



CAJA COSTARRICENSE DE SEGURO SOCIAL
AUDITORIA INTERNA
Tel.: 2539-0821 - Fax.: 2539-0888
Apdo.: 1010

ATIC-045-2016
4-04-2016

RESUMEN EJECUTIVO

El presente estudio se realizó según el Plan Anual Operativo 2016 del Área de Tecnologías de Información y Comunicaciones de la Auditoría Interna, con el fin de evaluar el fortalecimiento de la gestión de la seguridad de la información, y así contribuir con el aseguramiento de la confidencialidad, integridad y disponibilidad de la información.

En este sentido, es necesario que la Institución valore la inversión de nuevas herramientas que ayuden a fortalecer la seguridad de la plataforma tecnológica, ya que según las métricas expuestas por la empresa Gartner, recomienda a las empresas invertir aproximadamente un 6% del presupuesto total destinado a tecnologías de información y comunicaciones.

Otro aspecto fundamental, es la necesidad de disponer del personal humano suficiente y competente que permita gestionar razonablemente los recursos destinados a la seguridad en TIC, por tanto, es importante indicar que un profesional especializado en seguridad informática, debe ser capaz de aplicar las metodologías, tecnologías y herramientas que existen en las distintas áreas involucradas, como lo es criptografía, modelos formales de seguridad informática, análisis forense, etc. , así como en las áreas en las que la seguridad informática tiene su aplicación: redes, sistemas operativos, aplicaciones. De igual forma deben también ser capaces de gestionar incidentes, riesgos y garantizar la continuidad del negocio, protegiendo los activos críticos de la Institución.

Adicionalmente, es importante que la Institución disponga de políticas de seguridad de la información acordes con las Normas Técnica para la Gestión de las Tecnologías de Información de la Contraloría General de la República, así como otros estándares internacionales como el ISO27001, con el fin de articular la organización en cuanto a la seguridad de la información y brindando instrucciones claras a todos los funcionarios de las conductas esperadas y apropiadas, sirviendo como soporte para el logro de los objetivos de la Institución.

En este mismo orden de ideas, resulta relevante que la CCSS implemente indicadores que permitan alertar oportunamente cuando el límite de accesos a las aplicaciones es sobrepasado, detectar comportamientos irregulares en el uso de los sistemas de información, afectaciones al rendimiento de las herramientas tecnológicas, entre otros.