Evaluación de Ciberseguridad de la Red

SERVICIOS DE CIBERSEGURIDAD

EVALUACIÓN DE CIBERSEGURIDAD DE LA RED

INTRODUCCIÓN

La seguridad informática continúa creciendo debido a la **dependencia** que tienen las empresas de las **tecnologías de procesamiento de la información**. Estas tecnologías **administran información crítica** para las organizaciones y deben asegurar que la información **está completamente íntegra**, **tiene niveles de confidencialidad adecuados** y **está disponible cuando se requiera**.

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 lleva adelante un Análisis de Seguridad de la Red 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 identifica activos informáticos, recolecta la información relevante durante un período de tiempo, analiza la información y recomienda acciones que apoyen a disminuir o eliminar de forma significativa el riesgo a los que está expuesta la red.

El servicio evacuará un **reporte** que le permitirá al cliente **identificar activos, conocer las vulnerabilidades y corregir los problemas encontrados.**

¿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

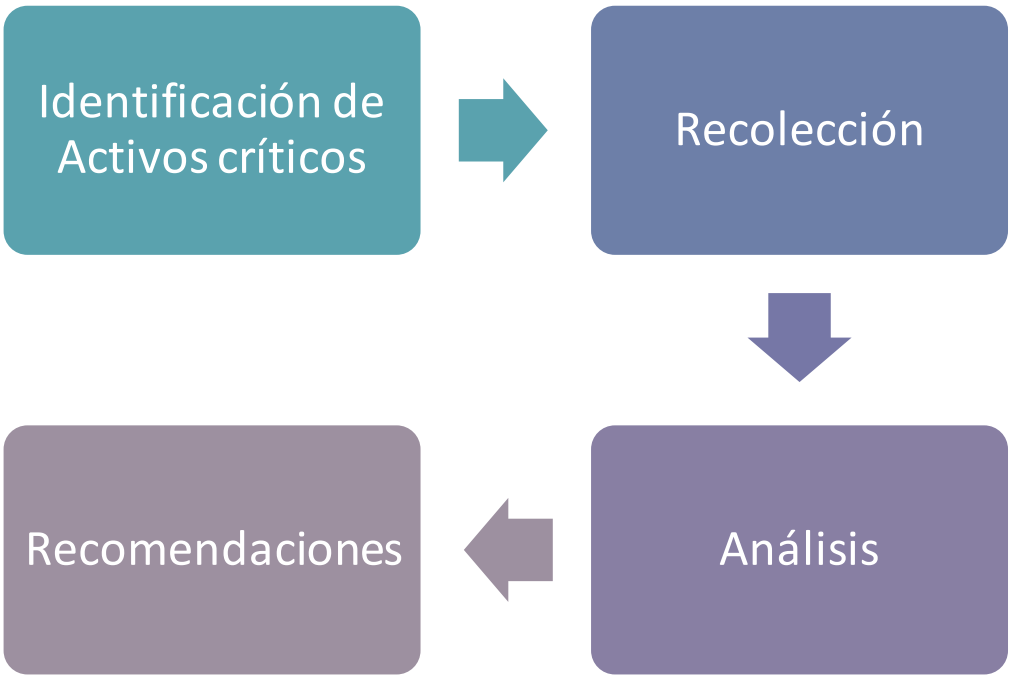
IIA posee **certificación ISO27001** vigente por más de 5 años consecutivos, lo que asegura al cliente experiencia necesaria **aplicando sistemas de gestión, buenas prácticas de seguridad informática**, así como la mejora continua de sus procesos y en el manejo de información crítica para nuestros clientes.

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.

Proceso

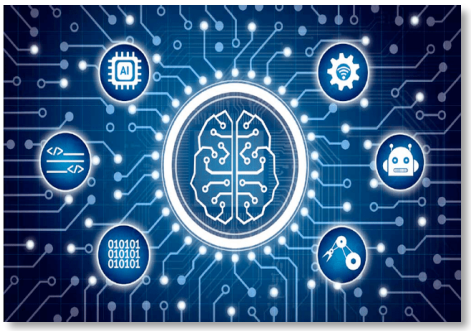
IIA adhiere a procesos conocidos en la Industria de servicios de seguridad que permiten a nuestros clientes obtener lo que necesitan de acuerdo con normas predefinidas que se ajustan a un marco de trabajo que permita analizar los resultados por etapas.



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

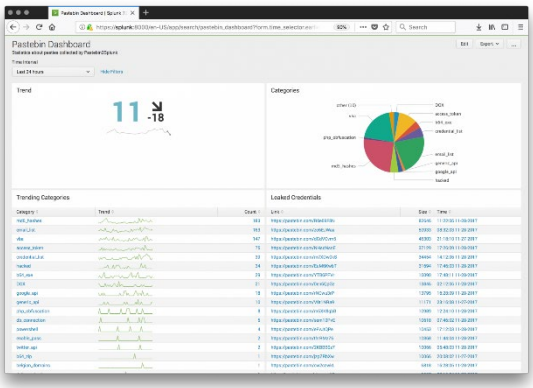


Luego de identificar los activos críticos se lleva a cabo La etapa de recolección de información relevante para el análisis. En esta etapa se usan herramientas que recolectan información durante un período de tiempo para luego ejecutar reportes que apoyan la labor de análisis. También se obtienen las 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 a las vulnerabilidades encontradas, de tal forma que el cliente pueda **tomar medidas de mitigación adecuadas** que eviten que las vulnerabilidades sean explotadas.

Evaluación de Ciberseguridad de la Red

Item	Entregable
Identificación, Análisis y Reporte desde 50 Activos críticos	Reporte de: • Activos críticos • Vulnerabilidades identificadas • Priorización según riesgo • Recomendaciones

Para más información contáctenos y solicite un presupuesto formal

CONTACTAR

228401000 – División Internet

30 AÑOS Generando soluciones integrales para su empresa