Seguridad de la información: nivel de aplicación de prácticas en las instituciones públicas

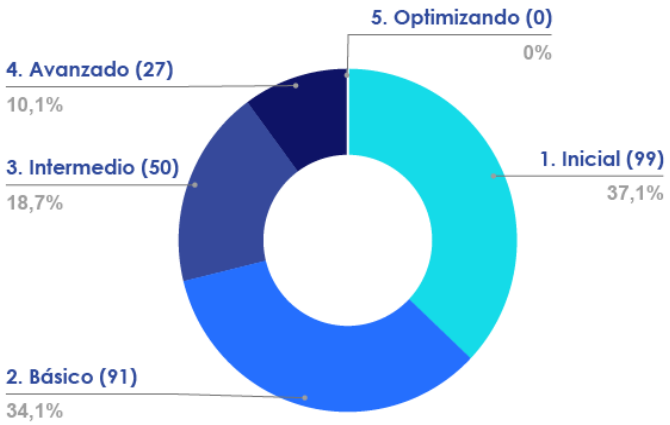
Panorama General

En el contexto actual, las instituciones públicas prestan sus servicios apoyándose cada vez más en tecnologías de información, por lo que están expuestas a eventos internos o externos, como los acontecidos durante el 2022 en los que algunas de ellas sufrieron incidentes de seguridad originados por ataques cibernéticos, que han afectado la continuidad de sus servicios. Es por ello, que surge la necesidad de tomar decisiones para contener, solucionar y prevenir nuevos ataques en contra de los sistemas de información de las instituciones públicas, para lo cual resulta relevante disponer de información sobre el nivel de aplicación de prácticas en esta materia, así como, los desafíos que deben gestionarse.

Para aportar en esa toma de decisiones, la Contraloría General ejecutó un análisis en coordinación con 59 auditorías internas, que permitió determinar el nivel de aplicación de prácticas de seguridad de la información en 267 instituciones, dando énfasis en los aspectos relevantes de ciberseguridad y la identificación de oportunidades de mejora. Esto con el propósito de que se ejecuten las acciones que permitan asegurar que la información y los sistemas son protegidos contra su divulgación a usuarios no autorizados, alteraciones y falta de acceso ante cualquier amenaza e intenciones maliciosas, de manera que se garantice la continuidad de los servicios públicos.

En términos generales, los resultados obtenidos reflejan que el sector público se encuentra en los niveles más bajos de aplicación de prácticas de seguridad de la información, ya que de las 267 instituciones analizadas, 190 se encuentran en los niveles inicial y básico, 50 en intermedio, 27 en avanzado y ninguna de ellas alcanzó el nivel más alto optimizando. -Figura 1-.

Figura 1. Distribución porcentual de las instituciones según nivel de aplicación



Fuente: Elaboración CGR.

Esta situación permanece en cada una de las dimensiones analizadas, evidenciando brechas en cuanto a las acciones para el establecimiento de la ruta a seguir a nivel estratégico y operativo, el esquema formal para el desempeño del sistema de gestión de seguridad de la información, así como la implementación de habilidades, conocimientos e idoneidad del personal.

Asimismo, a nivel sectorial se observa que la mayoría se encuentra en el nivel básico -Figura 2-. Siendo el sector financiero el que alcanza el mayor nivel, lo que refleja la necesidad de que las instituciones públicas apliquen prácticas para guiar el sistema de gestión de seguridad de la información, que contribuyan a fortalecer el resguardo de la información y aseguren la continuidad del servicio público, generando así valor a la ciudadanía.

Figura 2. Nivel de aplicación por sector

Fuente: Elaboración CGR.

Prácticas y Aprendizajes

A continuación, se detallan los aprendizajes obtenidos y las prácticas implementadas por las instituciones participantes, producto de la aplicación del instrumento elaborado por la Contraloría General:

1. **Instrumento como herramienta de autoevaluación institucional:** las instituciones públicas analizadas señalaron que a partir de la aplicación del instrumento de Prácticas de Seguridad de la Información obtuvieron un insumo para identificar aquellas áreas necesarias de fortalecer del sistema de gestión de seguridad de la información. Además sirvió para ampliar el conocimiento sobre el tema y para actualizar aquellas herramientas y mecanismos que permitan asegurar la operatividad de las instituciones.
2. **Necesidad de políticas integrales a nivel institucional y fortalecer las capacidades técnicas:** diversas instituciones indican que como reflexión final es necesario establecer políticas y capacitaciones al personal sobre seguridad de la información, así como, la incorporación del tema en la gestión de riesgos, bajo un enfoque de prevención de incidentes y priorización de riesgos informáticos.
3. **Enfoque interno y externo de las vulnerabilidades en seguridad de la información:** se plantea por parte de las instituciones públicas que no solamente identifiquen y controlen a nivel interno la seguridad de la información, sino que consideren los riesgos del entorno como amenazas por ciberataques que pueden perjudicar el resguardo de la información y la continuidad de los servicios públicos.

4. **Coordinación y comunicación interinstitucional:** se menciona la relevancia de que las instituciones que forman parte de un grupo, ministerio o sector institucional, implementen mecanismos para coordinar, comunicar y transmitir sus conocimientos y aprendizajes para que se fortalezca la cultura de seguridad de la información.

Desafíos identificados

Las instituciones públicas requieren adaptarse a la realidad actual que les enfrenta a un entorno tecnológico dinámico que implica gestionar las amenazas de ataques cibernéticos cada vez más frecuentes. Por ello, resulta relevante establecer medidas para gestionar los siguientes desafíos de seguridad para resguardar la confidencialidad, integridad y disponibilidad de la información:

1. **Disminuir brechas en la aplicación de prácticas:** el 71% de las instituciones se encuentran en niveles inicial y básico, lo que evidencia que se requiere de más acciones concretas para aplicar prácticas de seguridad de la información, ya que solamente el sector financiero obtuvo un nivel avanzado; por lo tanto es necesario que las instituciones de acuerdo con su complejidad y disponibilidad de recursos, establezcan una hoja de ruta que considere las brechas actuales en esta materia.
2. **Gestionar un plan de acción para el fortalecimiento de la seguridad de la información:** es indispensable que las instituciones dispongan de un plan de acción que considere las necesidades institucionales evidenciadas a partir de esta autoevaluación, en donde en línea con su presupuesto, permitan la mejora continua bajo un enfoque de prevención de incidentes y riesgos informáticos.
3. **Aplicar prácticas para el manejo y custodia de la información institucional:** un elemento esencial que debe aplicarse corresponde a la implementación de prácticas para identificar y clasificar su información crítica y sensible; sus procesos y activos críticos, así como, la ejecución de pruebas de funcionalidad de los respaldos de información de manera periódica, en procura de asegurar su disponibilidad, integridad y confiabilidad.
4. **Gestionar la continuidad y recuperación institucional ante posibles amenazas:** existe un desafío relevante respecto a la gestión de la continuidad institucional y de los servicios críticos, contar con planes basados en análisis de impacto al negocio, así como, de recuperación de incidentes que permita su identificación y clasificación; aplicar mecanismos alternos de adaptación del personal; coordinar con partes interesadas y ejecutar pruebas de recuperación, entre otras.
5. **Fortalecer las capacidades del personal institucional en materia de seguridad de la información:** únicamente el 12,4% (33) de las instituciones disponen de un programa de concientización del personal sobre seguridad de la información que considere la comunicación de la información que debe protegerse, los controles para protegerla, las funciones del personal y la promoción de conciencia sobre el riesgo de no seguir los procedimientos y políticas, entre otros. Además, esa misma cantidad de instituciones dispone de planes de capacitación en esta materia. Esto representa un desafío en el que se deben tomar acciones inmediatas para el establecimiento de una visión estratégica institucional y el fortalecimiento de capacidades del personal, siendo el eslabón más vulnerable ante amenazas por ciberataques.

Para mayor información sobre los niveles por sector, institución y dimensión puede consultarse la ***infografía*** que contiene un resumen de los resultados; así como, el ***sitio web***, en el cual se incluye el detalle de los mismos.