Sabor del mes

GESTIÓN DE RIESGOS DE CIBERSEGURIDAD

JULIO 2018

La Norma 2110.A2 –Gobierno– del IAI establece que "La actividad de Auditoría Interna debe evaluar si el gobierno de tecnología de la información de la organización apoya las estrategias y objetivos de la organización".

La Norma 2120.A1 –Gestión de Riesgos– del IAI establece que "La actividad de Auditoría Interna debe evaluar las exposiciones al riesgo referidas a gobierno, operaciones y sistemas de información de la organización, con relación a lo siguiente:

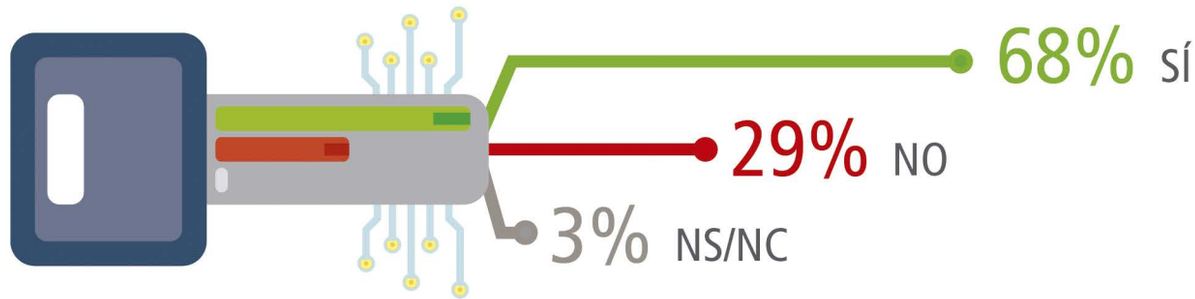
- Logro de los objetivos estratégicos de la organización;
- Fiabilidad e integridad de la información financiera y operativa;
- Eficacia y eficiencia de las operaciones y programas;
- Protección de activos; y
- Cumplimiento de leyes, regulaciones, políticas, procedimientos y contratos."

La ciberseguridad es un riesgo transversal en cualquier organización y con presencia continua debido a internet y los diferentes dispositivos de conexión a la red. Por dicha complejidad, requiere de un gobierno y de una serie de políticas y procedimientos para la prevención, para la gestión y para la mitigación de los riesgos que llegaran a materializarse.

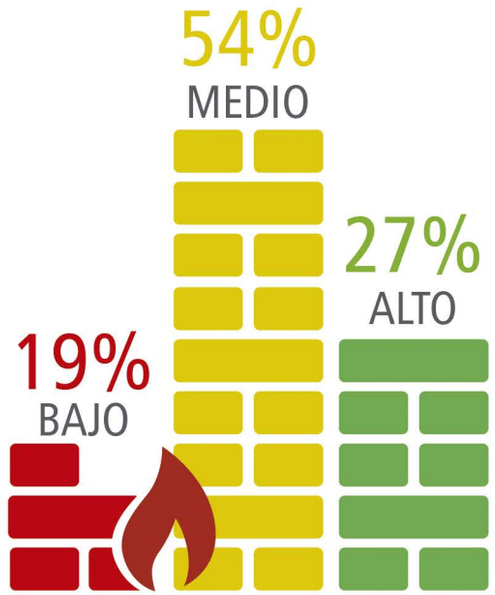
Así, Auditoría Interna debe evaluar, al menos, los siguientes aspectos:

- Si el gobierno de la ciberseguridad está alienado y apoya los objetivos y estrategias de la organización.
- Si existen políticas y procedimientos para la prevención y control de los riesgos de ciberseguridad y se están llevando a cabo.
- Y si existen políticas y procedimientos de gestión, respuesta y recuperación ante incidentes de seguridad y funcionan, en caso de que tuvieran que activarse.

¿VUESTRO PLAN ANUAL DE AUDITORÍA INTERNA CONTEMPLA REVISIONES DEL GOBIERNO DE LA CIBERSEGURIDAD?



¿EN QUÉ NIVEL DE MADUREZ CONSIDERAS QUE SE ENCUENTRA TU ORGANIZACIÓN PARA MITIGAR EL RIESGO DE CIBERSEGURIDAD?



¿CUENTA LA ORGANIZACIÓN CON PROCEDIMIENTOS/PROTOCOLOS DE GESTIÓN, RESPUESTA Y RECUPERACIÓN ANTE INCIDENTES DE CIBERSEGURIDAD?