Seguridad de datos en el sector de la salud: Reflexiones tras el ataque cibernético

Ana del Carmen Carolina Ángel Cepeda[1]

El 12 de septiembre de 2023, varios medios de comunicación en Colombia y otras partes de Latinoamérica informaron sobre la afectación de los servicios de la empresa IFX Networks debido a un ataque externo de ciberseguridad. Este incidente comprometió varios sistemas e información de diversas entidades públicas y privadas del país, generando una creciente preocupación debido a la posible vulnerabilidad de los datos e información privada que estas instituciones almacenan en sus bases de datos.

Entre las instituciones afectadas en Colombia se incluyen la Superintendencia de Industria y Comercio, la Superintendencia de Salud, el Consejo Superior de la Judicatura, el Ministerio de Cultura, la Cruz Roja y el Ministerio de Salud, entre otras.

De acuerdo con lo anterior, se puede concluir que varios sistemas de información y bases de datos se vieron comprometidos como resultado del ataque cibernético. Entre las diversas entidades afectadas, el sector de la salud fue uno de los más perjudicados. En algunos casos, los sistemas tuvieron que ser apagados temporalmente, y como medida de contingencia, se implementó una respuesta manual debido a la inaccesibilidad de las aplicaciones. Dado que los servicios de atención médica requieren una continuidad ininterrumpida, esta forma manual de solventar el incidente, aunque permitió una atención inmediata a los pacientes, usuarios, clientes o ciudadanos, generó la necesidad de volver a procesar la información en el sistema computacional una vez que se restablecieran los servicios.

El impacto del ataque fue de gran magnitud y adquirió una significativa importancia cuando consideramos que numerosos procesos en el país dependen de respuestas tecnológicas que conllevan una gran responsabilidad hacia los usuarios, clientes y ciudadanos debido a la información almacenada en sus bases de datos. Esta información, en su mayoría de carácter sensible y privado, así como datos de carácter público, se utiliza para procesos y mediciones esenciales cuyo objetivo principal es servir a la población, organizaciones y al gobierno.

A pesar de las afirmaciones del Ministerio de Salud y la Superintendencia de Salud de que no se ha producido una vulneración de los datos de pacientes o información clínica que pudiera dañarse o secuestrarse, persiste una sensación de preocupación, duda y, en algunos casos, desconocimiento sobre lo que realmente ocurrió y si la información de los ciudadanos se vio afectada. Esto no se debe a la falta de acción en el país, sino al impacto masivo que tuvo el ataque, lo que lleva a muchas entidades a evaluar las causas y a tomar decisiones definitivas para reducir significativamente la probabilidad de que esto vuelva a ocurrir, medidas también que deben adoptar las empresas que brinden servicios de alojamiento, administración, análisis y generación de sistemas computacionales.

Cuando estas soluciones y/o bases de datos se ven vulneradas, atacadas o secuestradas, es esencial implementar medidas de control que minimicen al máximo los efectos de dichos ataques. Estas medidas deben ser claras, documentadas y conocidas por todos los involucrados, y deben estar incluidas en las matrices de riesgos y planes de contingencia que forman parte de las políticas de seguridad de la información de cada organización. Algunas medidas comunes incluyen siempre respaldar

1. Ingeniera de Sistemas, Especialista en Auditoría de Sistemas de Información y Gerencia de Proyectos Profesional Especializado, Contratista en Observatorio de Salud de Bogotá SaluData Secretaría Distrital de Salud.

los datos en servidores diferentes, ya sea en la nube o en entornos locales (también conocidos como *on premise* o "en tierra"). Además, es una buena práctica cifrar ciertos datos sensibles almacenados en bases de datos para dificultar la obtención clara de información en caso de robo. Asimismo, se recomienda revisar las pólizas de ciberseguros que cubren incidentes de este tipo. Al hacerlo, es importante evaluar sus coberturas según el tipo de evento informático ocurrido, ya sea robo de información, daño o eliminación de archivos, virus informáticos, acceso no autorizado a los sistemas, entre otros. Es fundamental mantener las políticas mencionadas en constante actualización. Al mismo ritmo que día a día evolucionan los ciberataques, la respuesta a los mismos será más efectiva si se mantienen en renovación los mecanismos que permitan el control de cualquier incidente.

En este escenario sucedido solo se vieron afectadas algunas de las entidades que se encontraban vinculadas contractualmente con la empresa IFX Networks, pero esto no quiere decir que las demás instituciones gubernamentales estén libres de ataques o que todas las entidades que tenían a este proveedor fueron atacadas, lo cual refuerza el tema de visualizar que aparte de la supervisión a estos contratos con proveedores de servicios informáticos y de seguridad de la información, se debe reforzar la cultura interna organizacional frente a los mismos y los equipos internos deben velar por la protección y respaldo de sus activos informáticos indistintamente de los proveedores tecnológicos que vinculen.

Estos ataques llevan a cuestionarse cómo se gestionan los datos, especialmente los relacionados con la salud, en todas las fases que intervienen desde que se generan hasta su uso final. Esto incluye generación, almacenamiento, procesamiento, mantenimiento y visualización. Se deben establecer criterios claros sobre qué información se debe conservar y cuáles son las reglas de negocio que rigen su uso. Dentro de esos procesos es esencial determinar dónde se almacenarán estos datos y quiénes tendrán acceso a ellos, roles de accesos y listas de permisos, así como políticas claras sobre respaldos de información o *backups* que se encuentren dispuestos en centros de datos diferentes a los servidores de aplicación y bases de datos.

La aplicación de este enfoque en la gobernanza de datos, en conjunto con políticas y planes sólidos de seguridad de la información, es esencial en el sector de la salud y en cualquier otro sector. Esto se vuelve crucial para implementar u optimizar la seguridad y privacidad de la información ciudadana, así como para prevenir o saber cómo actuar frente a posibles incidentes de ciberseguridad en el futuro.

Referencias

1. Rico JCG. Así enfrenta Colombia su primer caso de "megasecuestro digital"; ¿qué está pasando? [Internet]. El Tiempo. 2023 [citado 6 de octubre de 2023]. Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/ciberataque-en-colombia-detalles-del-ataque-a-ifx-networks-806778

2. G. Conclusiones del ciberataque en Colombia: impacto y lecciones aprendidas [Internet]. ENTER.CO. 2023 [citado 6 de octubre de 2023]. Disponible en: https://www.enter.co/empresas/seguridad/conclusiones-del-ciberataque-en-colombia-impacto-y-lecciones-aprendidas/

3. Semana. Los datos de salud: del riesgo a la vulneración [Internet]. Revista Semana. 2023 [citado 6 de octubre de 2023]. Disponible en: https://www.semana.com/opinion/articulo/los-datos-de-salud-del-riesgo-a-la-vulneracion/202308/

4. MINTIC. Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas. Versión 4 [Internet]. 2021 [citado 6 de

octubre de 2023]. Disponible en: http://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

5. MINTIC. Plan Nacional de Infraestructura de Datos. Versión 1 [Internet]. 2021 [citado 6 de octubre de 2023]. Disponible en: https://www.mintic.gov.co/portal/715/articles-198952_anexo_1_pnid_documento_tecnico_hoja_ruta.pdf

6. Deloitte Spain. Pasos a seguir ante un ataque informático [Internet]. [citado 14 de noviembre de 2023]. Disponible en: https://www2.deloitte.com/es/es/pages/legal/articles/Pasos-a-seguir-ante-un-ataque-informatico.html

Foto: https://www.freepik.es