La inseguridad informática en el sector público

El sector público posee una amplia gama de información confidencial que es necesario que el gobierno reestructure para que no ocurran filtraciones de datos en línea como lo sucedido recientemente en el Organismo Supervisor de las Contrataciones del Estado (OSCE), cuando medios de comunicación develaron filtraciones en el sistema para favorecer a algunas empresas en las licitaciones públicas.

Al respecto, el docente de la Universidad San Ignacio de Loyola (USIL), Marco Antonio Salcedo Huarcaya, señala que el sector público no cuenta con un Plan de Seguridad Informática que esté formalizado y publicado para conocimiento y cumplimiento de las entidades estatales en el Perú.

“Este es un fundamento muy amplio, pues la seguridad informática se encarga de las implementaciones técnicas de la protección de la información, del despliegue de las tecnologías como antivirus, *firewalls*, detección de intrusos, anomalías, correlación de eventos, atención de incidentes, entre otros elementos que, articulados con prácticas de Gobierno de Tecnología de Información, establecen la forma de actuar y asegurar las situaciones de fallas parciales o totales, cuando la información se encuentra en riesgo”, explica.

No obstante esta situación, Salcedo señala que el gobierno peruano ha decidido dar el primer paso para establecer el liderazgo en la planificación y ejecución de un conjunto de

acciones que permitan el desarrollo articulado y sostenido de la sociedad de la información en el país, a través de la promulgación del Decreto Supremo N.° 066-2011-PCM: "Plan de Desarrollo de la Sociedad de la Información en el Perú – La Agenda Digital Peruana 2.0", que ha significado, desde su creación en el año 2011, un esfuerzo conjunto de consenso permanente entre el gobierno, el sector privado, el sector académico y la sociedad civil.

Además, refiere que, con la finalidad de mejorar la gestión pública en sus diferentes instancias, dependencias, entidades, organizaciones, procedimientos, y construir un Estado democrático; se promulgó la Ley N.° 27658: Ley Marco de Modernización de la Gestión del Estado.

Intercambio de información

Para Marco Antonio Salcedo en el sector público peruano, las organizaciones no deberían estar "aisladas", sino intercambiar información y conocimiento (interoperabilidad). En ese sentido, agrega que, si bien esto ya se viene avanzando, todavía no alcanza un nivel de madurez como requiere la ciudadanía.

"Adicionalmente, las estrategias deben estar orientadas a la seguridad de las infraestructuras y servicios, capacidades de respuestas ante incidentes de seguridad, cultura de innovación y formación, protección empresarial, seguridad de la información, seguridad en el ciberespacio y seguridad digital", sostiene.

Asimismo, indica que los riesgos de la seguridad en la nube se han multiplicado debido a la pandemia. Es así que la encuesta Cloud Security Report 2021 menciona que el 73% de las organizaciones están muy extremadamente preocupadas por la seguridad en la nube. Además, el experto sostiene que el 67% de los encuestados mencionaron como causas la mala configuración de la plataforma en la nube o configuración incorrecta, así como el uso de interfaces o APIs no validadas.

“Para contrarrestar lo mencionado, las organizaciones deberían establecer un Marco de Gobierno para Cloud, tal como lo establece el Object Management Group (OMG), así como aplicar las técnicas o herramientas expuestas por Open Web Application Security Project (OWASP)”, puntualiza.

Presentación física

Ante lo ocurrido en el OSCE, la Comisión de Contrataciones del Estado de la Cámara de Comercio de Lima (CCL) demanda a esta institución la implementación de mecanismos de control y seguridad de calidad internacional, que garanticen procesos transparentes y predecibles, además de cumplir con todos los requisitos que establecen la ley y los tratados internacionales.

En ese sentido, señala que, hasta que estos sistemas de garantía y control no se implementen, excepcionalmente se podría autorizar la presentación física y en acto público –con la presencia de un notario– de los documentos requeridos en todas las licitaciones convocadas por el Estado y a cargo del OSCE.

El gremio empresarial recuerda que hace cuatro años el OSCE dispuso el cambio de esta forma de presentación por otra virtual, modificación que por entonces la CCL cuestionó, pues el sistema puesto en marcha por dicha institución no estaba certificado por ninguna entidad y no daba garantías ante posibles manipulaciones.

La CCL considera que una presentación física de documentos evitará, por el momento, casos como la infiltración de los sistemas informáticos de dicho organismo que derivaron en un presunto espionaje a favor de empresas que ganaron millonarias licitaciones.

En tal sentido, la Comisión de Contrataciones del Estado sostiene que es urgente investigar las últimas denuncias relacionadas al OSCE y poner en marcha las medidas correctivas necesarias, que deberán garantizar la transparencia de las compras públicas, más aún en un contexto como el actual, donde las situaciones de emergencia conllevan a compras estatales rápidas.

Para el profesor de la USIL, Marco Antonio Salcedo la explicación de lo ocurrido en el OSCE es que existen aparentemente vulnerabilidades en la red de esta institución, por lo que se debería identificarlas, comprender, gestionar y reducir los riesgos cibernéticos y proteger sus redes y datos.

“Esta situación afecta los objetivos estratégicos, así como a la reputación y expone un riesgo financiero, por lo que se debe dar atención prioritaria”, advierte.

Cabe precisar que el OSCE, a raíz de lo ocurrido, dispuso que desde el 15 de junio los montos de las ofertas económicas ya no sean registrados por los postores en el Sistema Electrónico de Contrataciones del Estado (SEACE) durante la etapa de presentación de ofertas; sino que solo adjuntará, obligatoriamente, el archivo con detalle de monto ofertado.

La entidad precisa que esta medida aplicará para todos los tipos de procedimientos de selección electrónicos en trámite o por convocarse independientemente del régimen legal, excepto para la Subasta Inversa Electrónica y para la Selección de Consultores Individuales.

Revolucionar la estructura del Estado

De otro lado, la expresidenta del OSCE, Mónica Yaya considera que es necesario "revolucionar" la estructura del Estado, específicamente en el área de las Contrataciones del Estado, pues dice que el OSCE ya no cumple su función.

"No solamente me refiero al tema de la vulneración de la información de las ofertas económicas, sino por ejemplo que el Registro Nacional de Proveedores también tiene procedimientos que son cuestionables, en el caso de las empresas chinas que han sido además denunciadas por estafar incluso a ciudadanos peruanos para la ejecución de sus obras, han participado de este famoso "Club del Tarot" que ha recibido información

privilegiada”, precisa.

Refiere que, por ejemplo, la empresa china Gezhouba tiene un capital social de S/ 3.500, sin embargo, recibe una capacidad de contratación de S/ 20.000 millones, poniéndola en una situación de privilegio frente a las empresas nacionales. “La Ley de Contrataciones del Estados está fallando, está siendo utilizada por empresas chinas para perjudicar no solamente al estado peruano, sino a las empresas peruanas”, subraya.

En ese sentido, aclara que es necesario revisar la organización de otras instituciones que guardan información estratégica como las instituciones estatales del sector energético, Corpac, las Fuerzas Armadas y el Sistema Nacional de inteligencia, entidades que guardan información estratégica y que si son vulneradas ocasionaría un gravísimo riesgo para la seguridad del país.

Mónica Yaya recuerda que el SEACE se implementó en el Gobierno de Ollanta Humala. Sin embargo, considera que este cambio significó la vulnerabilidad de la información. Recuerda que con el sistema tradicional había un notario que se hacía responsable no solamente de las historias de las ofertas económicas, sino también de la reserva del contenido, indica que estas ofertas no se almacenaban durante tantos días como sí ocurre en el SEACE.

“Una verdadera seguridad informática funcionará si es que absolutamente nadie tuviera acceso a la información que allí se guarda, pero, lamentablemente, en el OSCE si hay personas que tienen acceso a información secreta, privilegiada y esto

ya hace todo el sistema vulnerable”, puntualiza.