Bogotá, junio de 2025

Entes Territoriales y Ciberseguridad en Colombia
Protección de la Información Pública y Activos Digitales

"*Qué tan preparadas están las alcaldías y gobernaciones en Colombia para recuperar su operación si sufrieran un ataque cibernético hoy*."

En el mundo actual, vinculado a la virtualidad, los entes territoriales en Colombia (alcaldías y gobernaciones) han asumido la gestión de grandes volúmenes de datos y recursos a través de sistemas interrelacionados. Sin embargo, se han evidenciado importantes debilidades institucionales en materia de ciberseguridad, lo cual ha permitido que se presenten ciberataques, fraudes financieros y acceso indebido a información sensibles.

En este dinámico contexto, los entes territoriales también deben revolver su situación frente a amenazas digitales presentes en el mundo interconectado en la red. Las principales, pero no las únicas, amenazas que enfrentan alcaldías y gobernaciones abarcan desde el ransomware que encripta los sistemas administrativos a cambio de rescates en criptomonedas; la suplantación de correos institucionales para realizar estafas; el acceso abusivo a bases de datos y sistemas financieros; pérdida o filtración de información ciudadana; hurto de recursos financieros por medio de accesos irregulares a cuentas bancarias, utilizando, por ejemplo, credenciales robadas o phishing.

El fraude o hurto virtual de cuentas bancarias del sector público es uno de los ataques más perjudiciales que se han registrado en los medios de comunicación y de los cuales referimos algunos casos como los sucedidos en la alcaldía de Cáchira (Norte de Santander) esta vez en abril de 2024, se sustrajeron 1.930 millones de pesos de las cuentas del Banco Agrario mediante cinco transacciones virtuales. El ciber criminal modificó las alertas de seguridad del banco, impidiendo la detección oportuna de los movimientos fraudulentos; en la alcaldía de El Tambo (Nariño). En mayo de 2024, la Tesorería Municipal denunció el hurto de entre 700 y 1.000 millones de pesos de las cuentas de la administración local. Pero las gobernaciones no han escapado a la acción de los cibercriminales. Mencionemos



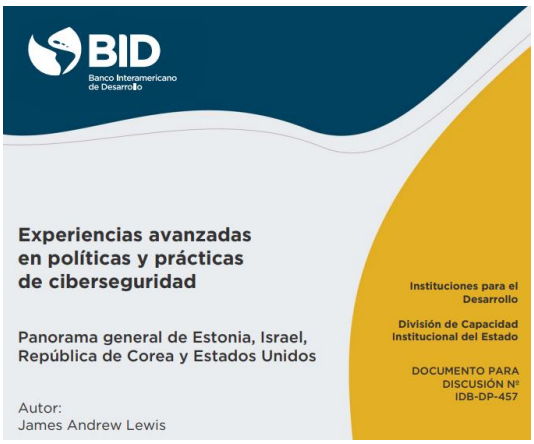
Fuente:https://www.elradardelsol.com/2024/05/01/denuncian-ciberataque-a-tesoreria-municipal-de-el-tambo-

lo sucedido en la gobernación de Putumayo donde fueron afectados en diciembre de 2022, cuando hackers sustrajeron más de 3.100 millones de pesos de una cuenta del ente territorial que correspondían a honorarios para más de 1.000 contratistas.

Este delito ocurre mediante el robo de credenciales de acceso bancario institucional (phishing, malware, insiders o persona que cuenta con acceso privilegiado a información o recursos no disponibles al público en general dentro de una organización); transferencias electrónicas fraudulentas desde sistemas internos comprometidos; suplantación de funcionarios ante plataformas bancarias; falta de autenticación robusta y monitoreo de transacciones. Estos eventos tienen efectos demoledores como la pérdida directa de recursos públicos, investigaciones penales, suspensión de proyectos, daño reputacional impactando la gestión pública y afectando a la sociedad bajo la jurisdicción del mandatario.

En Colombia, los Entes Territoriales se resguardan por leyes y otras normas que procuran salvaguardar con amplitud la ciberseguridad como la ley 1273 de 2009 que versa sobre los principios y objetivos para la protección de la información pública y la seguridad cibernética nacional, el decreto 2590 de 2010 que regula la ciberseguridad y la protección de la información en las entidades públicas, incluyendo los Entes Territoriales, la ley 1712 de 2014 establece la obligación de los Entes Territoriales de implementar medidas de ciberseguridad y protección de la información pública, la resolución 500 de marzo 10 de 2021 del Ministerio de Tecnologías de la Información y las Comunicaciones (Mintic) que establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.

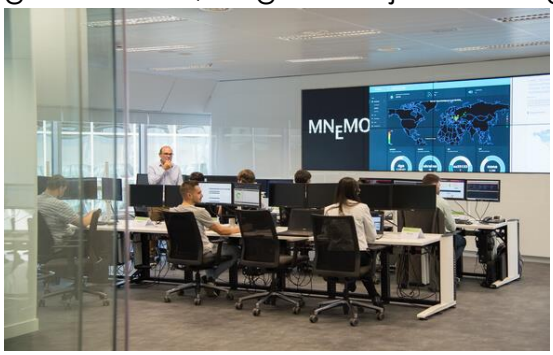
Los países más avanzados en ciberseguridad, como Estonia, Israel, Finlandia, Estados Unidos, Corea del Sur y Singapur, no dependen solo de la tecnología, sino de una visión integral y preventiva estatal, donde la seguridad de la información pública es considerada tan importante como la física. Estos modelos se soportan en un verdadero y efectivo liderazgo gubernamental, estrategias integrales y coordinadas para proteger la información pública, cooperación institucional, cultura digital y disposiciones normativas eficaces.



Fuente: Banco Interamericano de Desarrollo

Frente a este panorama, surge una inquietud ¿Qué permite que los entes territoriales sean vulnerables? Se ha evidenciado que el desconocimiento en torno a la ciberseguridad es marcada no solo por parte de un importante número de funcionarios sino en la comunidad en general que siguen viendo la seguridad cibernética como un asunto ajeno y exclusivo de "los ingenieros"; consecuentemente, ese desconocimiento por parte de los decisores motiva que el tema se desplace a un segundo plano reflejado en algunas ocasiones en la nula o poca asignación presupuestal para atender este rubro, la no aplicación de las regulaciones existentes, un esfuerzo incipiente en la capacitación en temas como la ciber higiene orientada a los empleados públicos y trabajadores oficiales y los compro hacen del asunto una alta vulnerabilidad.

En este sentido, es menester desarrollar un plan estratégico de ciberseguridad que define como una organización está preparada o no para proteger sus sistemas de información, datos y redes de las amenazas cibernéticas y formula acciones focales para garantizar la seguridad de la información y la ciberseguridad en torno, en este caso, a la cosa pública, albergada en el ciberespacio. Adicionalmente, este artículo formula algunas sugerencias de orden estratégico tales como reconocer la ciberseguridad como un componente esencial del gobierno y la gobernanza, asignar un jefe de seguridad de la información en los entes territoriales donde no exista esta figura, asignar presupuesto específico para infraestructura y talento humano en ciberdefensa, fortalecer alianzas con organismos técnicos y judiciales, crear canales de denuncia ciudadana digital, garantizar transparencia y rendición de cuentas en entornos digitales.



Fuente: https://colombia.mnemo.com/empresa/

Podemos concluir que los gobiernos locales deben asumir la defensa de sus activos como un asunto de gobernabilidad, no solo de tecnología. La ciberseguridad no es opcional: es un asunto axial de eficiencia y confianza pública. La protección de la información pública debe ser asumida como un eje estratégico de la gestión pública territorial, equiparable a la seguridad física, financiera o jurídica.

La ciberseguridad efectiva se construye con prevención, talento humano y cooperación. No se puede hablar de protección digital confiable sin una

cultura organizacional enfocada en la prevención, el desarrollo de capacidades técnicas continuas y l articulación entre gobierno, sector privado y comunidad técnica. Los entes territoriales deben migrar de un enfoque reactivo a uno proactivo, adoptando estándares globales, capacitando a sus funcionarios, así como a la comunidad en general y fortaleciendo alianzas para enfrentar amenazas digitales cada vez más complejas.

My (RP) Héctor Castro Corredor
Administrador Policial.
Especialista en seguridad, investigación criminal y alta gerencia.