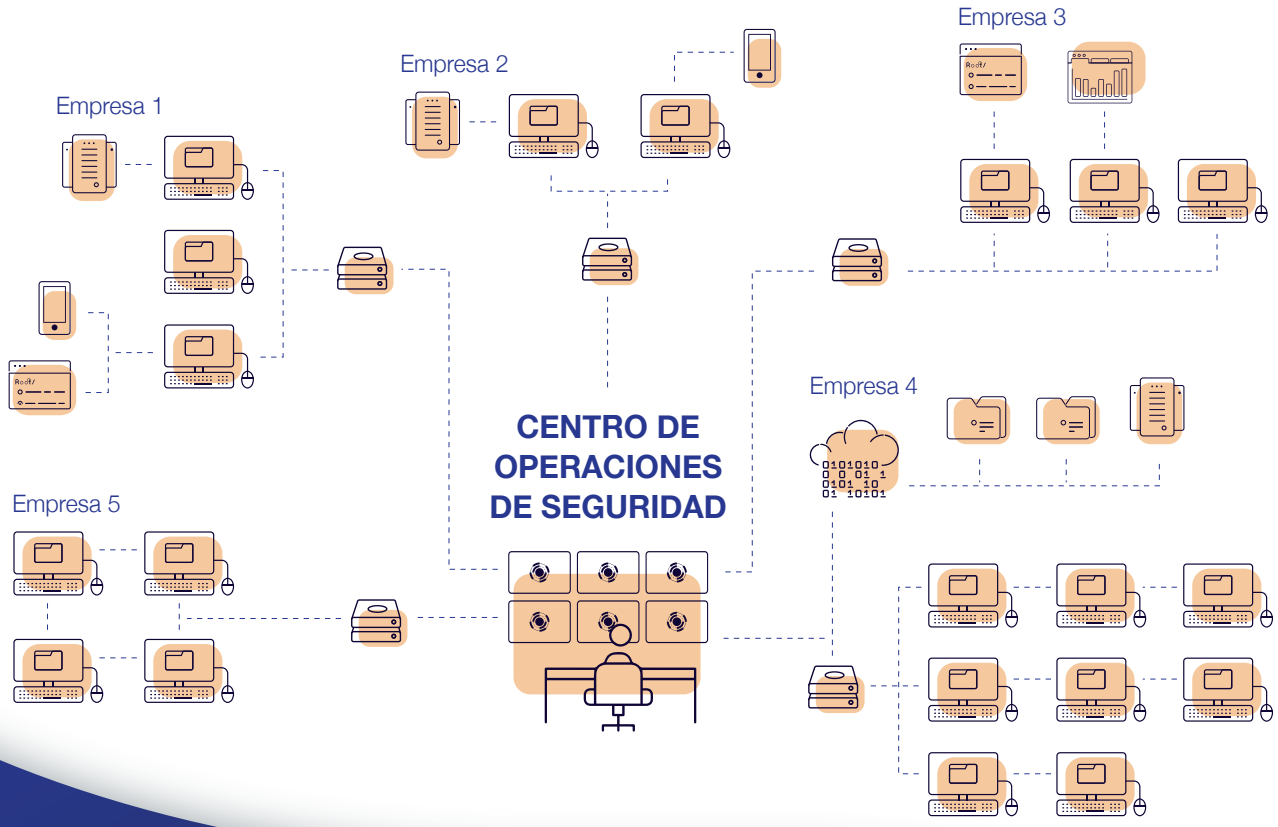
HYPATIA

SOLUCION INTEGRAL PARA LA GESTION TOTAL DE LA **CIBERSEGURIDAD**

Identificación, análisis y tratamiento
de los riesgos informáticos de un negocio

HYPATIA es un servicio para pymes y organizaciones que **detecta y previene amenazas cibernéticas**

El centro de operaciones de seguridad de HYPATIA monitoriza la seguridad de la red informática. Maneja una gran cantidad de datos que procesa y analiza para **actuar con rapidez ante situaciones de riesgo** o compromiso.



VENTAJAS

- **Control integral de la red informática** para identificar acciones sospechosas.
- Gestion de incidentes de seguridad para minimizar el impacto de forma rápida.
- **Búsqueda de amenazas sobre los activos** (servidores, ordenadores, aplicaciones, bases de datos, web…), por medio de diferentes técnicas de cribado y análisis de los eventos recibidos.
- Prevención de ataques de red mediante la identificación de vulnerabilidades.
- **Estudio detallado del tráfico interno de una red** en busca de movimientos laterales, usuarios maliciosos…
- **Escaneo de todo tipo de redes IT / OT.**
- Observamos y **comprobamos el cumplimiento de los principales marcos de seguridad** IT / OT (ISO, NIST, PCI, NERC CIP…)

SERVICIOS OFRECIDOS

	RED IT	RED OT
Control, identificación y análisis de incidentes de ciberseguridad utilizando **soluciones tecnológicas avanzadas y acciones diferenciales**	✓	✓
Descubrir y priorizar amenazas que puedan comprometer los servicios de las infraestructuras o los accesos a los datos	✓	✓
Escaneo de la actividad en redes, servidores, puestos de trabajo y periféricos para chequear su seguridad	✓	✓
Vigilancia y supervisión de sistemas operativos, bases de datos, aplicaciones y sitios web	✓	✓
Protección de servicios implementados en la nube y de todos aquellos equipos que funcionen en modalidad de teletrabajo	✓	✓
Detectar comportamientos irregulares que puedan indicar un incidente de seguridad o compromiso aprovechando las fuentes de inteligencia de amenazas	✓	✓
Contención temporal y solución de ataques informáticos	✓	✓
Operaciones de control y actualización de la **defensa perimetral**	✓	✓
Descubrimiento en tiempo real de software malicioso de control remoto	✓	✓
Visibilidad completa del **entorno industrial y redes ICS**		✓
Detección proactiva de cambios en los sistemas de control industrial		✓
Protección de sistemas SCADA, PLC, DCS, IED, HMI, etc.		✓
Cumplimiento de **mandatos de seguridad**	✓	✓
Informes periódicos de la actividad de usuarios y los eventos de seguridad registrados	✓	✓

Redes IT: hace referencia a las tecnologías de la información (equipos de oficina)
Redes OT: hace referencia a las tecnológicas de la operación (equipos de control industrial)

TARIFAS

	RED IT	RED OT
AUDITORÍA TÉCNICA DE SEGURIDAD	Desde 2.500€	
CUOTA MENSUAL POR DISPOSITIVO/IP	5,99€	6,99€

CONDICIONES:

- HYPATIA se instala sobre una máquina virtual o un appliance.
- Compromiso mínimo de contratación del servicio: 12 meses.
- Cuota mensual, trimestral, semestral o anual.
- IVA no incluido en los precios.

CUÁLES SON LAS FASES DE UN ATAQUE INFORMÁTICO

1

RECONOCIMIENTO

El atacante recopila información sobre su objetivo: publicaciones en abierto, redes sociales e interacciones por email, e indaga sobre la tecnología que utiliza.

2

PREPARACIÓN

Ataque específico. Por ejemplo, el atacante crea un documento PDF y lo incluye en un correo electrónico, suplantando la identidad de una persona legítima.

3

DISTRIBUCIÓN

Transmisión del ataque. Por ejemplo, mediante la apertura del documento infectado enviado por correo electrónico o accediendo a un *phishing* (suplantación de identidad).

4

EXPLOTACIÓN

Se compromete al equipo infectado y a la red a la que pertenece.

5

INSTALACIÓN

El atacante instala el virus a la víctima. Puede darse la circunstancia de que no se requiera instalación, como en el caso del robo de credenciales.

6

COMANDO Y CONTROL

Vigilancia del sistema de la víctima. Sustrae credenciales, toma capturas de pantalla, se lleva documentación confidencial, instala programas, conoce la red del usuario...

7

ACCIONES SOBRE LOS OBJETIVOS

El atacante se hace con los datos e intenta expandir su acción maliciosa hacia más objetivos.

HYPATIA actúa antes de que suceda un ataque descubriendo las posibles brechas de seguridad. Una vez que se produce detecta movimientos sospechosos en la red informática evitando que consigan sus objetivos.

HYPATIA
POWERED BY
ABF
CIBERSEGURIDAD
y SISTEMAS