# ANÁLISIS Y GESTIÓN DE AMENAZAS

## Disminuya los riesgos de ataques informáticos de forma proactiva a través de medidas preventivas periódicas

Durante los últimos años, las amenazas de seguridad presentes en las redes empresariales han aumentado de forma continua, junto con los riesgos asociados a ellos. Actualmente, amenazas como botnet, ransomware y phishing pueden llegar a afectar seriamente la operación normal de una organización llegando incluso a ser fuente de pérdidas financieras para las empresas.

Para responder a estas preguntas IIA entrega un servicio mensual de Análisis de Vulnerabilidades y Amenazas que permita reconocer los activos informáticos más importantes, determinar las vulnerabilidades a las que se está expuesto y recomendar acciones que ayuden a mitigar el riesgo.

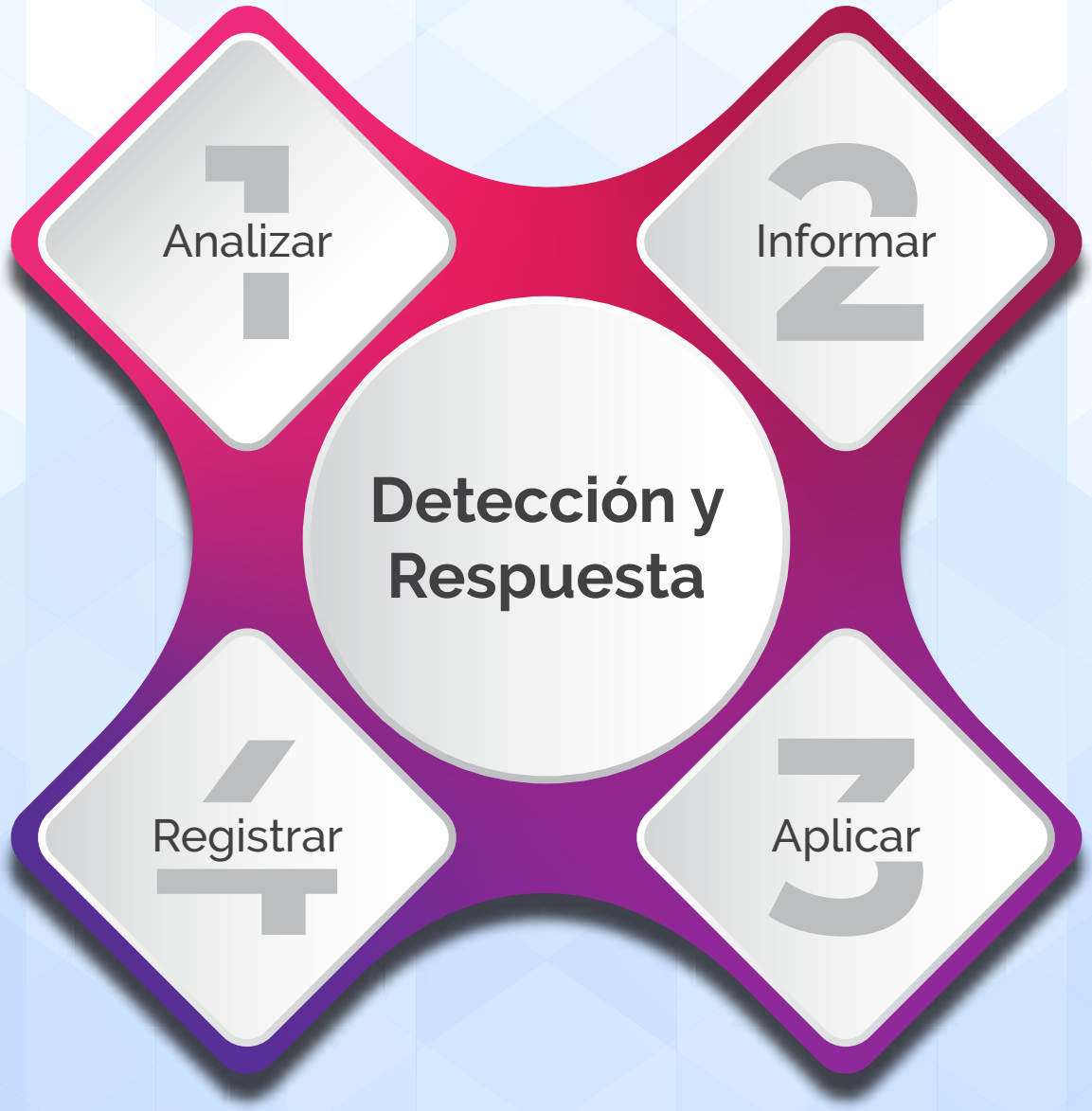
Este servicio se hace cargo de la necesidad de las empresas para:


En una primera fase de habilitación se ejecuta un Análisis de Ciberseguridad de la Red para identificar activos críticos, determinar vulnerabilidades y gestionar acciones de mitigación inicial.

En la fase de ejecución, el servicio recolecta información permanente del tráfico de Firewall generando reportes semanales de Amenazas de Seguridad presentes en la red. Estos reportes son analizados por personal capacitado para determinar el riesgo de las amenazas detectadas y genera recomendaciones semanales en forma de tareas específicas a ser realizadas por los encargados de los activos afectados. El servicio agrega la gestión de seguimiento de las tareas recomendadas junto con un Informe de Gestión Mensual presentado a los cargos directivos y encargados de TI de la organización.

## Detección y gestión preventiva de amenazas

El servicio está orientado a la prevención, de tal forma que las amenazas vayan disminuyendo en el tiempo, y que posibles nuevas amenazas tengan un impacto limitado al ser detectadas y mitigadas en plazos razonables.



## 1. Identificación de activos críticos

Primero, se lleva a cabo una evaluación que permita identificar los activos críticos en la red. Realizando escaneos de la red en conjunto con entrevistas a los responsables de la operación se determinan cuáles son los elementos críticos de los sistemas TI que podrían dañar el negocio en caso de no estar disponibles. Las aplicaciones o sistemas pueden ser desde ERP, sistemas contables o de facturación hasta estaciones de trabajo de personal crítico.

## 2. Recolección de Información

Luego de identificar los activos críticos se lleva a cabo La etapa de recolección de información relevante para el análisis. En esta etapa se usan herramientas que recolectan información durante un período de tiempo para luego ejecutar reportes que apoyan la labor de análisis. También se obtienen las versiones de firmware, Sistema Operativo y Software que se están ejecutando, así como las configuraciones que están operando.

## 3. Análisis de la información

Con la información disponible, se realiza un análisis para identificar las vulnerabilidades que se detectan en los sistemas y software que están operando en la red. Se determina el nivel de exposición que tiene cada una de estas vulnerabilidades y por último se estima el impacto que estas vulnerabilidades pueden llegar a tener. Esto permitirá al cliente tener una visión específica del grado de riesgo a la que sus activos están expuestos y cuáles sistemas son los que se deben priorizar.

## 4. Reporte y documentación de descubrimientos

La etapa final del proceso se refiere a documentar los descubrimientos obtenidos en cada etapa del proceso de tal forma que el cliente pueda usar la información para revisar sus procedimientos y sistemas de seguridad presentes. El reporte incluye también recomendaciones de acuerdo con las vulnerabilidades encontradas, de tal forma que el cliente pueda tomar medidas de mitigación adecuadas que eviten que las vulnerabilidades sean explotadas.

## Servicio de Análisis y Gestión de Amenazas

| Ítem | Entregable |
|---|---|
| **Análisis de Ciberseguridad de la Red** | Reporte de:<br>•Activos críticos<br>•Vulnerabilidades identificadas<br>•Priorización según riesgo<br>•Recomendaciones |
| **Recolección y Archiving en Fortianalyzer** | •Tráfico Sospechoso<br>•Amenazas Críticas<br>•Aplicaciones de alto riesgo |
| **Informe semanal con recomendaciones** | •Plan de mitigación<br>•Tareas específicas a responsables de activos |
| **Gestión y Seguimiento de recomendaciones** | •Gatillar acciones de mitigación requeridas<br>•Seguimiento de aplicación de tareas y recomendaciones<br>•Determinar cambios en el plan de acción inicial |
| **Reunión de seguimiento Mensual** | •Informe de gestión ejecutiva<br>•Informe de Riesgos de seguridad no resueltos<br>•Recomendaciones adicionales |

**CONTÁCTENOS**

Para más información 228401000 - División Internet

30 AÑOS | Generando soluciones TI integrales para su empresa