, si un equipo pertenece a varios grupos y cada grupo tiene una política), la política más específica o la que está más abajo en la jerarquía del árbol de red (o la que se asignó directamente si no hay herencia) tendrá prioridad.

6.2. **Módulos Disponibles en las Políticas**

Cuando crea o edita una política, tiene acceso a una amplia gama de módulos de seguridad que puede configurar:

- **Antimalware:**
  - Protección de Acceso (Escaneo en tiempo real)
  - Exploración Bajo Demanda (Escaneos programados)
  - Exclusiones
  - Control de Amenazas Avanzadas (ATP/HyperDetect)
  - Antivirus de Red
- **Firewall:**
  - Reglas de aplicación
  - Reglas de red
  - Detección de intrusiones (IDS)
  - Configuraciones de red (perfiles de red)
- **Control de Contenido:**
  - Filtrado Web (categorías de sitios web a bloquear)
  - Anti-phishing
  - Cifrado de correo electrónico
  - Reglas de contenido (para datos sensibles)
- **Control de Dispositivos**:
  - Reglas para unidades USB, CD/DVD, Bluetooth, etc.
  - Permisos (lectura/escritura, solo lectura, bloquear)
  - Excepciones para dispositivos específicos
- **Protección de Red:**
  - Prevención de Ataques de Red

  - Prevención de Ataques de Fuerza Bruta
  - Inspección SSL
- **EDR/XDR**:
  - Nivel de detección (bajo, medio, alto)
  - Reglas de exclusión para EDR
  - Configuración de telemetría y retención de datos
- **Sandbox Analyzer (Análisis de Sandbox):**
  - Configuración para enviar archivos sospechosos a un entorno de sandbox para un análisis profundo.
- **Control de Aplicaciones (Application Control):**
  - Permite listas blancas/negras de aplicaciones ejecutables.
- **Análisis de Riesgos:**
  - Configuración de la evaluación de vulnerabilidades y el análisis de comportamiento.
- **General:**
  - Actualizaciones (cómo y cuándo se actualiza el agente)
  - Reinicio
  - Interfaz del usuario (qué puede ver y configurar el usuario final)

Elaboro

Diego Vasquez
Líder de proyectos
diegovasquez@star-ti.com

NFORME TÉCNICO DETALLADO: IMPLEMENTACIÓN DE SEGURIDAD PERIMETRAL DE CORREO (HORNETSECURITY)

CLIENTE: INSTITUTO DE DEPORTES Y RECREACIÓN DE MEDELLÍN – INDER

CONTRATO: Suministro No. 6700045132 de 2025

HERRAMIENTA: HornetSecurity Total Protection (Enterprise Suite)

1. RESUMEN TÉCNICO DE LA IMPLEMENTACIÓN

El presente informe documenta el despliegue de la solución de seguridad de correo electrónico en la nube de HornetSecurity para el INDER Medellín. La implementación se centró en la creación de una pasarela de seguridad (Secure Email Gateway) que actúa como nodo intermedio entre el tráfico global de Internet y el tenant de Microsoft 365 de la entidad. Se ejecutaron tareas de reingeniería de registros DNS, sincronización de objetos de directorio mediante Azure AD Connector y el endurecimiento de políticas de filtrado mediante análisis heurístico e inteligencia artificial.

2. ARQUITECTURA DE SEGURIDAD Y MÓDULOS ACTIVADOS

Se ha implementado un esquema de "Defensa en Profundidad" activando los siguientes vectores de protección:

- **Spam & Malware Protection (Nivel 1)**: Filtro basado en reputación de IP, listas RBL (Real-time Blackhole Lists) y firmas de virus conocidas. Detiene el 99.9% del correo no deseado antes de procesar capas superiores.
- **Advanced Threat Protection - ATP (Nivel 2):** Módulo crítico que realiza:
    - Sandboxing: Ejecución de archivos adjuntos sospechosos en entornos virtuales aislados para detectar comportamiento de Ransomware.
    - URL Rewriting: Reescritura de enlaces para analizar el destino en el momento del clic (*Time-of-click protection*).
- **AI Email Security Analyst (Nivel 3):** Motor de aprendizaje automático que identifica anomalías en los patrones de comunicación, detectando intentos de *Business Email Compromise* (BEC) y suplantación de identidad (Spoofing) que no contienen malware tradicional.

- **Email Encryption:** Activación de cifrado TLS forzado y gestión de firmas digitales para asegurar que la información sensible de los procesos deportivos y administrativos del INDER no sea interceptada.

3. CONFIGURACIÓN DE ENRUTAMIENTO Y PERSISTENCIA DNS

Para garantizar la integridad del flujo de datos, se procedió con la configuración de los saltos de red y la validación de propiedad del dominio:

3.1. Configuración del Servidor de Destino (Relay Interno)

Se estableció la ruta de entrega final hacia el entorno de productividad del INDER. El sistema ha sido parametrizado para realizar el envío de correo limpio al host:

- Host de Destino: inder-gov-co.mail.protection.outlook.com
- Puerto: 25 (SMTP con cifrado STARTTLS requerido).
- Validación: Se configuró el *Inbound Connector* en Exchange Online para aceptar exclusivamente tráfico proveniente de los rangos de IP de HornetSecurity.

3.2. Propagación de Registros MX (Mail Exchanger)

Se modificó la zona DNS del dominio inder.gov.co para delegar la autoridad de recepción de correo a los clústeres de HornetSecurity. Se verificó la propagación exitosa de los siguientes registros con sus respectivas prioridades para garantizar alta disponibilidad:

1. mx-01.hornetsecurity.com (Prioridad 10)
2. mx-02.hornetsecurity.com (Prioridad 20)
3. mx-03.hornetsecurity.com (Prioridad 30)
4. mx-04.hornetsecurity.com (Prioridad 40)

4. GESTIÓN DE DIRECTORIO Y SINCRONIZACIÓN DE BUZONES

La integridad del sistema depende de la correspondencia exacta entre los usuarios de Microsoft 365 y la consola de seguridad.

4.1. Análisis Cuantitativo de Sincronización

El proceso de sincronización arrojó los siguientes resultados operativos:

- Buzones Sincronizados: 1,985 cuentas procesadas.
- Licencias Asignadas: 1,984 usuarios activos (1 cuenta en reserva/técnica).

- Dominios Protegidos: 3 (incluyendo el dominio principal y alias técnicos).

4.2. Detalle de Atributos Importados

Tras procesar el archivo mailboxes.csv, se confirma la correcta ingesta de metadatos para la segmentación de políticas por departamento. Se han sincronizado exitosamente usuarios de las siguientes dependencias críticas:

- Subdirección de Escenarios Deportivos y Recreativos: Ej. *Adiela Monroy Garcia*.
- Subdirección de Fomento Deportivo y Recreativo: Ej. *Adolfo Leon Villada*.
- Subdirección Administrativa y Financiera: Ej. Adrian Avalos Sanchez.

El sistema ha mapeado no solo la dirección principal (@inder.gov.co), sino también los alias de coexistencia en la nube (@https://www.google.com/search?q=indermedellin.onmicrosoft.com), asegurando que ninguna identidad quede desprotegida.

5. REGLAS DE DETECCIÓN Y ACCIÓN (EMAIL LIVE TRACKING)

Se han parametrizado reglas de acción inmediata en el panel de Live Tracking, permitiendo al equipo de TI del INDER una respuesta forense ante incidentes:

Categoría de Detección	Acción Configurada	Descripción Técnica
Clean / Limpio	Deliver (Entregar)	Tráfico legítimo que cumple con SPF/DKIM.
Infomail	Quarantine/Tag	Boletines y publicidad masiva (Graymail).
Spam	Reject / Quarantine	Bloqueo por firmas de baja reputación.
Content / Rejected	Block	Filtrado por extensión de archivo (ej. .exe, .scr) o palabras clave prohibidas.
Threat / AdvThreat	Quarantine + Alert	Amenazas detectadas por ATP/Sandbox. Se requiere liberación manual por administrador.

6. OBLIGACIONES ESPECÍFICAS DE IMPLEMENTACIÓN

Se certifica que la implementación cumple con los siguientes requisitos del Anexo Técnico:

1. Protección en Tiempo Real: El retardo de procesamiento es inferior a 2 segundos por mensaje.
2. Reportes de Cuarentena: Se configuró el envío automático de reportes de spam a los 1,985 usuarios para autogestión de correos bloqueados.
3. Seguridad de Salida: Se configuró el conector de salida (*Smart Host*) para que el correo enviado desde el INDER también sea filtrado, protegiendo la reputación del dominio contra posibles listas negras.

7. CONCLUSIÓN

La fase de implementación de HornetSecurity para el INDER Medellín ha finalizado con una cobertura del 100% de los buzones identificados. El sistema se encuentra en fase de monitoreo activo, con todas las reglas de ATP y AI operativas, garantizando una reducción inmediata en la superficie de ataque por correo electrónico.

Elaboro

Diego Felipe Vasquez
líder de proyectos
diegovasquez@star-ti.com

INFORME TÉCNICO DE IMPLEMENTACIÓN Y CUMPLIMIENTO DE OBLIGACIONES - INDER MEDELLÍN

FECHA: 16 de diciembre de 2025

CLIENTE: Instituto de Deportes y Recreación de Medellín - INDER

CONTRATO: Suministro No. 6700045132 de 2025

SOLUCIONES: Radware WAF.

Implementación de Radware WAF (CWAAP Advanced)

1. Sesión de Kick Off del Servicio CWAAP

El día 15 de diciembre de 2025 se llevó a cabo la sesión formal de Kick Off del servicio Radware Cloud Web Application and API Protection (CWAAP) – Plan Advanced, con la participación del equipo técnico del INDER Medellín Harrison Hernández, Star Solutions TI S.A.S. y el Customer Success Manager de Radware, Kendry Muro

Durante esta sesión se presentaron los siguientes aspectos clave del servicio:

- Descripción general del servicio CWAAP Advanced, su arquitectura cloud-native y su operación en modalidad Managed Service.
- Alcance contratado: protección de hasta 11 aplicaciones, con un throughput de 10 Mbps, bajo el tenant INDER Medellín
- Revisión de los módulos de seguridad habilitados en el plan Advanced, incluyendo:
    - WAF con protección OWASP Top 10
    - Protección de APIs
    - Rate Limiting
    - Geobloqueo
    - Control de acceso por IP
    - Protección contra ataques DoS/DDoS en capa 7
    - Reportería y analítica avanzada en tiempo real
- Explicación del modelo de onboarding, fases de estabilización, afinamiento de políticas y responsabilidades entre Radware, Star Solutions TI y el cliente

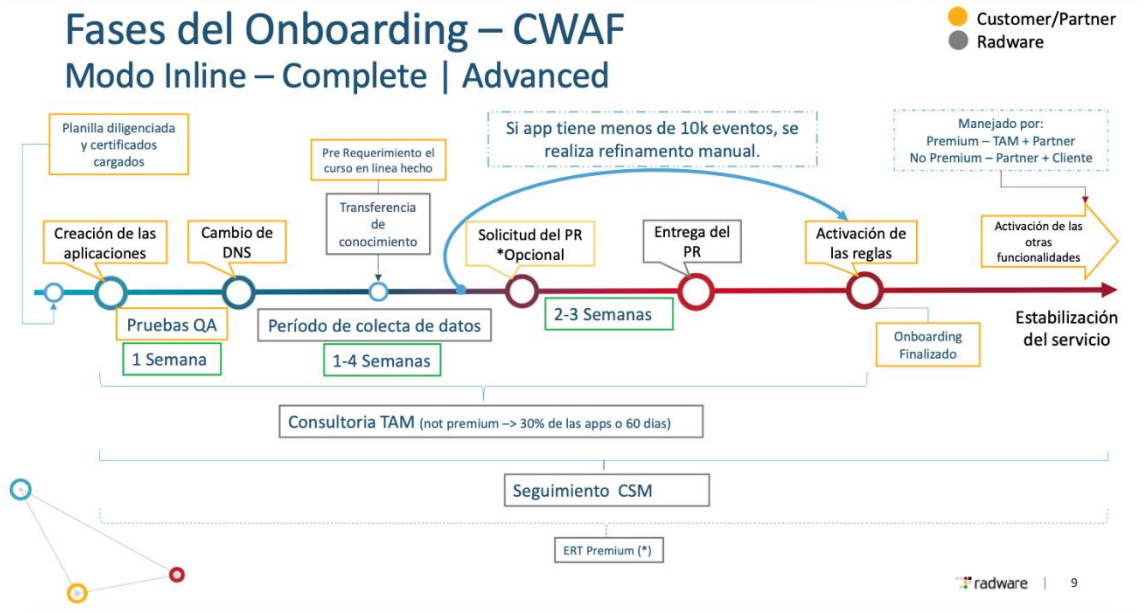
Como evidencia de esta actividad, se anexa al presente informe la presentación oficial utilizada durante la sesión de Kick Off, suministrada por Radware.

Planes de servicio de protección de aplicaciones

radware	Standard	Advanced	Complete
WAF	✓	✓	✓
Protección API	✓	✓	✓
Protección básica contra bots	✓	✓	✓
Límite de Tráfico	✓	✓	✓
Control de acceso y reglas geográficas de IP	✓	✓	✓
Informes, alertas y análisis	✓	✓	✓
Consultas al Threat Intelligence (Por mes)	50	50	50
Protección DDoS	1Gbps	10Gbps	10Gbps
Soporte estándar	✓	✓	✓
Soporte avanzado	X	✓	✓
WAF avanzado (Path Access Protection & IA)	X	✓	✓
ERT Active Attackers Feed (EAAF)	X	✓	✓
Client-Side Protection |Detección	X	✓	✓
Client-Side protection | Mitigación	X	X	✓
Descubrimiento de API & Protección BLA	X	X	✓
Bot Manager	X	X	✓
Balanceador de carga como servicio	Failover	Básico	Avanzado
Retención de data	30 Días	60 Días	90 Días
Extensión de Cumplimiento PCI DSS 4	X	Add-On	Add-On
AI SOC Xpert para Protección de Aplicaciones	Add-On	Add-On	Add-On
Protección web DDoS	Add-On	Add-On	Add-On
DNS como Servicio Administrado (DNSaaS)	Add-On	Add-On	Add-On
DDoS Ilimitado	Add-On	Add-On	Add-On
CDN como Servicio Administrado (CDNaaS)	Add-On	Add-On	Add-On

Fases del Onboarding – CWAF

Modo Inline – Complete | Advanced



2. Carga y Registro de Aplicaciones en la Plataforma CWAAP

Posterior a la sesión de Kick Off, se realizó la creación y carga inicial de las aplicaciones dentro de la consola de Radware CWAAP, conforme al alcance contratado y a la información técnica suministrada por el INDER.

Las actividades ejecutadas incluyeron:

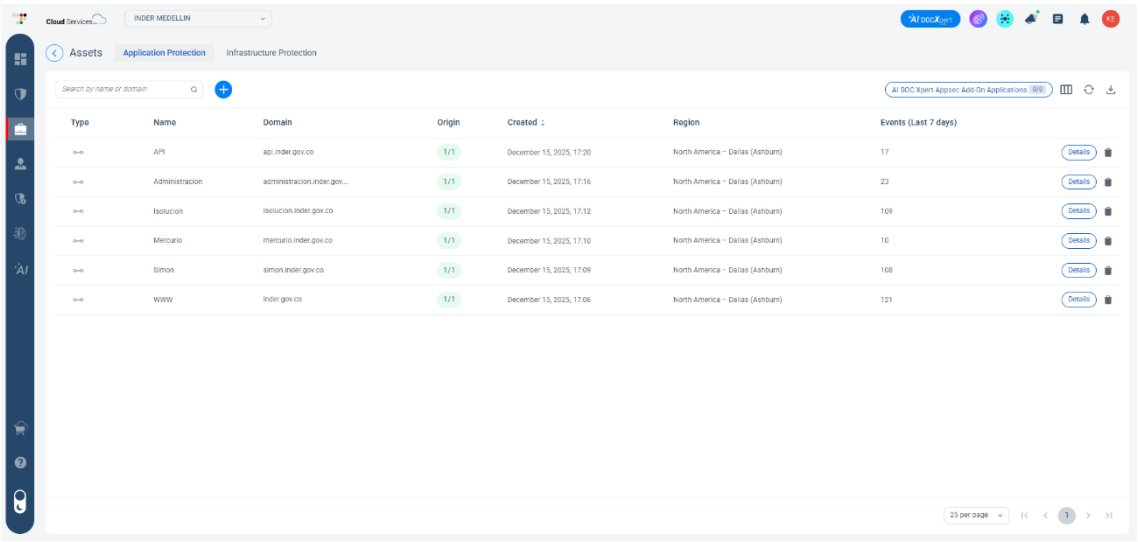
- Registro de las aplicaciones web institucionales dentro del tenant INDER Medellín.
- Asociación de cada aplicación a su respectivo perfil de protección WAF.
- Validación de visibilidad de tráfico, eventos y métricas iniciales.
- Verificación de conectividad y correcta resolución de los endpoints protegidos.

Como soporte documental, se anexan capturas de pantalla (screenshots) de la consola de Radware donde se evidencia:

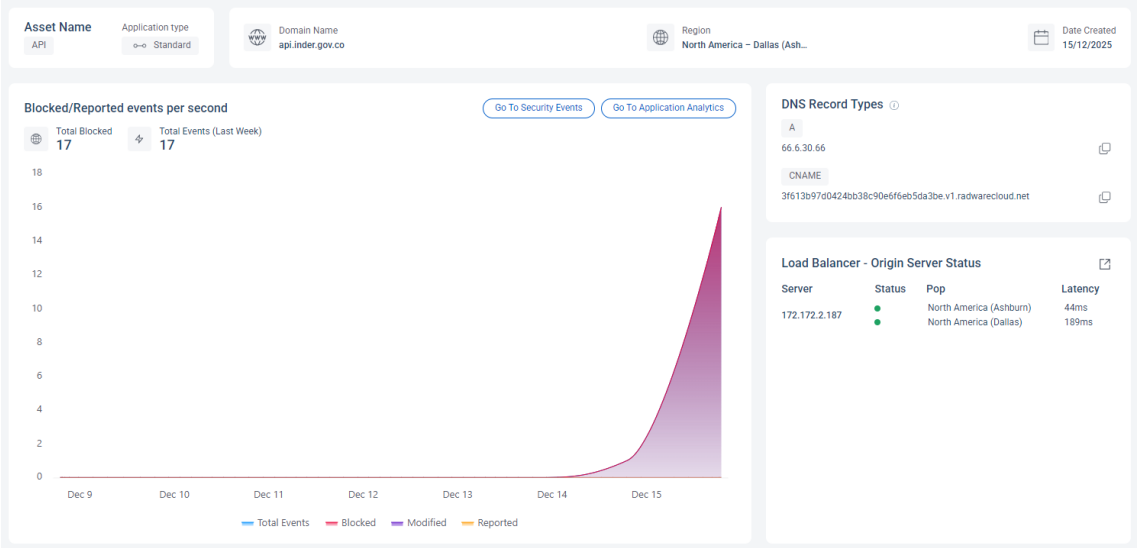
- La creación de las aplicaciones.
- El estado activo del servicio.
- La correcta asignación del plan CWAAP Advanced.

Estas evidencias confirman la correcta habilitación inicial del servicio y la disponibilidad de las aplicaciones bajo el esquema de protección contratado. A continuación:

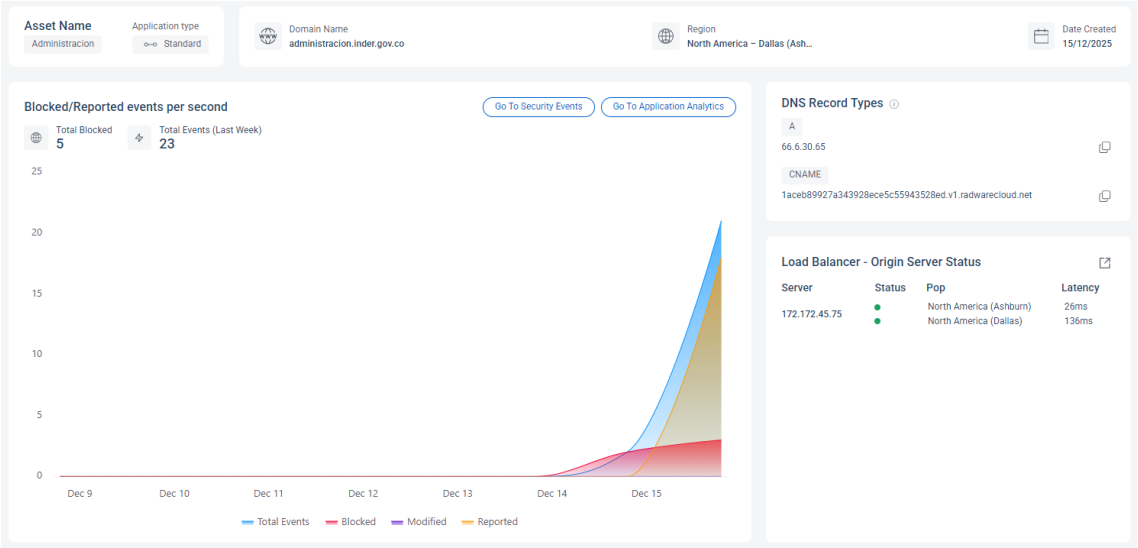
- General de aplicaciones:



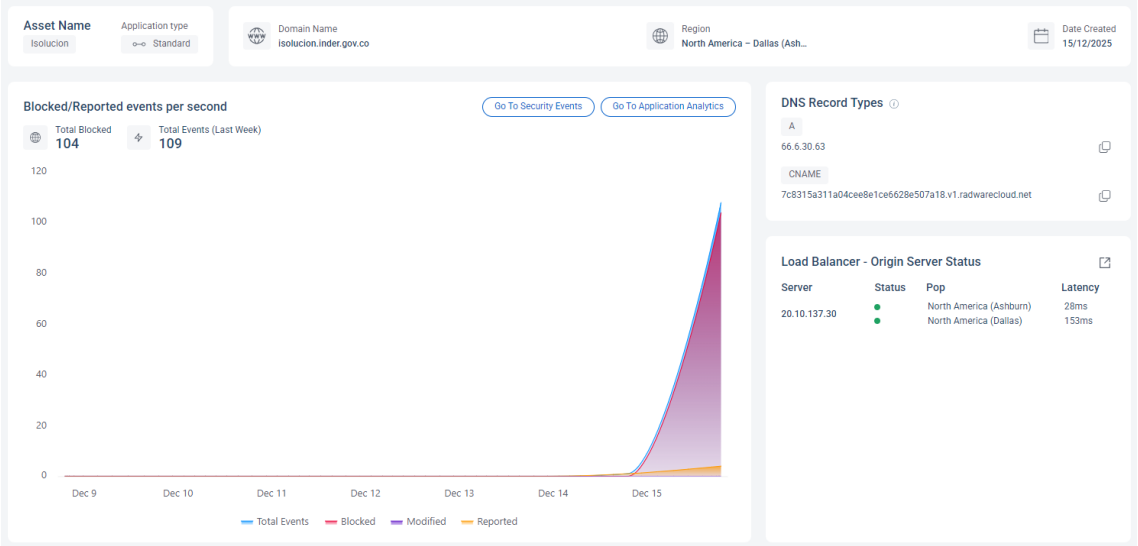
- API:



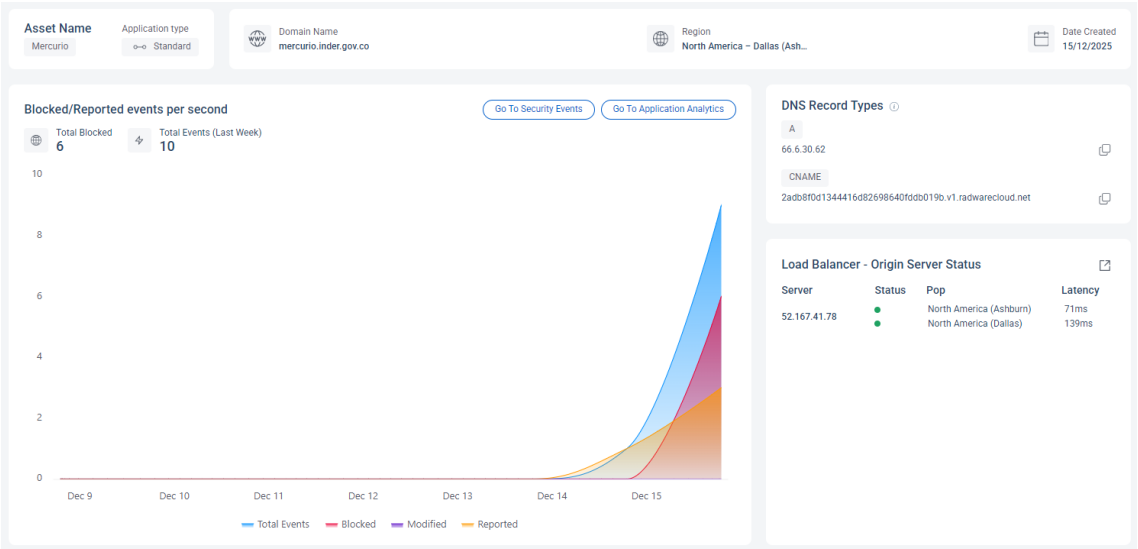
- Administracion:



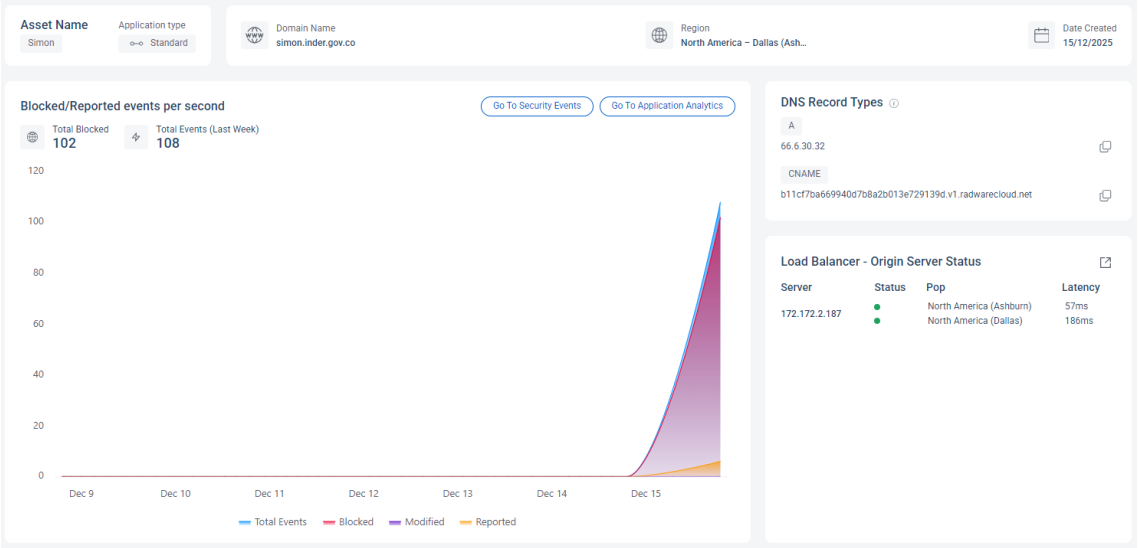
- Isolucion:



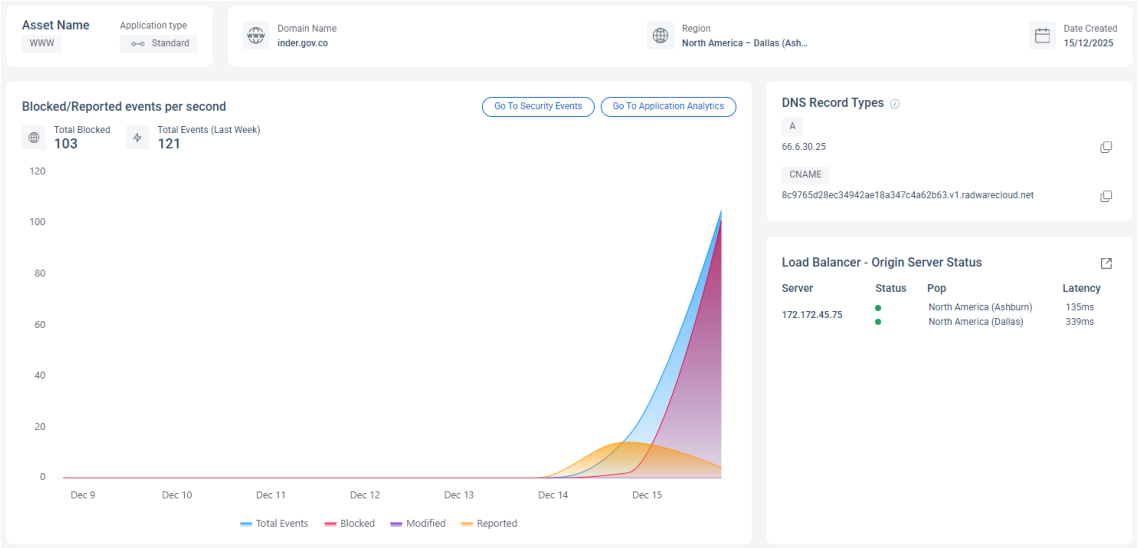
- Mercurio:



- Simon:



- WWW:



3. Alcance Actual del Servicio WAF

De acuerdo con el licenciamiento adquirido, el alcance vigente del servicio WAF es el siguiente

- **Servicio:** Radware Cloud Application Protection – CWAAP Advanced
- **Modalidad:** Servicio administrado (Managed Service)
- **Capacidad:** 10 Mbps
- **Número de aplicaciones:** hasta 11 aplicaciones protegidas
- **Vigencia:** 12 meses

- **Componentes incluidos:**
  - WAF avanzado
  - Protección de APIs
  - Protección contra bots básica
  - Protección DoS/DDoS en capa de aplicación
  - Reportes, alertas y analítica
  - Servicios administrados de revisión de políticas y análisis post-ataque

Este alcance se encuentra alineado con lo establecido contractualmente en el Contrato de Suministro No. 6700045132 de 2025, garantizando la protección de las aplicaciones críticas del INDER expuestas a Internet.

4. Próximos Pasos del Proyecto WAF
Una vez completada la fase inicial de Kick Off y carga de aplicaciones, los **próximos pasos definidos para la implementación del servicio WAF** son los siguientes:

1. **Fase de estabilización y monitoreo inicial**
   Recolección de tráfico y eventos para análisis de comportamiento normal de las aplicaciones.
2. **Afinamiento de políticas (tuning)**
   Ajuste de reglas WAF para minimizar falsos positivos y optimizar la protección, conforme al patrón de uso real de las aplicaciones.
3. **Activación progresiva de reglas avanzadas**
   Habilitación controlada de políticas OWASP Top 10, rate limiting, geobloqueo y protección de APIs.
4. **Integración y validación de reportería**
   Verificación de dashboards, alertas y visibilidad de eventos de seguridad.
5. **Sesiones de seguimiento**
   Reuniones periódicas entre INDER, Star Solutions TI y Radware para revisión del estado del servicio y recomendaciones de mejora continua.

Estos pasos permitirán consolidar la operación del WAF bajo un esquema estable, seguro y alineado con las mejores prácticas de seguridad de aplicaciones.

Cordial saludo,
Enrique Avila
STAR SOLUTIONS
Unidad de Ciberseguridad

Bogotá D.C. 17 de diciembre de 2025

Señores: INSTITUTO DE DEPORTES Y RECREACIÓN DE MEDELLÍN – INDER Atn: Supervisión de Contrato Suministro No. 6700045132 Ciudad

ASUNTO: Informe Detallado del Alcance de la Garantía Comercial del Servicio – Contrato No. 6700045132 de 2025.

Respetados señores:

Yo Fabian Alberto Palomares Velosa En mi calidad de Representante Legal de **STAR SOLUTIONS TI S.A.S.**, y en cumplimiento de las obligaciones establecidas en el Anexo Técnico y las condiciones contractuales del proceso de la referencia, me permito informar detalladamente el alcance de la **Garantía Comercial** de las soluciones de Antivirus (**Bitdefender**), Antispam (**HornetSecurity**) y WAF (**Radware**) suministradas:

1. Alcance de la Protección y Vigencia La garantía cubre el funcionamiento ininterrumpido y la eficacia técnica de las soluciones durante toda la vigencia contratada (12 meses), asegurando que el licenciamiento se mantenga activo y a nombre del **INDER Medellín**.

2. Soporte Técnico y Asistencia Especializada

- **Disponibilidad 24/7:** Se garantiza la atención de incidentes críticos las 24 horas del día, los 7 días de la semana, para fallos que afecten la disponibilidad de los servicios protegidos (especialmente el WAF en Azure y el flujo de correo).
- **Niveles de Servicio (SLA):** La garantía comercial asegura tiempos de respuesta y solución alineados con la criticidad de la infraestructura tecnológica del Instituto.
- **Asistencia Técnica:** Incluye acompañamiento remoto y presencial (según se requiera) por parte de ingenieros certificados por los fabricantes.

3. Actualizaciones y Mantenimiento

- **Firmas y Motores:** Se garantiza la actualización automática y permanente de las firmas de virus, bases de datos de spam y reglas de protección del WAF ante nuevas amenazas de "día cero".
- **Versiones de Software:** El servicio incluye el derecho a actualizar a las últimas versiones de las consolas de administración y agentes (Bitdefender GravityZone, HornetSecurity y Radware) sin costo adicional durante la vigencia.

4. Cumplimiento de Especificaciones Técnicas (WAF y SIEM) La garantía comercial respalda que la solución WAF mantendrá el rendimiento especificado en el anexo técnico:

- Compatibilidad total con **Azure East US 2**.

- Soporte de 730 horas de puerta de enlace, 5 unidades de proceso y transferencia de 2 TB.
- Garantía de persistencia en la ingesta de **2 GB diarios** de registros de análisis hacia **Microsoft Sentinel**.

5. Exclusiones de la Garantía La garantía no cubrirá fallos derivados de manipulaciones no autorizadas en las configuraciones por personal ajeno a Star Solutions o la supervisión del INDER, ni daños causados por el uso indebido de las credenciales de administración por parte de terceros.

Esta garantía comercial coincide plenamente con las características mencionadas en las especificaciones técnicas del contrato y busca asegurar la continuidad operativa y la integridad de la información del INDER Medellín.

Atentamente,

Fabian Alberto Palomares
Representante legal
fabianpalomares@star-ti.com

STAR SOLUTIONS TI S A S
NIT 900.968.161-7
CARRERA 27 # 49 19
Tel: (57) 3007010017
Bogotá - Colombia
facturacion@star-ti.com
www.star-ti.com

Factura electrónica de venta
No. FEST 1002

Señores	INSTITUTO DE DEPORTES Y RECREACION DE MEDELLIN		
NIT	800.194.096-0	**Teléfono**	(604) 3699000 - Ext. 000
Dirección	CALLE 47D No. 75 276	**Ciudad**	Bogotá - Colombia

Fecha y hora Factura	
Generación	16/12/2025, 14:50
Expedición	16/12/2025, 16:09
Vencimiento	31/12/2025

Ítem	Descripción	Cantidad	Vr. Total	% Desc.	Valor Impto.Cargo	Vr. Unitario
1	Antivirus con consola de administración. Protección de servidores de centro de datos con diferentes sistemas operativos: Windows server 2008 Windows server 2012 Windows server 2016 Linux Ubuntu CentOS Debe contar con agente para la instalación en el servidor Protección de equipos de cómputo de usuario final contra malware y ransomware. Detección y respuesta en endpoints (EDR). Gestión de vulnerabilidades y reducción de superficie de ataque. Supervisión en tiempo real y análisis de amenazas. Debe permitir bloqueo de puertos usb Debe contar con ageste para la instalación en el equipo de cómputo	1,020.00	246,947,100.00	0 %	0.00	242,105.00
2	DEBE SER COMPATIBLE CON EL CORREO DEL INDER MEDELLÍN MICROSOFT 365 Análisis de archivos y enlaces maliciosos (Safe Attachments y Safe Links). Prevención avanzada de phishing y suplantación de identidad. Explorador de amenazas (Threat Explorer) para investigar incidentes en tiempo real. Automatización de investigación y respuesta (AIR) ante amenazas. Simulaciones de ataques (phishing, malware) para capacitar a los usuarios. Seguimiento de campañas de amenazas y análisis forense. Integración con el ecosistema de seguridad	1,400.00	278,838,000.00	0 %	0.00	199,170.00
3	DEBE SER COMPATIBLE CON AZURE EN NUBE Protección contra ataques OWASP Top 10 Filtrado de tráfico HTTP/S Protección de APIs Mitigación de ataques DDoS a nivel de aplicación Gestión de bots maliciosos Reescritura y enmascaramiento de URLs Geobloqueo y control por IP Protección contra carga de archivos maliciosos Análisis de comportamiento y detección de anomalías Reglas personalizadas y automatización Integración con SIEM y herramientas de monitoreo Dashboard de monitoreo y reportes Soporte para HTTPS y certificados	1.00	65,875,000.00	0 %	0.00	65,875,000.00

Total items: 3

Total Bruto	591,660,100.00
Total a Pagar	591,660,100.00

Valor en Letras:
Quinientos noventa y un millones seiscientos sesenta mil cien pesos m/cte

Forma de pago:
Crédito

Medio de pago:
Otro - Clientes Nacionales - Cuota No. 001 vence el 2025-12-31 por $ 591,660,100.00

Observaciones:
"SOMOS REGIMÉN SIMPLE DE TRIBUTACIÓN FAVOR NO PRACTICAR RETENCIONES, SOLO RETENCIÓN DE IVA"

REALIZAR TRANSFERENCIA BANCARIA A LA CUENTA CORRIENTE NO. 021397849 DEL BANCO DE BOGOTÁ

A esta factura de venta aplican las normas relativas a la letra de cambio (artículo 5 Ley 1231 de 2008). Con esta el Comprador declara haber recibido real y materialmente las mercancías o prestación de servicios descritos en este título - Valor. **Número Autorización Electrónica 18764088028273 aprobado en 20250130 prefijo FEST desde el número 844 al 2000 Vigencia: 24 Meses**
Responsable de IVA - Actividad Económica 6202 Actividades de consultoría informática y actividades de administración de instalaciones informáticas Tarifa 6.9*1000
CUFE: 9b20b044121ac149a08434a2ceaf47a160f0113bebdf42e4aba30c1903df65e7ee048e78878e0514260f696a77e36e4f

UNIDAD ADMINISTRATIVA ESPECIAL **JUNTA CENTRAL DE CONTADORES**

Certificado No:

0 7 D 2 6 1 7 4 7 2 8 9 8 F F 6

LA REPUBLICA DE COLOMBIA

MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO

UNIDAD ADMINISTRATIVA ESPECIAL

JUNTA CENTRAL DE CONTADORES

CERTIFICA A:
QUIEN INTERESE

Que el contador público **JAVIER ISIDRO REYES PEDRAZA** identificado con CÉDULA DE CIUDADANÍA No 80773731 de BOGOTA, D.C. (BOGOTA D.C) Y Tarjeta Profesional No 246176-T SI tiene vigente su inscripción en la Junta Central de Contadores y desde los últimos 5 años.

NO REGISTRA ANTECEDENTES DISCIPLINARIOS ******************************* ** ***

Dado en BOGOTA a los 16 días del mes de Diciembre de 2025 con vigencia de (3) Meses, contados a partir de la fecha de su expedición.

SANDRA MILENA BARRIOS PULIDO
DIRECTOR GENERAL

ESTE CERTIFICADO DIGITAL TIENE PLENA VALIDEZ DE CONFORMIDAD CON LO ESTABLECIDO EN EL ARTICULO 2 DE LA LEY 527 DE 1999, DECRETO UNICO REGLAMENTARIO 1074 DE 2015 Y ARTICULO 6 PARAGRAFO 3 DE LA LEY 962 DEL 2005

Para confirmar los datos y veracidad de este certificado, lo puede consultar en la página web www.jcc.gov.co digitando el número del certificado

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - MINTIC

CERTIFICA QUE

Una vez consultada la base de datos de deudores alimentarios morosos **REDAM**, el(la) ciudadano(a) con número de identificación CC 80239727 **NO SE ENCUENTRA INSCRITO EN EL REGISTRO DE DEUDORES ALIMENTARIOS MOROSOS**

Esta certificación es válida en todo el Territorio Nacional, siempre y cuando el tipo y número consignados en el respectivo documento de identificación, coincidan con los aquí registrados.

Se expide en Bogotá el 16/12/2025 04:16 PM

Código Verificación: **MVYCKPU7ZS**

Válida hasta: **16/03/2026**

Dirección de Gobierno Digital

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - MINTIC

compensar | miplanilla.com

PLANILLA INTEGRADA DE AUTOLIQUIDACION DE APORTES

DATOS DEL APORTANTE						
TIPO	NÚMERO	NOMBRE APORTANTE	DIRECCIÓN	TELÉFONO	CORREO	EXONERADO PAGO PARAFISCALES Y SALUD
NI	900968161-7	STAR SOLUTIONS TI SAS	CARRERA 27 No. 29 19	3007010017	contacto@star-ti.com	
FORMA PRESENTACIÓN	CLASE APORTANTE	NOMBRE SUCURSAL	CÓDIGO	DEPARTAMENTO	CIUDAD / MUNICIPIO	
SUCURSAL	C – MIPYME	CENTRO	002	BOGOTÁ D. C.	BOGOTÁ, D.C.	SI

DATOS DE LA PLANILLA						
PLANILLA ASOCIADA	FECHA PAGO ASOCIADA (DIA/MES/AÑO)	TIPO PLANILLA	FECHA PAGO (DIA/MES/AÑO)	NÚMERO PLANILLA	CANTIDAD	
					EMPLEADOS	UPC
					9	0
PERIODO SALUD	PERIODO PENSIONES				TOTAL A PAGAR	
2025-12	2025-11	E	01/12/2025	91882769	$4.066.200	

TOTALES POR SUBSISTEMAS

TOTALES SALUD

Código EPS	Nombre	NIT	Cotización Obligatoria	UPC Adicional	Incapacidades		Licencia Maternidad		Días Mora	Valor Mora Cotización	Valor Mora UPC	Total a Pagar	No. Afiliados
					No. Autorización	Valor	No. Autorización	Valor					
EPS005	Sanitas EPS	800251440-6	171.000	0		0		0	0	0	0	171.000	3
EPS008	Compensar EPS	860066942-7	69.600	0		0		0	0	0	0	69.600	1
EPS017	Famisanar EPS	830003564-7	422.800	0		0		0	0	0	0	422.800	5

TOTALES PENSIÓN

Código AFP	Nombre	NIT	Cotización Obligatoria	Aporte Voluntario Afiliado	Aporte Voluntario Aportante	Aporte FSP - Solidaridad	Aporte FSP - Subsistencia	Días Mora	Valor Mora Cotización	Valor Mora FSP	Total a Pagar	No. Afiliados
230201	Proteccion (ING + Proteccion)	800229739-0	313.100	0	0	0	0	0	0		313.100	1
230301	Porvenir	800224808-8	1.428.000	0	0	0	0	0	0		1.428.000	4
231001	Colfondos	800227940-6	227.800	0	0	0	0	0	0		227.800	1
25-14	Colpensiones	900336004-7	683.400	0	0	0	0	0	0		683.400	3

TOTALES RIESGOS LABORALES

Código ARL	Nombre	NIT	Cotización Obligatoria	Incapacidades		Aportes Otros Sistemas	Valor Neto Cotización	Días Mora	Valor Mora Cotización	Subtotal Cotización	No. Radicado Saldo a Favor	Valor Saldo a Favor	Fondo Solidaridad	Total a Pagar	No. Afiliados
				No. Autorización	Valor										
14-11	ARL SURA	890903790-5	87.100				87.100	0	0	87.100			871	87.100	9

TOTALES CAJAS

Código CCF	Nombre	NIT	Valor Aporte	Días Mora	Valor Mora Aporte	Total a Pagar	No. Afiliados
CCF24	Compensar Caja	860066942-7	663.400	0	0	663.400	9

TOTALES PARAFISCALES

Valor Aporte	Días Mora	Valor Mora Aporte	Total a Pagar	No. Afiliados
SENA				
0	0	0	0	0
ICBF				
0	0	0	0	0
ESAP				
MEN				

TOTALES POR SUBSISTEMA

Tipo Administradora	No. Administradoras Reportadas	Valor antes de IGE, LMA, IRP y Mora	Total a Pagar
Salud	3	663.400	663.400
Pensión	4	2.652.300	2.652.300
Riesgos Laborales	1	87.100	87.100
CCF	1	663.400	663.400
ESAP	0	0	0
ICBF	0	0	0
MEN	0	0	0
SENA	0	0	0
TOTALES	9	4.066.200	4.066.200

compensar | miplanilla.com

PLANILLA INTEGRADA DE AUTOLIQUIDACION DE APORTES

DATOS DEL APORTANTE						
TIPO	NÚMERO	NOMBRE APORTANTE		DIRECCIÓN	TELÉFONO	CORREO
NI	900968161-7	STAR SOLUTIONS TI SAS		CARRERA 27 No. 29 19	3007010017	contacto@star-ti.com
FORMA PRESENTACIÓN	CLASE APORTANTE	NOMBRE SUCURSAL	CÓDIGO	DEPARTAMENTO	CIUDAD / MUNICIPIO	EXONERADO PAGO PARAFISCALES Y SALUD
SUCURSAL	C – MIPYME	CENTRO	002	BOGOTÁ D. C.	BOGOTÁ, D.C.	SI

DATOS DE LA PLANILLA						
PLANILLA ASOCIADA	FECHA PAGO ASOCIADA (DIA/MES/AÑO)	TIPO PLANILLA	FECHA PAGO (DIA/MES/AÑO)	NÚMERO PLANILLA	CANTIDAD	
					EMPLEADOS	UPC
					9	0
PERIODO SALUD	PERIODO PENSIONES				TOTAL A PAGAR	
2025-12	2025-11	E	01/12/2025	91882769	$4.066.200	

DETALLE POR COTIZANTE

INFORMACIÓN COTIZANTE									INFORMACIÓN NOVEDADES																		PENSIÓN							SALUD			RIESGOS LABORALES				CCF			PARAFISCALES				
No.	Tipo	No. de Identificación	Apellidos y Nombres	Cotizante	Subtipo	Extranjero	Colom. exterior	Exonerado	ING	RET	TDE	TAE	TDP	TAP	VSP	VST	SLN	IGE	LMA	VAC	AVP	VCT	IRL	CORRECCIÓN	Cód. AFP	IBC AFP	Cotización	Voluntario Afiliado	Voluntario Aportante	Fondo pensional de solidaridad	Fondo pensional de subsistencia	Cód. EPS	IBC EPS	Cotización / Valor UPC	Cód. ARL	IBC ARL	Clase de Riesgo	Cotización	Código CCF	IBC CCF	Aporte CCF	IBC otros parafiscales	Aporte SENA	Aporte ICBF	Aporte ESAP	Aporte MEN
1	CC	1001060911	JUZGA MOLANO JOHAN STEVEN	1	0			S																	230301	1.739.130	278.300	0	0	0	0	EPS008	1.739.130	69.600	14-11	1.739.130	1	9.100	CCF24	1.739.130	69.600	0	0	0	0	0
2	CC	1022995774	BURBANO RODRIGUEZ LIDY JANETH	1	0			S																	230201	1.956.522	313.100	0	0	0	0	EPS017	1.956.522	78.300	14-11	1.956.522	1	10.300	CCF24	1.956.522	78.300	0	0	0	0	0
3	CC	1024537986	VASQUEZ MOLANO DIEGO FELIPE	1	0			S																	230301	3.586.956	574.000	0	0	0	0	EPS017	3.586.956	143.500	14-11	3.586.956	1	18.800	CCF24	3.586.956	143.500	0	0	0	0	0
4	CC	1031123013	SALAS MONCALEANO NATALIA ISABEL	1	0			S																	231001	1.423.500	227.800	0	0	0	0	EPS017	1.423.500	57.000	14-11	1.423.500	1	7.500	CCF24	1.423.500	57.000	0	0	0	0	0
5	CC	52034285	MOLANO MONCALEANO ADRIANA MARIA	1	0			S																	25-14	1.423.500	227.800	0	0	0	0	EPS005	1.423.500	57.000	14-11	1.423.500	1	7.500	CCF24	1.423.500	57.000	0	0	0	0	0
6	CC	52384267	MOLANO MONCALEANO CLAUDIA ANGELICA	1	0			S																	25-14	1.423.500	227.800	0	0	0	0	EPS005	1.423.500	57.000	14-11	1.423.500	1	7.500	CCF24	1.423.500	57.000	0	0	0	0	0
7	PT	6410610	BORGES OSORIO DANILO ENRIQUE	1	0			S																	230301	2.173.913	347.900	0	0	0	0	EPS017	2.173.913	87.000	14-11	2.173.913	1	11.400	CCF24	2.173.913	87.000	0	0	0	0	0
8	CC	79641922	MOLANO MONCALEANO PEDRO ALBERTO	1	0			S																	25-14	1.423.500	227.800	0	0	0	0	EPS017	1.423.500	57.000	14-11	1.423.500	1	7.500	CCF24	1.423.500	57.000	0	0	0	0	0
9	CC	80257478	MOLANO MONCALEANO JORGE ENRIQUE	1	0			S																	230301	1.423.500	227.800	0	0	0	0	EPS005	1.423.500	57.000	14-11	1.423.500	1	7.500	CCF24	1.423.500	57.000	0	0	0	0	0

REPUBLICA DE COLOMBIA
IDENTIFICACION PERSONAL
CEDULA DE CIUDADANIA

NUMERO **80.239.727**

PALOMARES VELOSA
APELLIDOS

FABIAN ALBERTO
NOMBRES

FIRMA

INDICE DERECHO

FECHA DE NACIMIENTO **11-JUL-1981**

BOGOTA D.C.
(CUNDINAMARCA)
LUGAR DE NACIMIENTO

1.83	**O+**	**M**
ESTATURA	G.S. RH	SEXO

05-AGO-1999 BOGOTA D.C.
FECHA Y LUGAR DE EXPEDICION

REGISTRADORA NACIONAL
ALMABEATRIZ RENGIFO LOPEZ

A-1500113-45151892-M-0080239727-20061002 **00709**06275C 02 190665613

REPUBLICA DE COLOMBIA
IDENTIFICACION PERSONAL
CEDULA DE CIUDADANIA

NUMERO **80.773.731**

REYES PEDRAZA

APELLIDOS

JAVIER ISIDRO

NOMBRES

FIRMA

INDICE DERECHO

FECHA DE NACIMIENTO **29-AGO-1985**

BOGOTA D.C
(CUNDINAMARCA)
LUGAR DE NACIMIENTO

1.73
ESTATURA

O+
G.S. RH

M
SEXO

04-SEP-2003 BOGOTA D.C.
FECHA Y LUGAR DE EXPEDICION

REGISTRADOR NACIONAL
CARLOS ARIEL SÁNCHEZ TORRES

A-1500150-00723489-M-0080773731-20150716 **0045**082487A 1 16334746

STAR SOLUTIONS. T.I.
LO SIMPLE FUNCIONA

EL SUSCRITO REVISOR FISCAL DE

STAR SOLUTIONS TI SAS

NIT. 900.968.161-7

CERTIFICA

Que **STAR SOLUTIONS TI SAS,** identificada con el NIT **900.968.161-7** ha cumplido hasta la fecha y durante los últimos 6 meses con el pago oportuno de sus obligaciones frente al Sistema de Salud, Riesgos Profesionales, Pensiones y Parafiscales (Cajas de Compensación Familiar, SENA e ICBF), de conformidad con lo dispuesto en el artículo 50 de la Ley 789 del 27 de diciembre de 2002, en concordancia con la Ley 828 del 10 de julio de 2003.

Se expide en Bogotá D.C., a los dieciseis (16) días del mes de diciembre de 2025.

Javier Isidro Reyes Pedraza
C.C.NO. 80.773.731
TP. 246176-T

REPUBLICA DE COLOMBIA
IDENTIFICACION PERSONAL
CEDULA DE CIUDADANIA

NUMERO **80.773.731**

REYES PEDRAZA

APELLIDOS

JAVIER ISIDRO

NOMBRES

FIRMA

INDICE DERECHO

FECHA DE NACIMIENTO **29-AGO-1985**

BOGOTA D.C
(CUNDINAMARCA)
LUGAR DE NACIMIENTO

1.73 ESTATURA

O+ G.S. RH

M SEXO

04-SEP-2003 BOGOTA D.C.
FECHA Y LUGAR DE EXPEDICION

REGISTRADOR NACIONAL
CARLOS ARIEL SÁNCHEZ TORRES

A-1500150-00723489-M-0080773731-20150716 0045082487A 1 16334746

República de Colombia
Ministerio de Comercio, Industria y Turismo

UNIDAD ADMINISTRATIVA ESPECIAL | JUNTA CENTRAL DE CONTADORES

246176-T

JAVIER ISIDRO
REYES PEDRAZA
C.C. 80773731
RES. INSCRIPCION 701 DEL 17/08/2018
FUNDACION UNIVERSIDAD AUTONOMA DE COLOMBIA

OSCAR EDUARDO FUENTES PEÑA
DIRECTOR GENERAL

253569 273079