

# Análisis y Gestión de Amenazas

SERVICIOS DE CIBERSEGURIDAD



# ANÁLISIS Y GESTIÓN DE AMENAZAS

## INTRODUCCIÓN

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.

En este contexto, las empresas requieren establecer un fundamento que les permita entender:

- **¿Qué necesito proteger?**
- **¿Cuáles son las vulnerabilidades que pueden afectar mi negocio?**
- **¿Soy capaz de responder a estas amenazas?**

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:

- **Identificar** los riesgos presentes en activos informáticos
- **Analizar y priorizar** las vulnerabilidades detectadas
- **Recomendar** acciones concretas para mitigar los riesgos
- **Mantener y gestionar** un plan de acción permanente
- Contar con **personal entrenado** para estas acciones

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.

## ¿POR QUÉ IIA?

### CONFIANZA

Más de 30 años de experiencia apoyando a las empresas chilenas, entregando **confiabilidad y privacidad** a cada uno de nuestros clientes en el mercado de las Tecnologías de la Información. Desde armado de equipos, informática, Ingeniería e Internet hasta servicios de Datacenter y Seguridad de la Información, logrando así un proceso que cuenta con el respaldo de una empresa experimentada.

Más de 3.000 empresas avalan nuestra trayectoria y dedicado compromiso en lo que hacemos.

### EXPERIENCIA

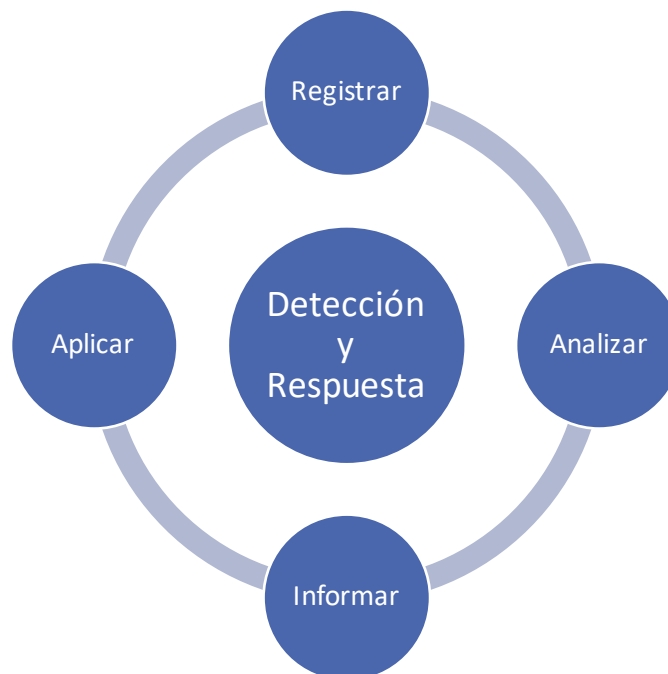
IIA posee **certificación ISO27001** vigente por más de 5 años consecutivos, lo que asegura al cliente experiencia necesaria **aplicando sistemas de gestión, buenas prácticas de seguridad informática**, así como la mejora continua de sus procesos y en el manejo de información crítica para nuestros clientes.

### KNOW-HOW

IIA cuenta con **personal capacitado y herramientas líderes** usadas en el rubro para reconocer las últimas vulnerabilidades conocidas y para intentar explotarlas de forma que nuestros clientes puedan aplicar las recomendaciones necesarias para proteger sus redes, sistemas y aplicaciones.

## 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.

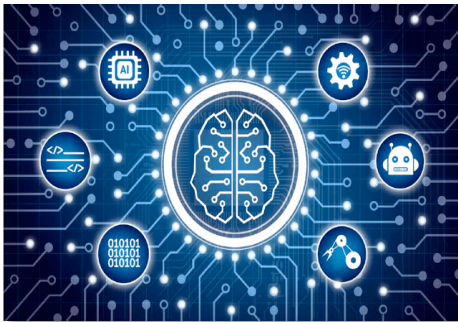


## IDENTIFICACIÓN



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.

## RECOLECCIÓN



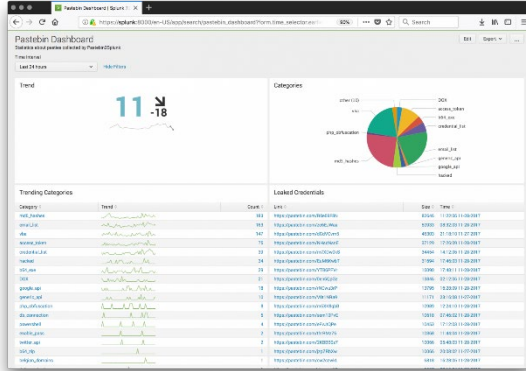
Luego de identificar los activos críticos se lleva a cabo la etapa de recolección de información relevante para el análisis. En esta etapa se usan herramientas que recolectan información durante un período de tiempo para luego ejecutar reportes que apoyan la labor de análisis. También se obtienen las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

## ANÁLISIS



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.

## REPORTE



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

Item	Entregable
<b>Análisis de Ciberseguridad de la Red</b>	Reporte de: <ul style="list-style-type: none"> <li>• Activos críticos</li> <li>• Vulnerabilidades identificadas</li> <li>• Priorización según riesgo</li> <li>• Recomendaciones</li> </ul>
<b>Recolección y Archiving en Fortianalyzer</b>	<ul style="list-style-type: none"> <li>• Tráfico Sospechoso</li> <li>• Amenazas Críticas</li> <li>• Aplicaciones de alto riesgo</li> </ul>
<b>Informe semanal con recomendaciones</b>	<ul style="list-style-type: none"> <li>• Plan de mitigación</li> <li>• Tareas específicas a responsables de activos</li> </ul>
<b>Gestión y Seguimiento de recomendaciones</b>	<ul style="list-style-type: none"> <li>• Gatillar acciones de mitigación requeridas</li> <li>• Seguimiento de aplicación de tareas y recomendaciones</li> <li>• Determinar cambios en el plan de acción inicial</li> </ul>
<b>Reunión de seguimiento Mensual</b>	<ul style="list-style-type: none"> <li>• Informe de gestión ejecutiva</li> <li>• Informe de Riesgos de seguridad no resueltos</li> <li>• Recomendaciones adicionales</li> </ul>

Para más información contáctenos y solicite un presupuesto formal

**CONTACTAR**

228401000 – División Internet

**30 AÑOS**

Generando soluciones integrales para su empresa

