

Oferta Técnica y Comercial

EDR

INSTITUCIÓN UNIVERSITARIA DIGITAL DE ANTIOQUIA - IU DIGITAL

Medellín, 8 de agosto de 2025

Señores

IU DIGITAL

Medellín

En Tigo Business entregamos diferentes servicios y soluciones tecnológicas que buscan acompañarlo en la evolución tecnológica de su empresa. Por esta razón y con el objeto de brindar una experiencia de comunicación memorable y a su medida hoy le presentamos, para su evaluación, una propuesta de Servicios de Ciberseguridad pensada en sus necesidades y acorde al crecimiento de su negocio y su operación.

Ponemos a su disposición todo nuestro capital humano y tecnológico para entregarle el mejor servicio que le permita una adecuada y mejor utilización de los productos que actualmente tiene de nuestro portafolio.

Gracias por su confianza.

Cordial saludo,

Christian Camilo Vanegas P.
Digital Sales Manager
Gerencia Sector Gobierno
VP. Negocios Empresas y Gobierno
Christian.Vanegas.P@tigo.com.co • (57) 316 834 70 29
Carrera 48 # 20-45 • Sede Principal • Piso 13 • Medellín - Colombia

Los servicios de CiberSeguridad son prestados por UNE EPM Telecomunicaciones S.A. Este documento contiene información confidencial perteneciente a Tigo Business, constituyendo secreto empresarial; por tanto, la información aquí consignada no deberá ser utilizada, parcial o totalmente, para fines diferentes al propósito de este documento; excepto en aquellos casos aprobados previamente por Tigo Business.

Tabla de Contenido

Tabla de Contenido 3
TIGO EDR 5
1. GENERALES 5
1.1 Características y Beneficios 5
1.2 Propuesta de Valor 6
2. DESCRIPCIÓN DE LA PROPUESTA 6
2.1 Objetivo 10
2.2 Alcance 10
2.4 Caracterización del servicio 11
2.3 Funcionalidades 12
2.3.2 Discover & Predict 12
2.3.3 Protect & Response 13
2.3.4 Discovery, Protect and Response 13
2.3.5 Responder y corregir 13
2.3.6 Post-Infección 14
2.3.7 Políticas de aplicaciones 15
2.4 Cloud Service 16
2.5 Topología General de la Solución 17
2.6 Alcance del Servicio Administrado incluido 17
2.6.1 Gestión de colectores en plataforma EDR: 18
2.6.2 Actividades de upgrade o actualización de Colectores 20
2.6.3 Gestión de Políticas de seguridad en la plataforma EDR 20
2.6.4 Gestión de aplicaciones y control de comunicaciones en la plataforma EDR 22
2.6.5 Gestión de eventos en la plataforma EDR 23
2.6.6 Delivery o aprovisionamiento 24
2.6.7 Monitoreo e Informes 25
2.6.8 Servicios Administrados ante Fallas 26
2.6.9 Atención Especializada 26
2.7 Implementación y/o transición 27
2.7.1 Metodología de aprovisionamiento 27

2.7.2 Tiempo de aprovisionamiento 28
2.7.3 Entregables 28
2.8 Propuesta Económica 28
2.9 Roles y Responsabilidades 29
2.10 Consideraciones generales: 29
3. COMPROMISOS DEL CLIENTE 32
3.1 Responsabilidades del cliente 32
3.2 Acuerdo de confidencialidad 32

TIGO EDR

1. GENERALES

Tigo EDR está diseñado para que cualquier tipo de empresa, sin importar su tamaño o la complejidad de sus necesidades, pueda contar con esquemas avanzados ante la protección contra ataques cibernéticos, aportando a la continuidad de negocio de las compañías y brindando el respaldo necesario para mantener su nivel de productividad. La seguridad de la información es uno de los pilares de la transformación digital de las compañías, por esta razón, es necesario contar con un aliado de negocios experto en materia de ciberseguridad. Las diferentes modalidades de Tigo EDR brindan niveles avanzados de protección contra amenazas a la confidencialidad, integridad y disponibilidad de la información de su negocio a través de la prevención, detección y respuesta a incidentes de seguridad, los cuales se complementan con Servicios Administrados de Seguridad que le permiten a su empresa contar con expertos capacitados para el diseño, configuración, monitoreo, pruebas y actualización de políticas y servicios de seguridad adquiridos.

1.1 Características y Beneficios

- EDR es una solución con capacidades de **protección, detección y respuesta automática** a incidentes de ciberseguridad causados por software malicioso en los dispositivos terminales o endpoints brindando protección tanto antes(pre-infección) como después de que ocurre una infección (post-infección).

- EDR previene la infección de malware y de ransomware, detecta y desactiva posibles amenazas en tiempo real y **automatiza procedimientos de respuesta y corrección** con tareas programables y automatizables.

- **Protección** Como se ha demostrado con los resultados de la evaluación ATT&CK de MITRE, FortiEDR permite una protección de endpoints proactiva, automatizada y en tiempo real con respuesta orquestada a incidentes en todas las plataformas. Detiene las brechas con bloqueo en tiempo real para proteger los datos de la exfiltración y el cifrado de ransomware.

- **Gestión** FortiEDR ofrece una plataforma unificada e intuitiva gestionada en la nube. automatiza tareas rutinarias de seguridad en los endpoint y también admite RBAC y shell remoto seguro.

- **Integración** integración nativa con otras plataformas Fortinet y también con soluciones de terceros como NGFW, NAC, SIEM y más para mejorar la seguridad y la orquestación.

- **Escalabilidad** Con una infraestructura nativa en la nube y un tamaño reducido, FortiEDR puede desplegarse rápidamente y escalar para proteger centenares de miles de endpoints.

- **Flexibilidad** Los endpoints están protegidos tanto dentro de la red como fuera de la red mediante IA integrada.

1.2 Propuesta de Valor

"Con Tigo EDR, las empresas cuentan con los recursos necesarios para prevenir, detectar y responder ante ataques, incidentes o vulnerabilidades de seguridad de la información de manera continua y confiable".

2. DESCRIPCIÓN DE LA PROPUESTA

Tigo presenta a IUDIGITAL una solución de EDR en modalidad de servicio, que cubre los componentes: Servicios de Ciberseguridad Endpoint Protection; el equipamiento, la instalación, el soporte, el mantenimiento, la operación, el monitoreo y el cumplimiento de ANS, a través del recurso humano, las herramientas, la seguridad y los procesos del ciclo de vida de servicios enmarcados en ITIL y COBIT. Con esta solución Tigo ofrece los siguientes diferenciadores:

Diferenciadores a nivel de servicio:

- Rápido proceso de implementación tecnológica y operativa
- Simplicidad en la operación
- Escalabilidad de la solución a brindar considerando el crecimiento del negocio
- Confidencialidad sobre la información y documentación procesada
- Flexibilidad en adiciones, cambios y modificaciones
- Oportunidad en la inclusión de nuevos servicios y/o funcionalidades que apoyen el negocio
- Soporte 24x7
- Despliegue
- Las licencias pueden ofrecerse en cualquier cantidad a los clientes finales
- La plataforma multi-tenant permite ofrecer servicios 100% gestionados o cogestionados con los clientes finales (hasta 100 sub-tenants + 50 de expansión)
- Infraestructura de nube asegurada y gestionada por Fortinet

Disponibilidad de la plataforma y del servicio:

- 99.8% para cualquier mes calendario
- Soporte técnico FortiCare™ 24x7, como se describe en las políticas de soporte de Fortinet vigentes en ese momento y descripción del servicio, disponible en el Portal de soporte u otro sitio designado por Fortinet.

Impactos y comportamientos esperados por componente:

Nombre de Componente	Descripción	Comportamiento	Mode de despliegue
Collector	Endpoint Component	Si se produce un error en el Collector el endpoint no estaría protegido, pero es muy poco probable que esto suceda. Eventualmente fallaría durante la instalación y no aparecerá en la GUI de administración (configuración incorrecta, pase de registro incorrecto, problemas de comunicación) o se	On-Prem

		mostrará como degradado si el sistema operativo no es compatible.	
Core	Logic and Enforcement	Sin impacto en la protección de endpoints Solo en la ejecución de ciertos Playbooks. En caso de que esté configurado como un Jumpbox para integrarse con otros dispositivos Fabric, esas integraciones no estarían disponibles. Si existe más de un-Core bajo el mismo agregador, los Collecotrs conmutarán automáticamente por error de la comunicación al siguiente más cercano disponible. Los Collectorss se mostrarán como Ejecutándose de forma autónoma en el administrador, si la comunicación con el agregador sigue vigente.	On-Prem, Cloud, Hybrid
Aggregator	Scaling/ Load balancer	Sin impacto en la protección de endpoints Los Collectors se mostrarán como desconectados en la GUI de administración. Los Collectors no pueden moverse a otro agregador. En caso de un fallo importante, reconstruya el agregador y los Collectors se volverán a conectar. Durante la interrupción, este agregador no aplicará cambios de configuración en los Collectors administrados.	On-Prem Cloud Hybrid
Component Name	Short Description	Behavior / Impact on Failure?	Deployment Mode
Central Manager	Platform Management	Sin impacto en la protección de endpoints El acceso a FCS no estará disponible, por lo que no se producirá la reclasificación de eventos. No hay acceso a los registros y la configuración. Este sistema tampoco es redundante.	On-Prem Cloud
Threat Hunting	Data Repository	Sin impacto en la protección de endpoints No se podrá acceder a los datos de telemetría, no se ejecutarán consultas proactivas.	On-Prem Cloud

Fortinet Cloud Services	Security Operations and Enrichment	Sin impacto en la protección de endpoints. No se producirá la reclasificación de eventos. Algunos Playbooks pueden verse afectados.	On-Prem Cloud

Funcionalidades soportadas por la solución:

ETAPA	FUNCIONALIDAD	DESCUBRIMIENTO, PROTECCION Y RESPUESTA
Descubrimiento	Descubrimiento de activos	•
	Evaluación de activos	•
	Reducción de superficie de ataque	•
	Control de aplicaciones	•
	USB Control	•
Protección	NGAV (pre-ejecución)	•
	Protección posterior a la ejecución	•
	Cloud Sandbox	•
	Inteligencia de amenazas en la nube	•
	Visualización de cadena de ataque	•
	Análisis forense avanzado de incidentes	•
	Etiquetado MITRE	•
	Filtrado web malicioso	•
Respuesta	Registro y análisis continuos	•
	Caza de amenazas	•
	Etiquetado de comportamiento basado en IA	•
	Ingestión y búsqueda de IOC (indicadores de compromiso)	•
	Investigación soportada por IA	•
	Security Fabric Integration*	•
	integración con terceras partes*	•
	Remediación automatizada	•
	Marco de respuesta automatizada a incidentes	•
	Shell remoto seguro	•

*Se valida como una factibilidad independiente y podría tener costos de servicios profesionales

Plataformas soportadas:

Windows:

- XP SP2/SP3, 7, 8, 8.1, 10, y 11 (versiones de 32 bits y 64 bits)
- Server 2003 SP2, R2 SP2, 2008 SP2, 2008 R2 SP1, 2012, 2012 R2, 2016, 2019, y 2022

MacOS:

- Capitan (10.11), Sierra (10.12), High Sierra (10.13), Mojave (10.14), Catalina (10.15), Big Sur (11.x), Monterey (12.x), y Ventura (13.x)

Linux:

- RedHat Enterprise Linux y CentOS:
  - 6.x, 7.x, y 8.x
- Ubuntu LTS:
  - 16.04.x, 18.04.x, y 20.04.x (solo 64 bits)
- Oracle Linux:
  - 6.x+, 7.7+, y 8.2+
- Amazon Linux AMI 2
- SuSE SLES:
  - 15.1

Detalles adicionales de Ubuntu LTS:

16.04.x server:

- Versiones del kernel: 4.4.0-131, 4.4.0-142, 4.4.0-145, 4.4.0-169, 4.4.0-173, 4.4.0-184
- 18.04.x server:
- Versiones del kernel: 4.15.0-34, 4.15.0-36, 4.15.0-54, 4.15.0-55, 4.15.0-66, 4.15.0-70, 4.15.0-72, 4.15.0-74, 4.15.0-76, 4.15.0-88 generic, 4.15.0-108 generic

20.04.x server:

- Versiones del kernel: 5.4.0-42, 5.4.0-47, 5.4.0-48 generic

Detalles adicionales de RHEL (CentOS):

Versión 6:

- CentOS & RHEL 6.8: 2.6.32-642
- CentOS & RHEL 6.9: 2.6.32-696
- CentOS & RHEL 6.10: 2.6.32-754

Versión 7:

- CentOS & RHEL 7.2: 3.10.0-327
- CentOS & RHEL 7.3: 3.10.0-514
- CentOS & RHEL 7.4: 3.10.0-693
- CentOS & RHEL 7.5: 3.10.0-862
- CentOS & RHEL 7.6: 3.10.0-957
- CentOS & RHEL 7.7: 3.10.0-1062

- CentOS & RHEL 7.8: 3.10.0-1127
- CentOS & RHEL 7.9: 3.10.0-1160

Versión 8:

- CentOS & RHEL 8.0: 4.18.0-80
- CentOS & RHEL 8.1: 4.18.0-147
- CentOS & RHEL 8.2: 4.18.0-193
- CentOS & RHEL 8.3: 4.18.0-240

Oracle Linux 8.2, 8.3 (User Space Collector)

Collector Version	App/kernel	Supported OS
v4.1 and lower	kernel	RHEL/CentOS 6, 7, 8, Ubuntu 16.04, 18.04, 20.04
v4.5.0.178+	application	Oracle 8.2+, Oracle 7.7+, Amazon AMI, SLES12, SLES15
v4.5.1	application/kernel	RHEL/CentOS 6, 7, 8, Ubuntu 16.04, 18.04, 20.04
v5.1	kernel	RHEL/CentOS 6,7,8

- VDI Environments: VMware Horizons 6 and 7 and Citrix XenDesktop 7
- Google Cloud Marketplace enablement for all supported OSes

Nota:

- Utilice siempre la última versión del instalador para las versiones y kernels compatibles.
- Collector 4.5.1 soporta CentOs, Ubuntu en modo Kernel o modo de aplicación.
- Collector 4.5.0 solo admite Oracle, Amazon, SUSE -> en modo de aplicación.
- Para actualizaciones refiérase a
- https://community.fortinet.com/t5/FortiEDR/Technical-Tip-FortiEDR-Latest-Release-Version-Chart/ta-p/209555
- Technical Tip: Linux Application Features and Limi... - Fortinet Community

2.1 Objetivo

El objetivo principal es presentar al cliente **IUDIGITAL** una solución de Tigo EDR en modalidad **Endpoint Protection Only** la cual proporciona una plataforma de seguridad ante ataques avanzados que le permitirá a **IUDIGITAL** proteger la confidencialidad, integridad y disponibilidad de la información de su negocio a través de la prevención, detección y respuesta a incidentes de seguridad involucrando componentes adicionales del portafolio de Tigo Business.

2.2 Alcance

El diseño contenido en este documento corresponde al HLD (High Level Design) de la solución. La elaboración del LLD (Low Level Design) se realizará en conjunto con **IUDIGITAL**, para definir los detalles de alcance y modos de operación de la infraestructura de seguridad en las diferentes fases propuestas para la Implementación.

2.4 Caracterización del servicio

A continuación, se definen los detalles de la infraestructura, capacidades y las características del servicio

El Antivirus de Nueva Generación (FortiEDR) ofertado es una herramienta de seguridad que brinda una protección multicapa, antes y después de la infección con el fin de contener los Malwares Avanzados en tiempo real. Esto permite evitar la exfiltración, secuestro de datos críticos en caso de cualquier amenaza sobre sus sistemas informáticos.

Tigo ofrece a IUDIGITAL el suministro de (1000) licencias de FortiEDR por doce (12) meses, junto con el servicio de gestión, monitoreo y notificación de alertas de seguridad, veinticuatro (24) horas, los siete (7) días de la semana, durante los trecientos sesenta y cinco (365) días del año.

Descripción	Ubicación	Versiones Soportadas
• Suministro de (1000) licencias de FortiEDR con vigencia por doce (12) meses. • Configuración y parametrización de la plataforma Central Manager • Servicios de gestión, monitoreo y notificación de alertas de seguridad 7*24 para (1000) agentes de FortiEDR por doce (12) meses.	El despliegue se realizará de manera remota en la ubicación designada por el cliente. No se incluyen desplazamientos a sitio.	Ver Compatibilidad con Sistemas Operativos

Requisitos de cómputo para los endpoints:

- Cpu: < 1%
- memory: 60-120MB
- Disk usage: 20MB
- Ancho de banda: 5 Mbps per 1K Collectors

Permisos de firewall: Aplican los relacionados con el collector o agente.

From	To	Port
Collector	Aggregator	TCP 8081
Collector	Core	TCP 555

Consideraciones del Alcance:

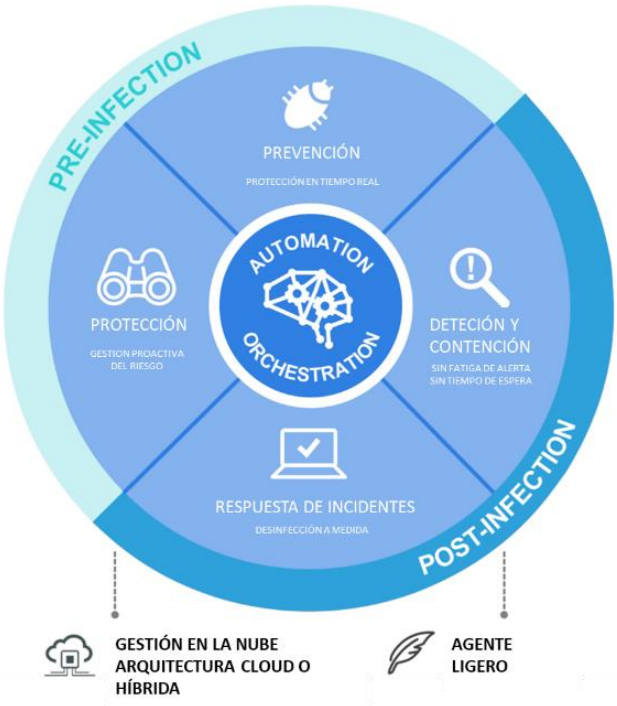
- El alcance del servicio está limitado a prestar los servicios de Antivirus de Nueva Generación a los equipos de IUDIGITAL. Cualquier cambio en el alcance deberá ser revisado en conjunto con Tigo, con el fin de validar si dicha modificación conlleva a costos adicionales.
- La presente oferta está diseñada para soportar, única y exclusivamente, (1000) licencias de FortiEDR para Endpoints y/o Servidores. Por ende, el incremento en la cantidad de Collectors o agentes tendrá costos adicionales, los cuales no se encuentran dentro de la presente oferta.

- La retención de logs se realiza de forma centralizada en la infraestructura cloud por 1 mes, para mayor retención de logs se debe comprar Add-On de Disk Expansión (512 GB storage).
- Tigo no se hace responsable por el rendimiento o efectividad de las funcionalidades descritas que ofrece el producto FortiEDR.
- Tigo brindará soporte, única y exclusivamente, de las funcionalidades del agente FortiEDR. Por ende, Tigo no será responsable ni brindará atención de requerimientos o incidentes relacionados a equipo ofimáticos como: lentitud del equipo, conexión a Internet, etc.

2.3 Funcionalidades

Las siguientes funcionalidades estarán habilitadas dependiendo del alcance puntual del caso de uso seleccionado, no todas aplican para todos los casos de uso, pero se describen a continuación para homologar conceptos:

El Servicio FortiEDR se presta a través de la plataforma en la nube FortiEDR, gestionada por Fortinet las veinticuatro (24) horas del día durante los siete (7) días de la semana. La plataforma en la nube FortiEDR se supervisa para garantizar la disponibilidad del servidor, la capacidad del servicio y la utilización de los recursos de red, y se basa en Google Cloud Platform para los servicios alojados y la infraestructura informática.



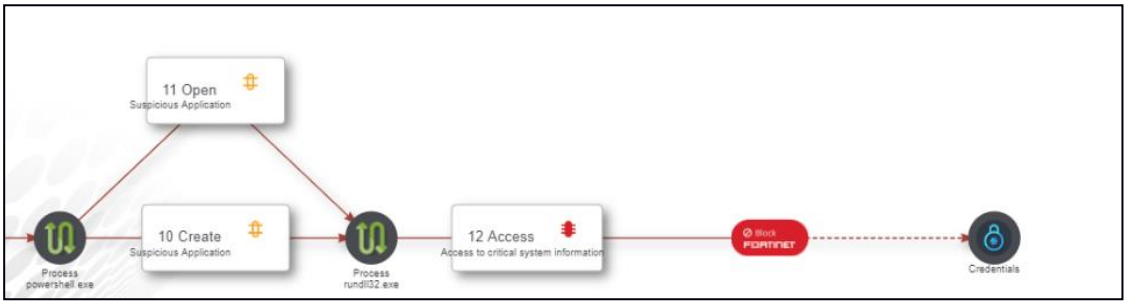
2.3.2 Discover & Predict

Motor de prevención pre-infección basado en las capacidades de Fortinet Next Generation Anti-Virus (NGAV); protección post-infección en tiempo real; mitigación proactiva de riesgos que incluye el descubrimiento de aplicaciones en comunicación y dispositivos IoT, gestión de vulnerabilidades y

clasificación de aplicaciones que potencia la reducción de la superficie de ataque; respuesta orquestada a incidentes que incluye investigación automatizada. Este paquete de servicios también se denomina Predict & Protect.

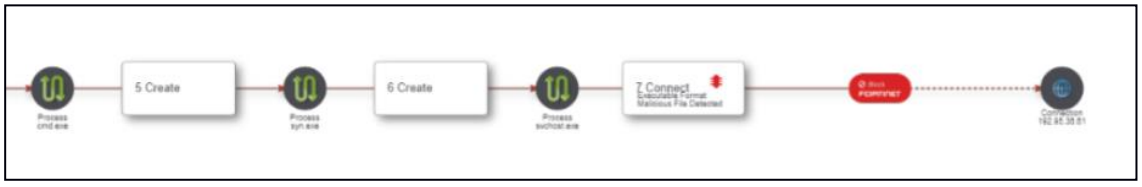
2.3.3 Protect & Response

Motor de prevención pre-infección basado en las capacidades de Fortinet NGAV; protección post-infección en tiempo real; capacidades de caza de amenazas con retención de datos de hasta un (1) mes; visión y control forense que incluye gráfico de ataque con rastreo de código y respuesta orquestada a incidentes que incluye capacidades de investigación y remediación automatizadas. Este paquete de servicios también se conoce como Proteger y Responder.



2.3.4 Discovery, Protect and Response

Motor de prevención pre-infección basado en las capacidades de Fortinet NGAV; protección en tiempo real post-infección; mitigación proactiva de riesgos que incluye descubrimiento de aplicaciones y dispositivos IoT en comunicación, gestión de vulnerabilidades y clasificación de aplicaciones que potencian la reducción de la superficie de ataque; capacidades de caza de amenazas con retención de datos de hasta un (1) mes; visión general y control forense que incluye gráfico de ataque con rastreo de código y respuesta orquestada a incidentes que incluye capacidades de investigación y remediación automatizadas. Este paquete de servicios también se conoce como Predecir, Proteger y Responder.



2.3.5 Responder y corregir

Organice las operaciones de respuesta a incidentes mediante guías personalizadas con información sobre distintos tipos de entornos. Agilice los procesos de respuesta y corrección de incidentes. Revierta manual o automáticamente los cambios maliciosos realizados por amenazas ya contenidas en un único dispositivo o en dispositivos de todo el entorno.

- Automatice la clasificación de incidentes para mejorar la respuesta a los mismos y facilitar su resolución.

- Recomienda acciones de respuesta a los analistas de seguridad
- Estandarice los procedimientos de respuesta a incidentes con la automatización de libros de jugadas
- Optimice los recursos de seguridad automatizando las acciones de respuesta a incidentes, como la eliminación de archivos, la terminación de procesos maliciosos, la reversión de cambios persistentes, la notificación a usuarios, el aislamiento de aplicaciones y dispositivos y la apertura de tickets.
- Permitir una respuesta a incidentes basada en el contexto utilizando la clasificación de incidentes y los sujetos de los ataques (por ejemplo, grupos de puntos finales).
- Obtenga visibilidad completa de la cadena de ataque y de los cambios maliciosos con el rastreo de código patentado.
- Automatice la limpieza y deshaga los cambios maliciosos preservando el tiempo de actividad del sistema.
- Obtenga ayuda adicional con el servicio opcional de detección y respuesta gestionadas (MDR)

FortiEDR detiene en tiempo real y de forma precisa las filtraciones de datos y los daños causados por el ransomware, permitiendo automáticamente la continuidad de la actividad empresarial incluso en dispositivos ya comprometidos.

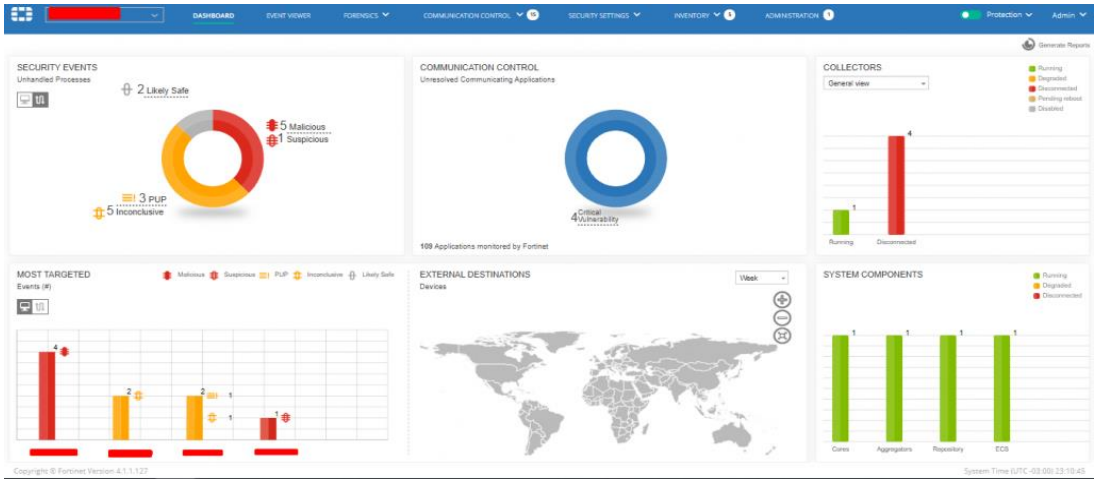
- Aprovecha la detección centrada en el sistema operativo altamente precisa en la detección de ataques sigilosos infiltrados incluidos los ataques basados en la memoria y del tipo " living off the land".
- Detiene las brechas en tiempo real y elimina el tiempo de permanencia de las amenazas
- Analiza todo el historial de registros
- Previene el cifrado de ransomware y el ataque a archivos y registros.
- Valida continuamente la clasificación de las amenazas

*NOTA: Estas características están disponibles única y exclusivamente bajo el modo “PREVENTION” En dado caso se tuviera activado el modo “Simulación” estas características no estarían disponibles.

2.3.6 Post-Infección

Detección y contención: actúa de forma rápida ante la ejecución de un archivo malicioso, pudiendo eliminarlo del endpoint y evitando el movimiento lateral del malware.

Respuesta a incidentes: bloquear las comunicaciones externas del malware al negarle el acceso a los sistemas de archivos evitando la filtración de datos e incluso el cifrado de ransomware en tiempo real.





*NOTA: Estas características están disponibles única y exclusivamente bajo las políticas de "COMMUNICATION CONTROL"

Podemos observar el despliegue de un bloque de políticas y como este contiene acciones que ofrecen mayor granularidad y personalización en cuanto a las acciones y habilitación políticas se refiere. Adicionalmente podemos observar cómo se asignan grupos colectores a bloques de políticas.

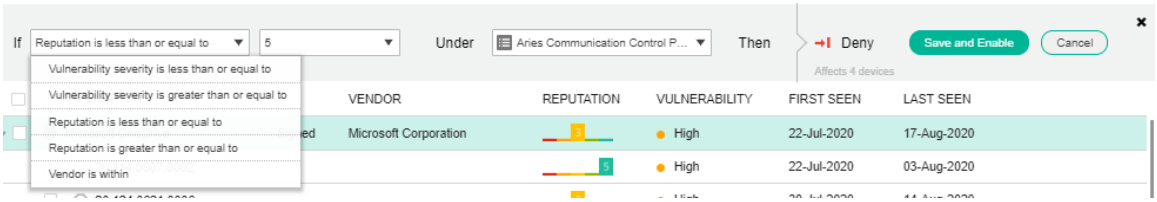


2.3.7 Políticas de aplicaciones

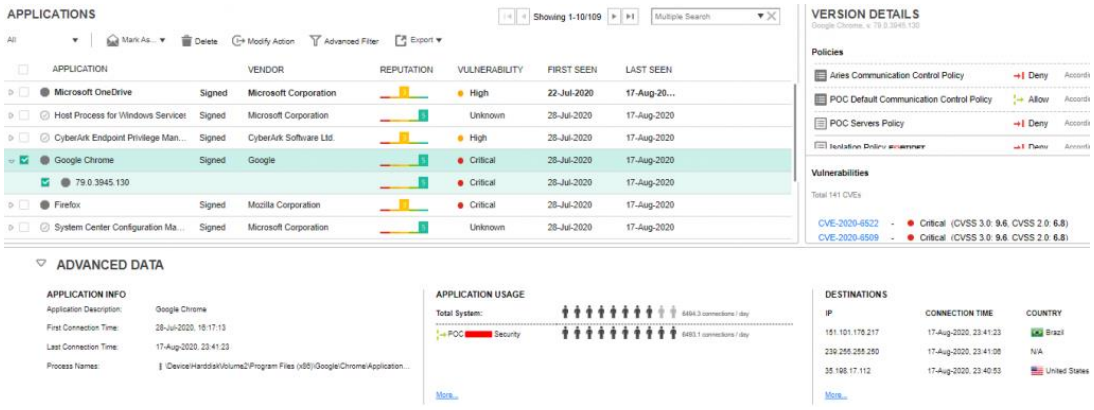
Se pueden aplicar políticas para denegar ó permitir el uso de ciertas aplicaciones.



Las reglas de aplicaciones se pueden aplicar usando condicionales bajo los siguientes criterios:



N° de CVE de la aplicación, ip de destino en función de las conexiones realizadas por la aplicación.



2.4 Cloud Service

El servicio en la nube FortiEDR Cloud Service (FCS) enriquece y mejora la seguridad del sistema realizando análisis e investigaciones profundos y exhaustivos sobre la clasificación de un evento de seguridad. El FCS es un servicio basado en la nube, compatible con GDPR y basado únicamente en software que determina la clasificación exacta de los eventos de seguridad y actúa en consecuencia basándose en dicha clasificación, todo ello con un alto grado de precisión.

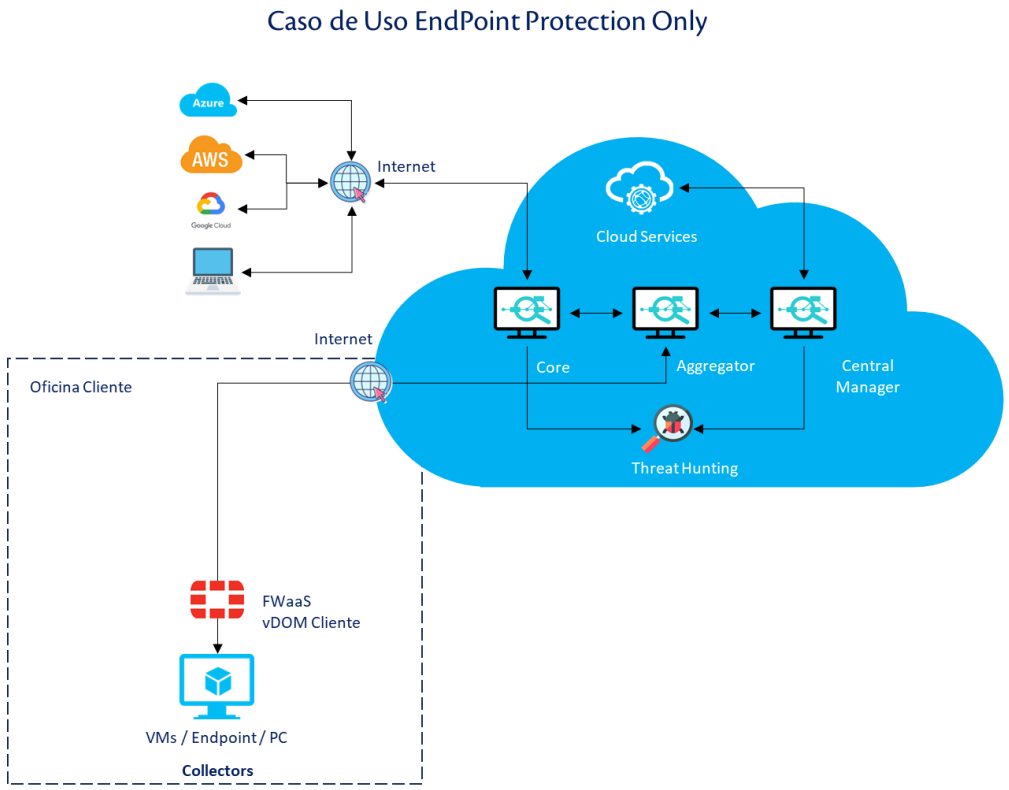
El proceso de clasificación de eventos de seguridad del FCS se realiza mediante el enriquecimiento de datos y un análisis e investigación mejorados, profundos y exhaustivos, habilitados por procesos automatizados y manuales. Los procesos mejorados pueden incluir (lista parcial) servicios de inteligencia, análisis de archivos (estáticos y dinámicos), sandboxing, análisis de flujos mediante aprendizaje automático, análisis de puntos en común, deducción de datos por crowdsourcing y mucho más.

Junto con la posible reafirmación o reclasificación de la clasificación, una vez conectados, los FCS también pueden permitir varias acciones de seguimiento, que pueden dividirse en dos actividades principales:

- Ajuste: Excepción automatizada de eventos de seguridad (allowlisting). Después de que un evento de seguridad activado se reclasifique como Seguro, se puede enviar una excepción automatizada entre entornos y caducar el evento, impidiendo que se active de nuevo.
- Acciones de Playbook: Todas las acciones de política de Playbook se basan en la determinación final del FCS.

*NOTA: Los ajustes y acciones descritas anteriormente están sujetas a configuraciones previas a que suceda el evento de seguridad.

2.5 Topología General de la Solución



2.6 Alcance del Servicio Administrado incluido

A continuación, se detallan los servicios administrados incluidos en todas las etapas del servicio Tigo EDR contratado por el cliente:

- **Instalación y puesta en marcha:** se implementa una muestra de hasta 10 estaciones de trabajo o end-points dentro de los tiempos pactados en los ANS y una vez entregada por parte del cliente la información requerida. El cliente se encarga de hacer la instalación de los agentes en las estaciones de trabajo. Esta instalación se puede hacer por medio de políticas de GPO o por medio de software de terceros. Este tiempo de instalación no cuenta dentro de los 10 días en los que el agente está

en modo supervisión. *Durante estos 10 días el agente o collector solo se hará notificación de eventos, no aplicara políticas de protección ni bloqueará conexiones del endpoint hasta que pase en el día 11 a modo protección.*

- Si en el momento de la implementación el cliente no solicita la configuración de todos los servicios adquiridos, la habilitación de los servicios que se soliciten posteriormente a la implementación inicial tendrá un cargo adicional no recurrente, correspondiente al Servicio Profesional necesario para implementar el o los servicios faltantes contratados.
- Los cambios solicitados por emergencia o contingencia de seguridad para mitigación de algún incidente reportado directamente por el cliente no se descontarán de los cambios mensuales incluidos.
- No se incluye reingeniería de políticas, análisis o rediseño del esquema de seguridad configurado a petición del cliente.

2.6.1 Gestión de colectores en plataforma EDR:

EL equipo de RSOC realizará el monitoreo del estado de los colectores desde el Central Manager y se dará gestión de acuerdo con la siguiente tabla:

Estado	Descripción	Gestión RSOC	Nota
Running	El collector está arriba y se encuentra funcionando de manera correcta.	No hay gestión, ni notificación de eventos ya que se encuentra funcionando de manera correcta.	Estado deseado de operación.
Running (Autonomously)	El Core está temporalmente inaccesible. Sin embargo, la aplicación de políticas la realiza el collector.	El RSOC validará el estado de los componentes de la plataforma EDR, específicamente el estado de los Cores.	En caso de que el estado o la disponibilidad de los Cores de la plataforma sea la correcta: *Estado Running*, es necesario ejecutar la rutina de *validación de conexión al Core.*

Disconnected	El Endpoint o host está offline (apagado o no tiene conexión con el agregador).	El RSOC notificará al cliente los Endpoints o hosts que lleven 3 o más días en estado de desconexión para la validación del estado de este.	En caso de que el Endpoint o host lleve 3 días desconectado y se reciba una respuesta del cliente donde el host está encendido, es necesario ejecutar la rutina de *validación de conexión al agregador.* En caso contrario la gestión es responsabilidad del cliente.
Disconnected (Expired)	El Endpoint o host no ha estado conectado durante 30 días o más consecutivos.	El RSOC notificará al cliente los Endpoints o hosts que lleven 30 o más días en estado desconectado.	La gestión es responsabilidad del cliente. La plataforma EDR liberará el licenciamiento del Endpoint o host.
Pending Reboot	Este estado significa que el Collector está listo para ejecutarse después de reiniciar el Endpoint o host.	La gestión del RSOC aplica solo para actualizaciones de collectores, donde se realizará con la respectiva notificación al cliente.	En fase de implementación el grupo de Delivery es el responsable de coordinar los reinicios y dejar el collector en estado *running*.
Disabled	El Endpoint o host ha sido deshabilitado desde el ***Central Manager*** de la plataforma.	El RSOC gestionará el requerimiento del cliente con su respectiva carta de riesgo o correo de aceptación de responsabilidad.	Es necesario limitar el tiempo que un Endpoint o host quedará deshabilitado. La responsabilidad de la seguridad del Endpoint o host es del cliente.
Degraded	Especifica que el collector no puede funcionar a su máxima capacidad (puede ser por la falta de recursos en el host o problemas de compatibilidad).	El RSOC notificará al cliente los Endpoints o hosts que estén degradados para dar pronta gestión y revisión.	El cliente validará el problema presentado a nivel de OS y/o compatibilidad con el collector, en caso de no encontrar la causa raíz el RSOC apoyará con la gestión del TAC del fabricante y la recolección de información del collector desde el *Central Manager*.

Isolation*	Identificación de procesos o archivos maliciosos en el endpoint o host.	Gestión de collectores en el grupo de *High Security Group* (HSG) donde el RSOC realizará la identificación e investigación del evento. Posterior al proceso de análisis, el RSOC notificará al cliente.	La gestión y alcance del RSOC es para políticas en modo protección (***Protection***). Si las políticas están en modo simulación (***Simulation***) es responsabilidad del cliente el proceso de remediación y recuperación.

Para contener las infecciones la plataforma EDR utiliza el modo de aislamiento (Isolation Mode) con políticas estrictas y control de comunicaciones a todas las aplicaciones para contener la amenaza. Una vez se activa el Isolation Mode el endpoint será asignado al grupo de collectores High Security Collector Group donde el RSOC realizará la identificación e investigación del evento.

Nota: Se utilizarán las notificaciones de usuario final (End-User) por medio de mensajes tipo pop-up con el objetivo de dar información sobre el estado del collector: Protection Off, Degraded y Isolation mode. Las notificaciones también van a servir para notificar si la plataforma EDR está realizando algún bloqueo de una aplicación autorizada y donde se hace necesario la configuración de una excepción, la cual es necesario gestionar por medio del proceso de gestión de solicitudes.

2.6.2 Actividades de upgrade o actualización de Colectores

Para las actividades o tareas con respecto a la actualización de los collectores se realizarán siguiendo las buenas prácticas recomendadas por el fabricante, primero manteniendo versiones actualizadas y estables del collector y segundo la ejecución de la actualización se realizará en grupos o lotes pequeños para realizar las respectivas pruebas de funcionamiento y compatibilidad de los Endpoints y la plataforma EDR. Para esta actividad el RSOC realizará la notificación al cliente de la necesidad de actualización con el propósito de construir un plan de actividades de acuerdo con las necesidades de la operación del cliente.

2.6.3 Gestión de Políticas de seguridad en la plataforma EDR

EL equipo RSOC realizará la configuración o clonación de políticas de seguridad, así como las configuraciones de las acciones para las reglas de acuerdo con la siguiente tabla:

Política	Descripción	Gestión RSOC	Nota
Execution Prevention	Esta política bloquea la ejecución de archivos identificados como maliciosos o que se sospecha que lo son. Para esta política, cada archivo se analiza para encontrar evidencia de actividad maliciosa.	Gestión de solicitudes para realizar cambios en las acciones de la política, así como el monitoreo de eventos de acuerdo con las detecciones de la plataforma EDR. Si es detectada una amenaza se procede a realizar el proceso de gestión de incidentes.	Monitoreo de eventos en el *Event Viewer* de acuerdo con las detecciones de la política configurada en la plataforma EDR y notificación de eventos cuya acción es Block y Log.
Exfiltration Prevention	Esta política permite a la plataforma EDR distinguir qué solicitudes de establecimiento de conexión son maliciosas.	Gestión de solicitudes para realizar cambios en las acciones de la política, así como el monitoreo de eventos de acuerdo con las detecciones de la plataforma EDR. Si es detectada una amenaza se procede a realizar el proceso de gestión de incidentes.	Monitoreo de eventos en el *Event Viewer* de acuerdo con las detecciones de la política configurada en la plataforma EDR y notificación de eventos cuya acción es Block y Log.
Ransomware Prevention	Esta política permite a la plataforma EDR detectar y bloquear malware que impide o limita el acceso de los usuarios a su propio sistema.	Gestión de solicitudes para realizar cambios en las acciones de la política, así como el monitoreo de eventos de acuerdo con las detecciones de la plataforma EDR. Si es detectada una amenaza se procede a realizar el proceso de gestión de incidentes.	Monitoreo de eventos en el *Event Viewer* de acuerdo con las detecciones de la política configurada en la plataforma EDR y notificación de eventos cuya acción es **Block** y **Log**.
Device Control	Esta política permite a la plataforma EDR detectar y bloquear el uso de dispositivos USB, como dispositivos de almacenamiento masivo USB.	Gestión de solicitudes para realizar cambios en las acciones de la política, así como el monitoreo de eventos de acuerdo con las detecciones de la plataforma EDR. Si es detectada una amenaza se procede a realizar el proceso de gestión de incidentes.	En esta política, la detección se basa en el tipo de dispositivo.

La plataforma EDR realiza la protección de los endpoints basada en sus políticas de seguridad, las cuales están compuestas por un conjunto de reglas y sus respectivas acciones, por lo tanto, las recomendaciones del RSOC siempre estarán basadas en la configuración de políticas restrictivas para minimizar el riesgo de infección. Es responsabilidad del cliente comprender el/los impacto(s) de la configuración(es) de acuerdo con sus necesidades de negocio u operación.

Para las políticas en modo simulación es importante que el cliente comprenda que la plataforma EDR no está aplicando ninguna protección sobre los endpoints o hosts. Sin embargo, la plataforma EDR permite la configuración de una regla cuya acción es dejar un log, el cual permite analizar el comportamiento de la política y ejecutar la respectiva gestión de eventos en el Event Viewer de la plataforma EDR.

Todas las configuraciones de políticas y sus reglas aplican para Grupos de Collectores en la plataforma EDR. No aplican para endpoints o hosts específicos.

2.6.4 Gestión de aplicaciones y control de comunicaciones en la plataforma EDR

EL RSOC realizará la configuración de políticas de control de comunicaciones, así como las configuraciones de las acciones para las reglas de acuerdo con la siguiente tabla:

Política	Descripción	Gestión RSOC	Nota
allowlist	La plataforma EDR verifica todas las comunicaciones externas que realizan las aplicaciones a nivel de red, por lo tanto, es posible configurar una lista de permitidos (*allowlist*) para que solo las aplicaciones de la lista tengan permitida una comunicación externa.	Gestión de solicitudes para realizar cambios en las acciones de la política, así como el monitoreo de eventos de acuerdo con las detecciones de la plataforma EDR. Si es detectada una amenaza se procede a realizar el proceso de gestión de incidentes.	Monitoreo de eventos en el *Event Viewer* de acuerdo con las detecciones de la política configurada en la plataforma EDR. Adicionalmente en el panel *Communication Control- Applications* es posible obtener información de la aplicación, detalle de la versión, estadísticas de uso y destinos de comunicación.
Por reputación	La plataforma EDR asigna un *reputation score* para las aplicaciones de la siguiente forma: Know bad (1) Trusted (5)	El monitoreo de eventos de acuerdo con las detecciones de la plataforma EDR. Si es detectada una amenaza se procede a realizar el proceso de gestión de incidentes.	Monitoreo de eventos en el *Event Viewer* de acuerdo con las detecciones de la política configurada en la plataforma EDR.

Por vulnerabilidad *	La plataforma EDR realiza una evaluación del riesgo basado en las vulnerabilidades conocidas CVE que pueda tener la aplicación entregando un score basado en el CVSS 2.0 y 3.0.	El monitoreo de eventos de acuerdo con las detecciones de la plataforma EDR. Si es detectada una amenaza se procede a realizar el proceso de gestión de incidentes.	Monitoreo de eventos en el *Event Viewer* de acuerdo con las detecciones de la política configurada en la plataforma EDR.
Por fabricante (vendor)	La plataforma EDR permite realizar configuraciones por fabricante (vendor).	El monitoreo de eventos de acuerdo con las detecciones de la plataforma EDR. Si es detectada una amenaza se procede a realizar el proceso de gestión de incidentes.	Monitoreo de eventos en el *Event Viewer* de acuerdo con las detecciones de la política configurada en la plataforma EDR.

La plataforma EDR proporciona visibilidad de cualquier comunicación o conexión que realiza las aplicaciones lo que permite establecer un conjunto de políticas donde el control de comunicaciones está basado en la reputación de la aplicación. Estas políticas se pueden configurar como un NGFW para bloquear automáticamente las comunicaciones de aplicaciones potencialmente no deseadas. Por ejemplo, aplicaciones con mala reputación o distribuidas por fabricantes cuestionables.

Adicionalmente, el control de comunicaciones proporciona datos y herramientas para una evaluación y control eficientes de las vulnerabilidades a nivel de aplicación; con la característica de virtual patching es posible bloquear automáticamente las conexiones de aplicaciones vulnerables.

2.6.5 Gestión de eventos en la plataforma EDR

El RSOC realizará el proceso de gestión de eventos de acuerdo con la clasificación y acción que realiza la regla configurada en la política de seguridad de la plataforma EDR y se procederá a realizar la gestión en el Event Viewer de acuerdo con la siguiente tabla:

Por Política	Descripción	Gestión RSOC	Nota
Execution Prevention Exfiltration Prevention Ransomware Prevention	Para los eventos de exfiltration (exfiltración) la plaforma EDR por defecto registra un evento cuando la acción es bloquear (Block).	RSOC realiza notificación al cliente ya que la plataforma esta detectando una comunicación sospechosa.	Monitoreo de eventos en el *Event Viewer* de acuerdo con las detecciones de la política configurada en la plataforma EDR y notificación de eventos cuya acción es Log.

Las notificaciones aplican para los eventos de seguridad critica, aplicaciones que realizan comunicaciones sospechosas o eventos donde es necesaria la gestión del cliente a nivel de los endpoints o hosts.

Por Clasificación	Descripción	Gestión RSOC	Nota
Malicious Suspicious Inconclusive	La plataforma EDR realiza la clasificación de los eventos con base en el análisis y detección de los componentes de la misma: Security Policies y Communication Control.	RSOC realiza notificación al cliente ya que la plataforma está detectando una comunicación sospechosa.	Monitoreo de eventos en el *Event Viewer* de acuerdo con las detecciones de la política configurada en la plataforma EDR y notificación de eventos cuya acción es Log.

2.6.6 Delivery o aprovisionamiento

A continuación, se describen las configuraciones de implementación incluidas en la entrega y gestión del servicio:

- incidentes no manejados
- vulnerabilidades criticas
- comunicaciones sospechosas

Se manejan 3 tipos de clasificación:

- Archivado
- No manejado
- Excepción

Aprovisionamiento:

- En la fase inicial la plataforma se configura en modo supervisión durante 10 días.
- Luego de la fase de supervisión la plataforma se implementa en modo protección.
- Sí se requiere integración al AD del cliente se debe implementar una máquina virtual (VM) con rol de core/Jumbox y con los siguientes recursos de cómputo: (No se incluye en la oferta)

FortiEDR Core ejecutado como Jumpbox	Recurso
RAM(GB)	16Gb
vCPU	4
Storage(HD)	250GB

Consideraciones: Aplica para las siguientes modalidades o casos de uso:

- La retención de logs se realiza de forma centralizada en la infraestructura cloud por 1 mes, para mayor retención de logs se debe comprar Add-On de Disk Expansión (512 GB storage). No incluido en esta oferta
- El plazo máximo contemplado para el suministro de información de implementación es de 96 horas o 4 días hábiles, si no se recibe la información se configurarán valores estándar sujetos a buenas prácticas por parte de Tigo.
- Los 10 días del modo supervisión cuentan a partir del momento en el que el agente queda instalado y aprovisionado en la máquina del cliente.
- El reporte por incluido en el servicio es el reporte ejecutivo.
- Si los cambios solicitados requieren análisis preventa, dependerá de este análisis si se requiere realizar un pago adicional por implementación, licenciamiento, actualización.
- Cada solicitud de gestión de cambio se deberá generar un ticket de atención, para contabilizar como una unidad de cambio dentro del plan contratado, a pesar de que en el ticket pueda haber configuraciones distintas solicitadas.
- Proveer reportes semanales de la cantidad de gestiones de cambio que se ha utilizado por cada cliente como también los disponibles a la fecha.
- El jumpbox es requerido únicamente para aquellos casos donde el cliente requiere integraciones con plataformas de red que no están publicadas en internet como el directorio activo, por ejemplo.

2.6.7 Monitoreo e Informes

- Los servicios administrados incluyen en el monitoreo el seguimiento 7x24 a las alertas de seguridad con severidad alta y/o critica. Todas las alertas de tipo información o severidad baja son descartadas.
- Los servicios administrados incluyen en los informes automáticos mensuales los incidentes de seguridad de la solución.
- Informe de Seguridad: Comprende estadísticas y comportamiento del tráfico asociado a los controles aplicados a través de los Servicios de Tigo EDR contratados.

- El reporte por incluido en el servicio es un reporte ejecutivo

2.6.8 Servicios Administrados ante Fallas

La solución de Tigo EDR cuenta con los siguientes criterios de atención ante fallas en la prestación del servicio contratado:

SLA Regional (NOC, DOC, SOC) / Nivel 2	
Clasificación SLA	Tiempo Atencion
Menor	24 horas
Moderado	4 horas
Significativo	2 horas

*Esto considera atención remota, para atención en sitio se contempla más abajo en el ANS On-premise.
*El tiempo se empieza a considerar desde el momento en el que el cliente reporta la falla mediante tiquete.

Impacto	Inicio de la solución	Tipo de Atención	Horario de Atención
Significativo	Inmediato	Conexión remota, telefónica, correo	Lunes a domingo de 00:00 a 23:59 horas.
Moderado	Inmediato		
Menor	4 horas		

2.6.9 Atención Especializada

Soporte para Gestión de Incidentes

Un Incidente es una interrupción no planificada de un servicio de TI/Telecomunicaciones o una reducción en la calidad de este. La falla de un elemento de configuración que aún no ha afectado al servicio también puede ser considerada un incidente.

La prioridad asignada por Tigo a cada incidente reportado se define de acuerdo con el impacto sobre el servicio, el tipo de atención requerida y el portafolio del Cliente. Esta prioridad será definida por Soporte Técnico con base en la información suministrada por el Cliente sobre el incidente.

El Impacto determina la importancia del incidente dependiendo de cuanto éste afecta a los procesos de negocio y/o del número de usuarios afectados. La siguiente tabla ilustra las características que se analizan para definir el impacto del incidente sobre el servicio:

Criterios de falla	Impacto
2 o más Intermitencias de servicio en dónde el período de afectación acumulado sea superior o igual a 30 minutos, en un día.	Significativo
Problema mayor o incidente muy serio que compromete o detiene al negocio	
Caída total del servicio	
Degradación de los servicios hasta el punto de que no puedan ser utilizados.	
2 o más Intermitencias de servicio en donde el período de afectación acumulado en un día sea menor a 30 minutos	Moderado
Problema significativo que ocasiona que los servicios estén degradados, genera un impacto limitado al negocio y afecta la productividad seriamente.	
Degradación de los servicios sin afectación total del mismo.	
No afecta ni degrada la prestación del servicio, se incluyen eventos en monitoreo.	Menor
Problema que causa ineficiencias en los procesos normales del negocio y no tienen un impacto cuantificable o significativo	
Gestión de cambios en políticas, nuevas políticas, solicitud de información. Solicitud de reconfiguración, reporte o consulta.	
Intermitencias esporádicas con periodicidad de uno o más días y con duración menor a 5 minutos	

2.7 Implementación y/o transición

2.7.1 Metodología de aprovisionamiento

Para llevar a cabo la entrega de una solución operativa al cliente, Tigo asigna un Project Manager responsable de canalizar las necesidades y comunicaciones del cliente e integrar tecnológicamente los proveedores y aliados requeridos.

El Project Manager utiliza metodologías y herramientas de gestión de proyectos para realizar el aprovisionamiento de la solución. En el inicio y planificación del proyecto, analiza el alcance de la solución, identifica los riesgos y controles del proyecto, solicita los recursos requeridos y construye el plan de trabajo asociado.



2.7.2 Tiempo de aprovisionamiento

La duración del aprovisionamiento es de 45 días calendario, a partir del perfeccionamiento del contrato y de la reunión de inicio. Estos tiempos dependen de la modalidad o caso de uso seleccionado por el cliente.

Consideraciones

- En todo caso se realizará el mejor esfuerzo para tener implementado el servicio en el menor tiempo posible.
- Para la instalación de enlaces nuevos no se consideran los tiempos imputables a permisos con entidades municipales y locales de energía, iluminación, entre otras.
- En cualquier modalidad de la solución en la nube de Tigo, se cuenta con factibilidad previa para realizar el despliegue en los tiempos aquí establecidos

2.7.3 Entregables

Entregable	Descripción
Acta de entrega	Documento donde se realiza verificación y entrega de cantidad, calidad y operatividad de la solución de acuerdo con lo establecido en la oferta técnica.

Nota: Se podrá pactar entregas parciales de acuerdo con cronograma definido con cliente.

2.8 Propuesta Económica

Se relaciona la propuesta económica con la tarifa mensual y con el proyecto a 12 meses.

Descripción	Meses	Cantidad	Valor Unitario	Valor Mensual	Valor 12 meses
Licenciamiento FortiEDR para 1000 endpoints	12	1000	$13.000	$13.000.000	$156.000.000
Total, Mensual antes de IVA				$13.000.000	$156.000.000
Moneda				**Pesos Colombianos (COP)**	

2.9 Roles y Responsabilidades

Se relacionan los roles y responsabilidades de Tigo y del cliente requeridos durante el aprovisionamiento de la solución:

Actividad	Tigo	Cliente
Evaluación inicial de seguridad	X	
Instalación del agente EDR en endpoints	X	
Configuración de políticas de seguridad	X	
Monitoreo continuo de amenazas	X	
Análisis de incidentes de seguridad	X	
Respuesta a incidentes de seguridad	X	
Actualización de la base de datos de amenazas	X	
Soporte técnico para problemas de agente EDR	X	
Reportes mensuales de estado y seguridad	X	
Gestión de vulnerabilidades	X	
Revisión y ajuste de políticas de seguridad	X	
Soporte y garantía	X	
Formación y concienciación de seguridad para empleados		X
Coordinación de accesos y permisos		X
Soporte técnico para problemas de endpoints y Sistema Operativo		X
Gestión del cambio en la infraestructura de TI		X
Gestión y Soporte en la infraestructura LAN		X
Provisión de infraestructura de red y conectividad		X
Suministro de información sobre la infraestructura de TI		X
Facilitar el acceso físico y remoto a los equipos		X
Notificación de cambios en la infraestructura de TI		X
Participación en simulacros y pruebas de recuperación		X
Colaboración en la implementación de recomendaciones de seguridad		X

2.10 Consideraciones generales:

Hace parte de la presente oferta las siguientes consideraciones a efectos de establecer el alcance de las actividades y compromisos de las partes para la adecuada prestación de los servicios contratados:

1.Definiciones:

Incidente de seguridad digital: Ocurrencia de una situación que pone en peligro la confidencialidad, integridad o disponibilidad de un sistema de información o la información que el sistema procesa, almacena o transmite; o que constituye una violación a las políticas de seguridad, procedimientos de seguridad o políticas de uso aceptable.

Infraestructura crítica cibernética: Sistemas y activos, físicos o virtuales, soportados por Tecnologías la Seguridad de la Información, cuya afectación significativa tendría un impacto grave en el bienestar social o económico de los ciudadanos, o en el funcionamiento efectivo del gobierno o la economía.

Ciberseguridad: Es el proceso de proteger los activos de información por medio del tratamiento de las amenazas a la información que es procesada, almacenada y/o transportada a través de sistemas de información interconectados.

Incidente de Seguridad: Es un evento inesperado y no deseado que compromete la Seguridad de la Información.

Evento de seguridad: Un evento de seguridad de la información indica que el sistema, la seguridad o los servicios de red y de infraestructura han sido comprometidos o vulnerados. Esto indica que los controles implementados han fallado y/o que no se ha seguido la política de seguridad de la información de la organización

Cualquier ocurrencia relacionada con los activos o el entorno que indique un posible compromiso de las políticas o la falla de los controles, o incluso una situación no asignada que pueda afectar a la seguridad.

LIMITACIONES DE RESPONSABILIDAD:

TIGO BUSSINESS no será responsable por la prestación del servicio en los siguientes eventos:

1. Cuando las interrupciones, caídas, problemas o deficiencias en los servicios o afectación de indicadores tengan origen en la infraestructura física y tecnológica del CLIENTE.
2. En los eventos de errores, decisiones, cambios en procesos y procedimientos por parte de EL CLIENTE que no hayan sido oportunamente informados al SOC.
3. En aquellos casos en los cuales los sistemas, plataformas y aplicativos del CLIENTE que no hagan parte de los sistemas, servicios o componentes de los servicios Ciberseguridad contratados, y éstos tengan falencias de seguridad que faciliten eventos de fraudes, hayan sido o no detectadas y/o advertidas por TIGO BUSINESS.
4. Por fuerza mayor o caso fortuito.

En caso de presentarse suspensión o afectación del servicio por cualquiera de los eventos señalados en los numerales 1 ,2 y 3 el cliente asumirá los costos en los que incurrió TIGO BUSSINESS , por la no prestación del servicio, durante el período de tiempo que dure la suspensión o afectación del mismo.

OBLIGACIONES ADICIONALES DEL CLIENTE:

EL CLIENTE deberá realizar copias de seguridad de su información en el medio que considere pertinente.

EL CLIENTE es el directo responsable de la Información que se ingrese procese, genere y mantenga en relación del uso de sus equipos y servicios de CIBERSEGURIDAD y deberá garantizar el cumplimiento adecuado y oportuno de la implementación de las mejores prácticas que el equipo de SOC , NOC remoto le informe.

El cliente será responsable de implementar las configuraciones y demás recomendaciones que le entregue TIGO BUSINESS en aras de cumplir con el alcance de los servicios ofrecidos. En caso que éstas no sean debidamente implementadas en su totalidad, TIGO BUSINESS no será responsable de los efectos, vulnerabilidad, amenazas o efecto adverso que se derive de esta situación.

Es responsable de autorizar la contención de los riesgos detectados y notificados; de no autorizar la contención, TIGO no será responsable de los riesgos o la posible materialización de un evento de seguridad.

REGIMEN DE RESPONSABILIDAD

Igualmente y tratándose de Servicios Administrados de Ofimática, Conectividad, Voz y Colaboración, Movilidad, Infraestructura de TI, Cloud, Data Center, Servicios Administrados y Seguridad, TIGO BUSSINESS no garantiza resultado alguno por los usos y/o aplicaciones específicos que realice EL CLIENTE y de manera particular por: (a) Interrupciones de los servicios originadas en causas ajenas a su control, tales como: mal funcionamiento de Internet, problemas satelitales, interrupción o insuficiencia de energía eléctrica, huelgas, desastres naturales, conflictos bélicos, actos de la autoridad, etc.; (b) pérdida de datos almacenados en el servidor, ya sea por causas imputables al CLIENTE, por fallas en el sistema, por eventos o incidentes de seguridad perpetuados por terceros (por ejemplo ataques de denegación de servicio, virus, malware, ransomware, entre otros) que comprometan la integridad, confidencialidad o la disponibilidad de la información o por actualización de los servidores; (c) demoras en los trámites de Registro de Dominio y transferencias de DNS por causas imputables al CLIENTE o a terceros; (d) por fraude cometido por El CLIENTE o por terceros; (e) por fallas de tipo técnico tales como la seguridad informática de los ambientes en hosting, cloud y de soluciones de terceros atribuibles al CLIENTE o a terceros; (f) en caso de ataques informáticos a los PBX por causas imputables al CLIENTE. En caso de que en la Orden de Compra y/o Servicio se incluya la entrega al CLIENTE de cuentas administradoras de cualquier servicio, EL CLIENTE exime a TIGO BUSSINESS de cualquier evento de indisponibilidad, seguridad y confidencialidad que pueda ocurrir. Adicionalmente, en los casos en que EL CLIENTE solicite deshabilitar y/o desinstalar las herramientas de Antivirus implementadas por TIGO BUSSINESS o por un tercero para proteger los servicios, EL CLIENTE exime a TIGO BUSSINESS de cualquier evento de indisponibilidad, seguridad, confidencialidad, virus, malware, ransomware o cualquier otro software malicioso que pueda generar algún tipo de afectación durante la prestación del servicio. Esto aplica para cualquier servicio que se pueda afectar con la deshabilitación solicitada. Parágrafo: Cuando se trate de servicios de Cloud para distribuidores o revendedores, TIGO BUSSINESS no será responsable de la prestación o suministro de servicios (venta, aprovisionamiento, soporte técnico, licenciamiento y demás) frente al cliente final.

Exclusión de responsabilidad por daños indirectos y otros. Sin perjuicio de los casos en que la ley aplicable prohíba la limitación de responsabilidad por daños, TIGO BUSINESS no se responsabilizará en ningún caso de daños directos e indirectos, cualquiera que sea su naturaleza u origen incluidos, entre otros los daños por lucro cesante, pérdida de la información confidencial o de otro tipo, interrupción de negocios, pérdida de privacidad, incumplimiento de obligaciones (ya sea de buena fe o con diligencia razonable, negligencia y cualquier perdida pecuniaria o de otro tipo)], que se deriven o de otro modo este relacionados con la materialización de un incidente de seguridad. Tigo BUSINESS se excluye expresamente cualquier responsabilidad por falta de disponibilidad del servicio y/o de equipos del CLIENTE en un momento

determinado, ya sea por causas técnicas, tareas de mantenimiento del sistema no notificadas al SOC, falla eléctrica en las instalaciones del CLIENTE y todas aquellas que estén bajo su control y gestión.

3. COMPROMISOS DEL CLIENTE

3.1 Responsabilidades del cliente

ESU – Empresa para la Seguridad y Soluciones se compromete a garantizar el suministro, exactitud y completitud de toda la información requerida por Tigo. Si la información es incompleta o incorrecta, cualquier retardo o requisito adicional que pueda generarse para corregir los problemas originados por el uso de tal información incompleta o inexacta será tratado como una solicitud de cambio del cliente al alcance del servicio, por lo tanto, estará sujeta al proceso de control de cambios, lo que implica una nueva factibilidad y posibles costos adicionales.

3.2 Acuerdo de confidencialidad

La información oral, escrita, gráfica, en lenguaje de máquina, o en cualquier otra forma conocida o no, incluyendo, pero sin limitarse a documentos, catálogos, cartas, correos electrónicos, memorandos, fórmulas, estadísticas, presentaciones que Tigo ponga en conocimiento del cliente en esta oferta se entiende que tiene un carácter eminentemente confidencial, en consecuencia, el cliente tendrá las siguientes obligaciones frente a la misma:

- Mantener la reserva de la información, y tomar todas las medidas razonables para protegerla, incluyendo, pero sin limitarse, todas las precauciones que el cliente utiliza respecto de su información confidencial.
- Abstenerse de usar, facilitar, divulgar o revelar, sin causa justificada y sin consentimiento de Tigo, cualquier información entregada o derivada de la misma, a cualquier tercero, o ponerla a su disposición o para su beneficio.