CIBERSEGURIDAD DE LA ORGANIZACIÓN

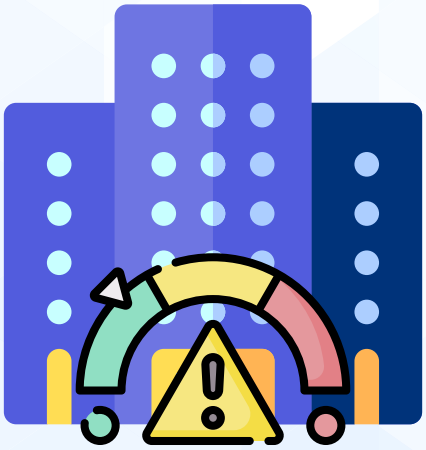
Determine el nivel de preparación de su empresa para enfrentar potenciales ataques informáticos

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 dónde 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.



Nivel de Riesgo

El servicio desarrollará un informe que le permitirá al cliente conocer

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

Determinar perfil de riesgo

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

1. Tecnologías y tipos de conexión
2. Canales de Entrega
3. Productos Online/móviles y Servicios Tecnológicos
4. Características Organizacionales
5. Amenazas Externas

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 se clasifican en:

Mínimo	Menor	Moderado	Significativo	Mayor

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:

1 Supervisión y Gestión de Riesgos Cibernéticos

- Gobierno
- Gestión Riesgo
- Recursos
- Entrenamiento y Cultura

2 Colaboración e Inteligencia de Amenazas

- Fuentes de Inteligencia
- Análisis y Monitoreo
- Información Compartida

3 Controles Ciberseguridad

- Controles Preventivos
- Controles Detección
- Controles Correctivos

4 Gestión de Dependencias Externas

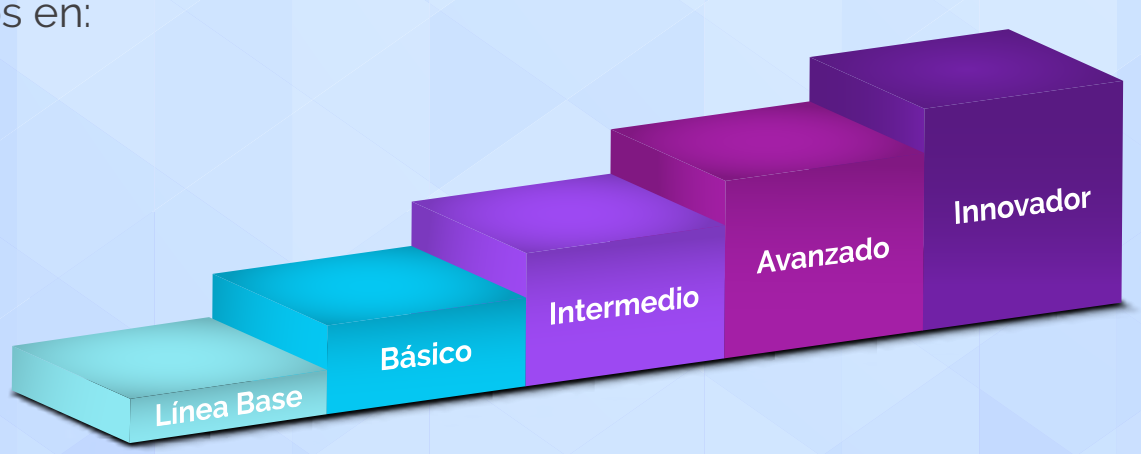
- Conexiones
- Gestión de relaciones

5 Gestión de Incidentes y Resiliencia

- Planificación y Estrategia de resiliencia de incidencias
- Deteción, Respuesta y Mitigación
- Escalamiento y Reportes

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

La mayor parte de información 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

Nivel de madurez de Ciberseguridad en cada dominio

	Mínimo	Menor	Moderado	Significativo	Mayor
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

Evaluación de Ciberseguridad de la Organización

Informe de análisis

- Nivel de Riesgo Organizacional
- Nivel de madurez de Ciberseguridad
- Recomendaciones para cada categoría
- Propuesta de implementación

CONTÁCTENOS

Para más información 228401000 - División Internet