KERBEROS
MANAGING GENERAL AGENCY

CIBER-RIESGO

EN LA TRANSFORMACIÓN DIGITAL GUBERNAMENTAL

Septiembre – 2025

Gestión de Ciber-Riesgo como componente fundamental en los programas de transformación digital de los gobiernos

Gestión de Ciber riesgo como componente fundamental en los programas de transformación digital de los gobiernos

KERBEROS
MANAGING GENERAL AGENCY

Según el informe de Check Point Research, los eventos cibernéticos en entidades estatales aumentaron cerca de un **51% en el primer trimestre del 2025**, arrojando cifras cercanas a casi **3 mil ataques por semana** en este sector. Considerando que durante los últimos años ha sido uno de los sectores con mayor atractivo para el ciber crimen.

Para entender la creciente atención de los ciber delincuentes es importante identificar elementos claves que han convergido durante las ultimas décadas, y que hoy en día el nivel de exposición sea significativo frente a otros sectores:

Los avances tecnológicos han permitido en todas las industrias generar valores agregados y experiencias mucho más eficientes hacia las personas (usuarios), y de esta manera los gobiernos han concentrado esfuerzos para facilitar la prestación de servicios a los ciudadanos, como el recaudo de impuestos o tramites digitales que hace un tiempo se debía hacer de manera presencial.

La sociedad digital que consume diferentes servicios tecnológicos demanda el desarrollo de planes transformación digital, que permitan gestionar la relación gobierno-ciudadano de una manera mucho más rápida y eficiente.

La tecnificación de las instituciones ha permitido aumentar las capacidades relacionadas con el almacenamiento, consulta y protección de la información. Sin embargo, esto ha implicado la concentración de grandes volúmenes de datos e información de personas naturales y jurídicas lo cual genera interés en actores externos.

Entidades que prestan servicios importantes al ciudadano o tienen un papel importante en la función estatal, al verse interrumpidas por un evento cibernético, pueden generar afectación y materialización de riesgos colaterales y provocar un estado de conmoción interna afectado integralmente a la sociedad.

Teniendo en cuenta los elementos mencionados, los gobiernos se han convertido hoy en día en un objetivo especialmente atractivo para los ciberdelincuentes. Esto se debe a la gran cantidad y sensibilidad de la información que administran, al control sobre infraestructuras críticas y al impacto social que generan cuando sus servicios se ven afectados. Además, el interés de los atacantes no se limita a provocar pérdidas económicas: también buscan desestabilizar y minar la confianza de los ciudadanos en sus instituciones, aprovechando los contrastes y tensiones políticas de cada país.

Durante los últimos años América Latina ha sido blando de los ciber ataques, por ejemplo, en el **2022 Costa Rica sufrió un ataque que generó una crisis nacional** cuando un grupo de ransomware (Conti) logró afecta la operación de la Caja Costarricense de Seguro Social, retrasando y suspendiendo la opción de recolección de pagos y citas médicas de los ciudadanos. **En el 2023, Colombia sufrió una paralización de las funciones de varias entidades del estado** principalmente de la Rama Judicial, debido al ataque que interrumpió a uno de los proveedores tecnológicos más importantes a nivel mundial (IFX) y que generaba una dependencia importante en estos servicios. **En México se presentó el llamado “Guacamaya Leaks”** donde se expuso información sensible de las fuerzas militares del país y la afectación de varios servicios digitales de diferentes plataformas.

Principales retos en generar una política estatal que solidifique la barrera contra el cibercrimen

Garantizar la seguridad de la información que constantemente se está recolectando ya que los gobiernos pueden tener acceso a grandes volúmenes de información que contiene datos personales, de salud, financieros, sensibles e incluso planes estratégicos de orden nacional.

Mantener la operación de infraestructuras críticas y servicios esenciales que pueden afectar significativamente a los ciudadanos, como lo es servicios de energía, transporte, agua o salud, que pueden comprometer la integridad de las personas.

Ausencia de capacidades dentro de las entidades estatales para garantizar procesos de resiliencia y gestión de crisis con el fin de permitir una adecuada respuesta ante el caos que genera un evento de esta magnitud.

Contar con los recursos financieros suficientes y de manera oportuna para garantizar procesos de resiliencia organizacional.

Ausencia y falta de definición marcos regulatorios que permitan implementar de manera transversal operaciones seguras, alineadas a estándares internacionales enfocados en estrategias de gestión y prevención del riesgo cibernético.

¿Dónde deberían enfocar los esfuerzos los gobiernos?

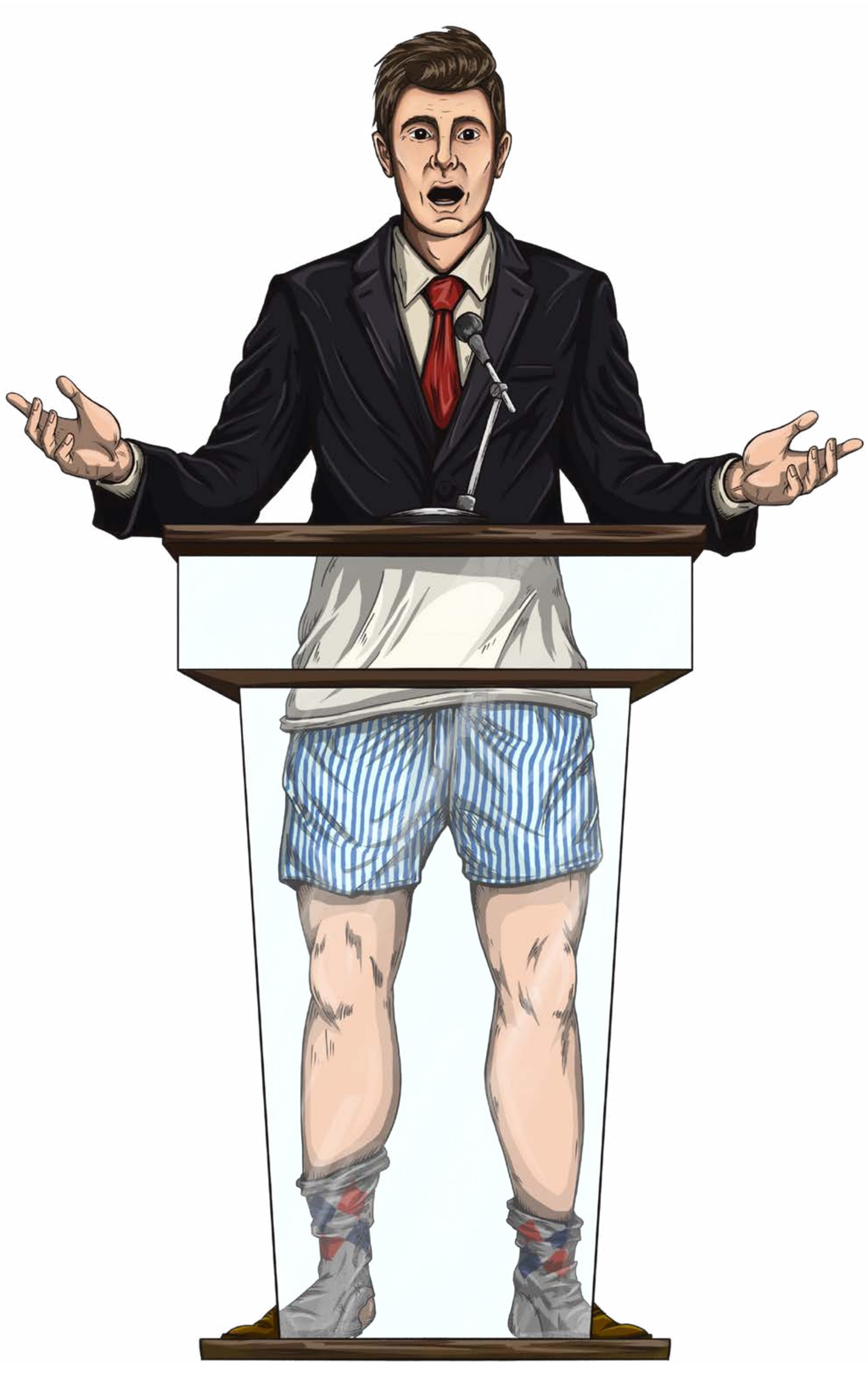
Interiorizar el nivel de exposición que tiene la entidad y desarrollar mecanismos que garanticen la asignación presupuestal para llevar a cabo la implementación de la estrategia de seguridad digital.

Definición de estándares y requisitos que se deben tener en cuenta al momento de clasificar y proteger de manera segura la información.

Desarrollar capacidades que permitan construir estrategias de contingencia efectivas, garantizando la continuidad de las operaciones en caso de tener materializado un evento.

Creación de agencias o entidades especializadas en materia de ciber riesgo enfocadas en la coordinación, definición, implementación y apoyo en la gestión de incidentes para las demás entidades estatales que se enfrenten a este tipo de situaciones.

Actualización de la regulación y creación de nuevas las leyes en torno a la protección de la información y la seguridad digital, entiendo lo complejo y dinámico que es el riesgo.



Es importante que los gobiernos comiencen a desarrollar compromisos en el corto y mediano plazo, según el Banco Interamericano de Desarrollo (BID), **solo 7 de los 32 países de Latinoamérica tienen planes para proteger su infraestructura crítica** y solo un poco mas de la mitad (20) cuentan con equipos especializados en la respuesta ante incidentes (CSIRT), mostrando oportunidades grandes de crecimiento en materia de gestión de riesgos tecnológicos.

La seguridad digital de los estados es un reto complejo que demanda la sinergia integral de esfuerzos que combinan ciudadanos, recursos económicos, tecnología, legislación y cooperación mutua entre países. La cual no solo debe enfocarse en blindar los sistemas tecnológicos; si no de fortalecer la confianza de los ciudadanos en las entidades, garantizar el buen manejo de la información y reconocer adecuadamente el panorama actual de amenazas derivadas de este mundo digital.

KERBEROS

MANAGING GENERAL AGENCY

www.kerberosre.io