

Evaluación de Ciberseguridad de la Organización

SERVICIOS DE CIBERSEGURIDAD



EVALUACIÓN DE CIBERSEGURIDAD DE LA ORGANIZACIÓN

INTRODUCCIÓN

Actualmente la información que se procesa se encuentra no sólo en sistemas informáticos sino repartido a través de las organizaciones. De esta forma, los riesgos inherentes a ciberseguridad también se encuentran distribuidos tanto como las personas de una organización. Por esta razón, las organizaciones necesitan entender y comprender hasta donde pueden estar expuestos y que tipo de controles pueden aplicar para disminuir los riesgos.

Además de esto, las organizaciones necesitan comparar su nivel de exposición con otras organizaciones de su industria, de tal forma de asegurar ventajas competitivas para ellas y sus clientes.

Para determinar el nivel de preparación en aspectos de ciberseguridad que tiene una organización, IIA lleva adelante un Análisis de Ciberseguridad de la Organización que provee al cliente de un informe repetible y medible para informar a la dirección los riesgos de su institución y la preparación de ciberseguridad.

Este servicio identifica el perfil de riesgo que tiene una organización y la madurez de los controles existentes para diferentes dominios y categorías. Esto permitirá a la organización priorizar aquellas áreas críticas que pueden tener mayor probabilidad de ocurrencia junto con obtener recomendaciones para mejorar el nivel de madurez.

El servicio desarrollará un **informe** que le permitirá al cliente conocer:

- **Nivel de Riesgo Organizacional** en categorías estándar de riesgo
- **Nivel de madurez de ciberseguridad** en diferentes dominios aplicables
- **Posición de su organización** en comparación con otras de la industria
- **Recomendaciones** para cada categoría
- **Propuesta de implementación** de recomendaciones



¿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

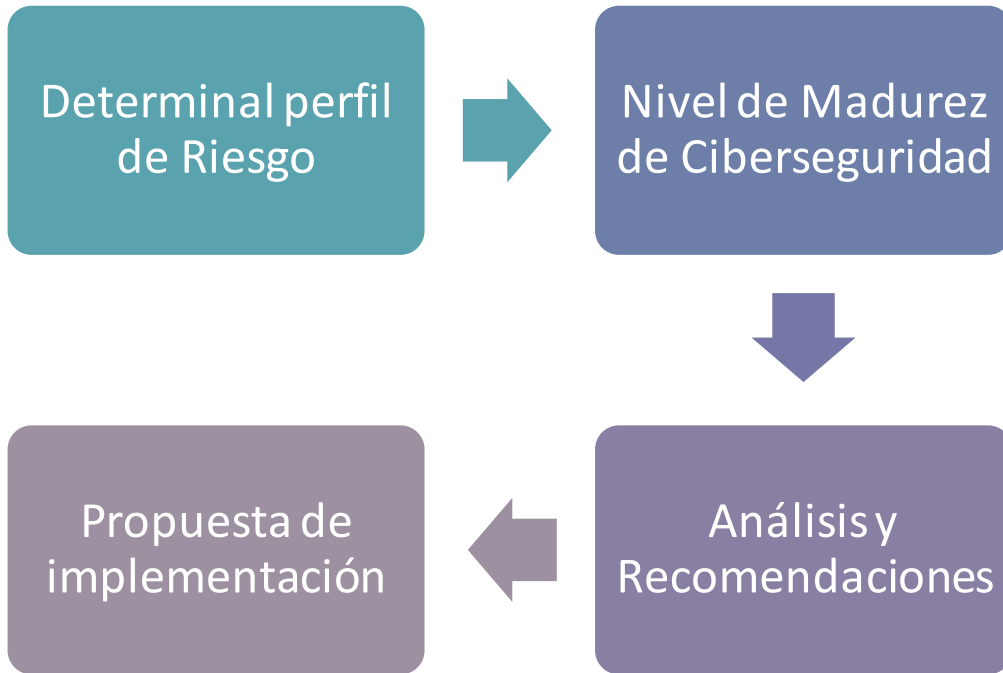
IIA posee **certificación ISO27001** vigente por más de 5 años consecutivos, lo que asegura al cliente experiencia necesaria **aplicando sistemas de gestión, buenas prácticas de seguridad informática**, así como la mejora continua de sus procesos y en el manejo de información crítica para nuestros clientes.

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.

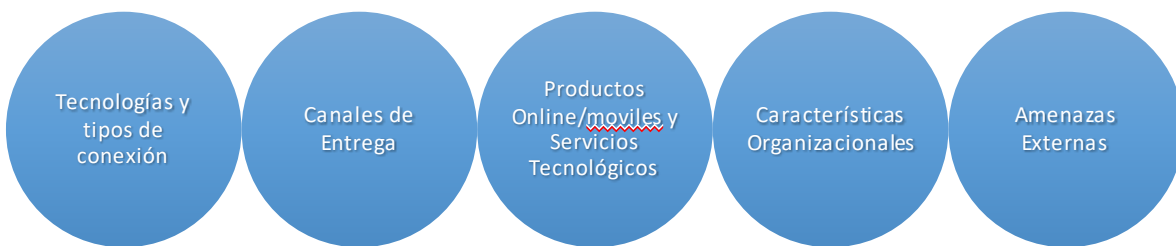
PROCESO

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.



DETERMINAR PERFIL DE RIESGO

Se definen 5 categorías de riesgo inherentes a la organización que deben ser evaluadas:



El riesgo inherente incorpora el tipo, volumen y complejidad de las operaciones de la institución y amenazas dirigidas a la organización. El perfil de riesgo ayuda a determinar el nivel de exposición que tiene la organización en actividades, servicios y productos que individual y colectivamente aportan a la institución.

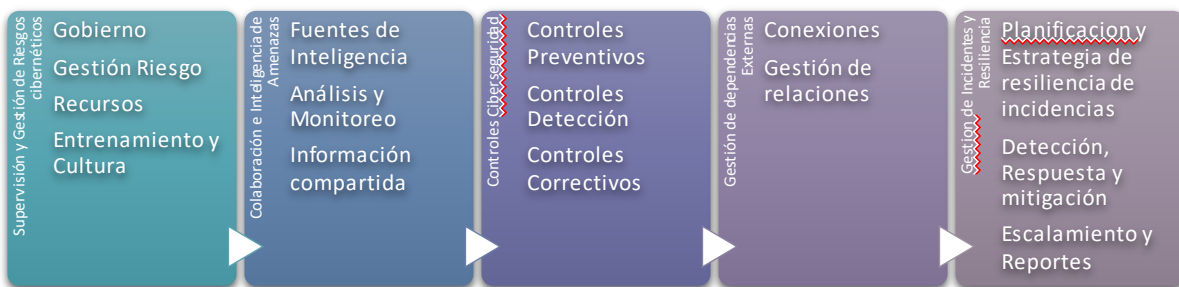
Estos niveles se clasifican en:



NIVEL DE MADUREZ DE CIBERSEGURIDAD

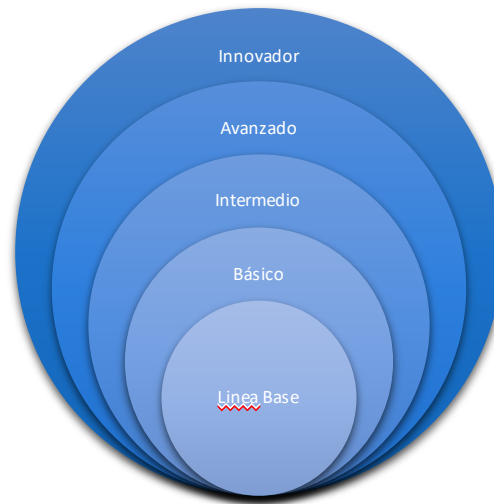
La segunda parte de la evaluación es determinar el nivel de madurez en ciberseguridad, diseñada para apoyar a la dirección a medir el nivel de riesgo y sus controles correspondientes.

La Madurez de Ciberseguridad incluye declaraciones para determinar si los comportamientos, practicas y procesos de la organización soportan la preparación de ciberseguridad en los siguientes dominios:



Cada dominio incluye factores de evaluación y componentes que contribuyen a determinar el nivel de madurez. En cada componente, una declaración de estado describe las actividades que soportan el factor de evaluación para cada nivel de madurez.

Los niveles de madurez para cada componente del dominio quedarán definidos en:



PROCESO DE ENTREVISTAS

Para determinar tanto el Perfil de Riesgo como el Nivel de Madurez de CiberSeguridad, se realizan entrevistas con los responsables de diferentes áreas para determinar tanto la exposición al riesgo que tiene la organización junto con controles de CiberSeguridad ya existentes.

En general los responsables que se requieren para determinar el nivel de Exposición son:

- Roles Mandatorios
 - Responsable de TI/CiberSeguridad
- Roles Opcionales
 - Responsable de la Organización
 - Responsable de Recursos Humanos
 - Responsable de Administración/Finanzas

En la primera reunión se informa el alcance los datos que se requieren y se designan los responsables idóneos para obtener la información. En la mayoría de los casos, el responsable de TI/Ciberseguridad puede recolectar parte de la información previamente sin necesidad que el consultor entreviste al responsable directo.

La mayor parte de información, en todo caso, se obtendrá del responsable TI/Ciberseguridad, quién se espera sea parte de todo el proceso de entrevistas.

ANÁLISIS Y RECOMENDACIONES

Luego de determinar el riesgo inherente y los niveles de madurez en ciberseguridad para cada dominio, ambos indicadores quedarán relacionados entre sí en cada dominio:

		Nivel de Riesgo Organizacional				
		Mínimo	Menor	Moderado	Significativo	Mayor
Nivel de Madurez de Ciberseguridad en Cada dominio 	Innovador					
	Avanzado					
	Intermedio					
	Básico					
	Línea Base					

El objetivo general es que, a mayor riesgo organizacional, mayor debe ser el nivel de madurez de ciberseguridad del dominio.

Una vez se determina el riesgo organizacional se definen las recomendaciones aplicables a cada caso, de tal forma de llegar a niveles de madurez deseables para cada caso.

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** para obtener el nivel de madurez adecuado junto con una propuesta de implementación de estas.



INFORME DE HALLAZGOS Y PRESENTACIÓN FINAL

Item	Entregable
Evaluación de Ciberseguridad de la Organización	Informe de análisis: <ul style="list-style-type: none"> • Nivel de Riesgo Organizacional • Nivel de madurez de Ciberseguridad • Recomendaciones para cada categoría • Propuesta de implementación

Para más información contáctenos y solicite un presupuesto formal

CONTACTAR

228401000 – División Internet

30 AÑOS

Generando soluciones integrales para su empresa

