República Argentina - Poder Ejecutivo Nacional
2021 - Año de Homenaje al Premio Nobel de Medicina Dr. César Milstein

Resolución

Número: RESOL-2021-146-APN-DNPDP#AAIP

CIUDAD DE BUENOS AIRES
Viernes 17 de Septiembre de 2021

Referencia: EX-2020-83150939- -APN-DNPDP#AAIP - RESOLUCIÓN CENCOSUD SA

VISTO el EX-2020-83150939- -APN-DNPDP#AAIP, las leyes Nros 25.326 y 27.275, los Decretos Nros. 1558 del 29 de noviembre de 2001, 746 del 25 de septiembre de 2017, 899 del 3 de noviembre de 2017 y 1012 del 16 de diciembre del 2020; las Resoluciones Nros. 30 del 14 de mayo del 2018 y 83 del 23 de abril de 2020; la Disposición DNPDP Nº 7 del 8 de noviembre del 2005 y sus modificatorias; y

CONSIDERANDO:

Que por las actuaciones mencionadas en el VISTO tramita una investigación de oficio efectuada por la Dirección Nacional de Protección de Datos Personales (en adelante, también "DIRECCIÓN NACIONAL" o "DNPDP") de la Agencia de Acceso a la Información Pública (en adelante "AAIP"), Autoridad de Aplicación de la Ley Nº 25.326, al grupo CENCOSUD S.A. (en adelante, "CENCOSUD") por haber tomado conocimiento de ciertos hechos públicos y notorios relacionados con una vulneración que habría ocurrido en los sistemas informáticos del Grupo en el mes de noviembre de 2020, multinacional que opera en el país a través de las empresas Jumbo, Easy, Supermercados Vea y Disco, que se habrían desencadenado a raíz de un ataque informático conocido como "ransomware Egregor", malware que encripta información.

Que en atención a que entre la información recolectada por los atacantes habría "movimientos de compras y ventas de la empresa", así como datos de clientes y tarjetas de crédito, y que se habría solicitado un rescate a CENCOSUD "para no publicar lo obtenido", la mencionada DIRECCIÓN NACIONAL ha considerado que dicho incidente de seguridad podría implicar la filtración de datos personales de titulares argentinos en su carácter de clientes, situación que afectaría los principios protectorios de la Ley N° 25.326 de Protección de Datos Personales, en particular, los deberes de seguridad y confidencialidad a cargo del responsable del tratamiento CENCOSUD S.A.

Que al respecto, teniendo en consideración que el incidente de seguridad podría implicar una vulneración masiva de los datos personales de titulares de datos argentinos, de conformidad con el artículo 9 de la Ley Nº 25.326, la DNPDP mediante la nota identificada como NO-2021-16213472-APN-DNPDP#AAIP, intimó a CENSODUD para que en el plazo de DIEZ (10) días hábiles de notificada la misma: (i) Confirme si existió un incidente de seguridad en su empresa. En caso afirmativo, detalle las vulneraciones, las medidas adoptadas por el responsable

para su mitigación y las medidas aplicadas para evitar futuros incidentes; (ii) Informe si en dicho contexto existió filtración y/o revelación de información confidencial o datos personales de clientes argentinos de las respectivas empresas que integran CENCOSUD S.A. En caso afirmativo, indique desde cuando se tiene conocimiento de la filtración de los datos, que medidas fueron adoptadas en consecuencia, la cantidad de datos comprometidos y si ha notificado a los titulares afectado; (iii) Explique las medidas técnicas y organizativas implementadas por la empresa para garantizar la seguridad y confidencialidad de los datos personales de sus clientes, para evitar su tratamiento no autorizado, por riesgos provenientes de la acción humana y/o medios técnicos, de acuerdo con el artículo 9 de la Ley N° 25.326 y recomendaciones de la Resolución AAIP N° 47/2018; (iv) Informe la existencia de procesos judiciales y/o penales en curso en relación con la presente cuestión, y en caso afirmativo, detalle los datos de su respectiva tramitación; y (v) Denuncie un correo electrónico para futuras comunicaciones en el marco de la presente requisitoria.

Que mediante IF-2021-26939180-APN-DNPDP#AAIP luce agregado el descargo efectuado por el Sr. [redacted] en su carácter de representante de CENCOSUD SA, conforme lo acredita mediante copia del poder general que le ha sido conferido a tales efectos.

Que a través de dicha presentación, la empresa CENCOSUD manifestó que: (i) “fue objeto de un malware que afectó levemente la infraestructura Argentina, no habiendo comprometido la operación de Cencosud SA, ni se ha identificado la existencia de daños”; (ii) que ante dicha situación las medidas adoptadas han consistido en las siguientes: “a) instalación de una nueva solución de Protección de “Endpoints & Servidores” mejorando la detección y prevención de malware; b) implementación de una herramienta de gestión de vulnerabilidades, lo que les posibilitaría contar con un proceso continuo de identificación, evaluación y corrección de vulnerabilidades en su infraestructura; y c) que estarían implementando un servicio de SOC (Security Operation Center) para el monitoreo y análisis de la actividad/eventos de seguridad de nuestra infraestructura crítica y “tener alarmas proactivas ante posibles brechas/ataques”.

Que del análisis del descargo recibido, la referida DIRECCIÓN NACIONAL advirtió que, si bien CENCOSUD ha confirmado que existió un incidente de seguridad en su organización, haciendo alusión a que el mismo “afectó levemente la infraestructura Argentina”, no dio cuenta de manera específica (a) en qué consistieron las vulneraciones ocurridas en su organización; (b) ni en qué consistió la afectación “leve” sufrida que refiere afectó su infraestructura nacional. Sin perjuicio de ello, en el mismo descargo aclara que “no se ha identificado la existencia de daños”.

Que con relación al segundo punto consultado, la DNPDP consideró que la respuesta de CENCOSUD resultó insuficiente puesto que la empresa se limitó a mencionar los nombres de las soluciones tecnológicas nuevas -que habría adoptado o que estaría adoptando tras el incidente-, no acompañando una explicación concisa sobre lo requerido, es decir, sin brindar detalles sobre las medidas técnicas y organizativas preventivas implementadas previo al incidente, ni las correctivas para su mitigación, minimización de impactos y plan de contingencia para evitar futuras vulnerabilidades.

Que en este orden de cosas, la DNPDP destacó que la Resolución AAIP Nº 47/2018 detalla las medidas de seguridad derivadas de las obligaciones del artículo 9 de la Ley Nº 25.326 para facilitar a las organizaciones su cumplimiento, advirtiéndose que CENCOSUD no llevó a cabo ninguna de éstas para prevenir incidentes de seguridad por diseño, como así tampoco para la gestión de incidentes.

Que, por ejemplo, (i) no realizó un informe detallado del incidente de seguridad y tampoco lo notificó a la DNPDP oportunamente, (ii) no dio cuenta de haber comunicado el incidente a sus clientes como titulares de datos

para que se encuentren prevenidos de posibles maniobras fraudulentas ulteriores al incidente, (iii) no presentó detalles de los procedimientos internos implementados por la organización en el manejo de la información y los estándares de seguridad en la protección de datos personales en su tratamiento, (iv) no informó concretamente las medidas que hacen a su plan de contingencia y mitigación, ni especificó cuáles fueron los procesos de revisión implementados para la corrección de las vulneraciones en sus sistemas informatizados, y (v) no informó el responsable asignado que llevará a cabo las tareas preventivas y correctivas transversales que hacen a la protección de los datos personales en su organización conjuntamente con las distintas áreas implicadas.

Que en la misma línea, la DNPDP advirtió que CENCOSUD no respondió concretamente (i) si a raíz del incidente de seguridad existió filtración y/o revelación de información confidencial o datos personales de clientes argentinos de las respectivas empresas que integran CENCOSUD S.A.; (ii) desde cuándo tiene conocimiento de la filtración; y (iii) cuál es la cantidad de datos comprometidos.; (iv) tampoco respondió lo consultado sobre la existencia de procesos judiciales y/o penales en curso en relación a la presente cuestión, ni denunció un correo electrónico para futuras comunicaciones en el marco de la presente investigación.

Que además, la DIRECCIÓN NACIONAL resaltó que, -en forma posterior a la intimación cursada-, ha llegado a su conocimiento por diversos medios comunicación, que algunos usuarios después del incidente de seguridad investigado, han recibido mails fraudulentos (bajo la modalidad conocida como "phishing"), desde el correo electrónico "easyteayuda@hotmail.com", simulando en apariencia ser correos electrónicos oficiales de una de las empresas del Grupo CENCOSUD para engañar a los usuarios y que estos brinden datos personales adicionales a través de ese medio. (Fuente: "Hackeo a Cencosud: malestar de los clientes por estafas en marcas asociadas").

Que en la mayoría de los casos, se habría dado cuenta que, los correos recibidos por los usuarios en nombre de CENCOSUD comunican a los titulares de datos que, determinada compra efectuada por ellos no pudo perfeccionarse y que, para procesarse los cobros correctamente, resultaría necesario que se aporten datos personales adicionales, enviando por ese medio, una imagen de sus tarjetas de crédito y números del DNI. En particular, los titulares de datos resaltaron el riesgo adicional que importan dichas comunicaciones fraudulentas, en atención a que, en las mismas efectivamente se alude a números verídicos de operaciones y transacciones que efectivamente han realizado.

Que en dicho contexto, la DNPDP labró el Acta de Constatación identificada como ACTA-2021-39555541-APN-DNPDP#AAIP mediante la cual se verificaron las infracciones incurridas.

Que la conducta de CENCOSUD S.A. de no haber tomado las medidas técnicas y organizativas preventivas necesarias para garantizar el principio de seguridad en su organización, configura UNA (1) infracción grave consistente en: *"Mantener bases de datos locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen"*, conforme el punto 2, inciso k) del Anexo I, de la Disposición DNPDP N° 7/05 y modificatorias.

Que la conducta de CENCOSUD S.A. de no haber tomado las medidas técnicas y organizativas correctivas necesarias para garantizar el deber de seguridad en su organización, configura UNA (1) infracción grave consistente en: *"Mantener bases de datos locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen"*, conforme el punto 2, inciso k) del Anexo I, de la citada Disposición.

Que la conducta de CENCOSUD S.A. de no haber comunicado a sus clientes titulares de datos que podían ser víctimas de filtraciones de datos personales por el incidente de seguridad sufrido en su organización en una

primera oportunidad, configura UNA (1) infracción muy grave consistente en: *"Tratar los datos de carácter personal en forma ilegítima o con menosprecio de los principios y garantías establecidos en Ley No 25.326 y normas reglamentarias"*, conforme el punto 3, inciso f) del Anexo I de la Disposición DNPDP N° 7/05 y modificatorias.

Que la conducta de CENCOSUD de no haber comunicado a sus clientes titulares de datos que podían ser víctimas de filtraciones de datos personales por el incidente de seguridad sufrido en su organización en una segunda oportunidad, configura UNA (1) infracción muy grave consistente en: *"Tratar los datos de carácter personal en forma ilegítima o con menosprecio de los principios y garantías establecidos en Ley No 25.326 y normas reglamentarias"*, conforme el punto 3, inciso f) del Anexo I de la Disposición indicada precedentemente.

Que la referida acta fue notificada a CENCOSUD el 6 de mayo de 2021, conforme surge de la constancia agregada bajo IF-2021-42486569-APN-DNPDP#AAIP.

Que como consecuencia de lo actuado, el 19 de mayo del corriente año la entidad investigada presentó su descargo a través del envío de un correo electrónico a la dirección oficial de éste Organismo.

Que en su presentación, CENCOSUD manifestó que: (i) en relación al malware que afectó la infraestructura de la empresa en Argentina destaca que, "no se habrían comprometido datos personales de clientes"; (ii) para explicar las medidas aludidas en su descargo anterior acompañó DIEZ (10) Anexos que darían cuenta de modo general de los distintos manuales o programas que internamente llevaría a cabo (por ejemplo "Política de Satisfacción del Cliente, Principios de Marketing Responsable", "Política de Oferta Sostenible", "Declaración de Seguridad de la Información, Política de seguridad de la información, "Norma de Administración de Usuarios", Programa de Ciberseguridad", entre otros); y (iii) respecto al correo fraudulento "easyteayuda@hotmail.com" que simulaba ser un correo oficial enviado por una de las empresas del Grupo ("Easy"), manifestó que presentó una denuncia ante la Unidad Fiscal Especializada en Ciberdelitos para que se investigue dicha conducta ilícita.

Que del último descargo recepcionado, en primer lugar, la DIRECCIÓN NACIONAL considera que, ha quedado corroborado que CENCOSUD reconoció que un malware afectó la infraestructura de la empresa en Argentina y que posteriormente no contestó cabalmente lo consultado en dos oportunidades (desde cuándo tiene conocimiento de la filtración, y en qué consistieron las vulneraciones sufridas).

Que en segundo lugar, la DNPDP advierte que, en su último descargo CENCOSUD tampoco respondió específicamente lo consultado sobre el detalle de las medidas preventivas y correctivas que debió haber implementado. En este punto, se pone de resalto que no corresponde, ni resulta competencia de este Organismo proceder al análisis de los DIEZ (10) Anexos presentados por CENCOSUD a fin de interpretar si de los mismos, surge lo que se le consultó en el marco de la presente investigación.

Que a modo de ejemplo respecto a la documental recepcionada, si bien la empresa presenta un Anexo referido a "Política de Seguridad de la Información"; no ha informado concretamente cómo ha gestionado, mitigado, comunicado y documentado los incidentes investigados en el marco del presente. Como corolario, de la documentación acompañada, surgiría que la Política de Privacidad de la empresa pretende eximirse de sus obligaciones de seguridad estableciendo que: *"[n]o puede garantizar que la información transmitida a través [de su] sitio web, se encuentra completamente segura, con lo cual [el usuario] asume este riesgo que declara conocer y aceptar"*.

Que en tercer lugar, con relación a los deberes de seguridad contemplados en el artículo 9 de la Ley Nº 25.326, CENCOSUD tampoco contestó, ni logró desvirtuar con prueba idónea que -ante la ocurrencia de los incidentes de

seguridad-, ha brindado información efectiva a los titulares de datos de modo que puedan estar prevenidos sobre lo acontecido para prevenir daños adicionales, o bien para que estén anoticiados en el caso que decidieran proceder al ejercicio de sus derechos en el marco de la Ley 25.326.

Que, merituándose las circunstancias particulares del caso, y atento al alcance masivo del primer incidente de seguridad, -que luego se siguió por un segundo incidente donde se evidenciaron filtraciones de datos a través de correos fraudulentos reportados por titulares de datos-, la DNPDP interpreta que resulta insuficiente la documental aportada por CENCOSUD ya que de la misma, no surge que haya comunicado de manera efectiva a los titulares de datos los incidentes de seguridad investigados, de acuerdo a los deberes de seguridad de la información a su cargo (artículo 9 de la Ley Nº 25.326).

Que, en otras palabras, la DNPDP entiende que ambos incidentes han puesto en riesgo la protección de los datos personales de los titulares de datos en dos ocasiones y que CENCOSUD como responsable de tratamiento en el marco de sus obligaciones, debió haber reportado proactivamente a los usuarios afectados para que éstos pudieran estar prevenidos de posibles maniobras, y/o pudieran ejercer sus derechos en el marco de la Ley Nº 25.326 si lo consideraran pertinente.

Que en esta instancia la DNPDP considera conveniente dejar en claro que la Resolución AAIP Nº 47/2018, fue concebida -tal como figura en sus considerandos- *"[c]on el objetivo de facilitar el cumplimiento de la Ley N° 25.326 de Protección de los Datos Personales"* en relación a los deberes de seguridad del artículo 9, como así también para *"[a]ctualizar las medidas de seguridad que deben observar quienes hagan tratamientos de datos personales en archivos, registros, bancos y bases de datos públicos y privados, con el objeto de eliminar y/o mitigar los riesgos de dicha información"*. Dicha Resolución determina que dichas medidas serán llevadas a cabo por las organizaciones en el marco de su responsabilidad proactiva en atención a *"[l]a composición orgánica que mejor satisfaga sus intereses y funcionamiento"*, tal como figura en el Anexo I de la mentada Resolución.

Que en este orden de cosas, también corresponde merituar el tema tomando en cuenta brevemente algunos Principios internacionales.

Que en efecto, los estándares de protección aprobados por la Red Iberoamericana de Protección de Datos (RIPD), de la que la Agencia de Acceso a la Información Pública forma parte junto con otros países de la región, establece en su artículo 21 en relación al principio de seguridad que *"[c]uando el responsable tenga conocimiento de una vulneración de seguridad de datos personales ocurrida en cualquier fase del tratamiento, entendida como cualquier daño, pérdida, alteración, destrucción, acceso, y en general, cualquier uso ilícito o no autorizado de los datos personales aun cuando ocurra de manera accidental, deberá notificar a la autoridad de control y a los titulares afectados dicho acontecimiento, sin dilación alguna…"*

Que en la misma línea, los Principios actualizados del Comité Jurídico Interamericano sobre la Privacidad y la Protección de Datos Personales determinan sobre esta cuestión que las: *"[n]otificaciones permiten a las personas afectadas tomar medidas de protección y posiblemente tener acceso a los Datos y pedir que se corrijan Datos inexactos o el uso indebido de los Datos como consecuencia de su vulneración"*.

Que, en virtud de todo lo expuesto, y habiéndose analizado las defensas esgrimidas por CENCOSUD en su último descargo, se concluye que no se ven modificados los elementos de juicio que han sido tenidos en cuanto al momento de labrar el Acta de Constatación cuestionada, razón por la cual se ratifican las conductas allí atribuidas.

Que, ahora bien, con el fin graduar la sanción, los parámetros a tener en cuenta para su ponderación razonable,

conforme el Anexo II de la citada Disposición DNPDP Nº 7/05 son: Ante la comisión de INFRACCIONES GRAVES, la sanción a aplicar será de hasta CUATRO (4) APERCIBIMIENTOS, SUSPENSION DE UNO (1) a TREINTA (30) DIAS y/o MULTA DE PESOS VEINTICINCO MIL UNO ($ 25.001,00) a PESOS OCHENTA MIL ($ 80.000), mientras que en los casos de INFRACCIONES MUY GRAVES se aplicarán hasta SEIS (6) APERCIBIMIENTOS, SUSPENSIÓN DE TREINTA Y UNO (31) a TRESCIENTOS SESENTA Y CINCO (365) DIAS, CLAUSURA o CANCELACIÓN DEL ARCHIVO, REGISTRO O BANCO DE DATOS y/o MULTA de PESOS OCHENTA MIL UNO ($ 80.001,00) a PESOS CIEN MIL ($ 100.000,00).

Que, asimismo, conforme el punto 6 del Anexo II de la Disposición citada, la sanción a aplicar deberá graduarse considerando proporcionalidad respecto de la entidad de la falta, la naturaleza de la infracción cometida y los antecedentes de la empresa.

Que el punto 7 establece que cada infracción deberá ser sancionada en forma independiente, debiendo acumularse cuando varias conductas sancionables se den en las mismas actuaciones.

Que en razón de lo expuesto, corresponde aplicar la sanción contemplada en artículo 31 de la Ley N° 25.326, normas reglamentarias y complementarias; consistente en una multa por la suma de PESOS DOSCIENTOS NOVENTA MIL ($ 290.000,00) compuesta del siguiente modo: PESOS SESENTA MIL ($ 60.000,00) por cada una de las infracciones graves y de PESOS OCHENTA Y CINCO MIL ($85.000,00) por cada una de las infracciones muy graves cometidas por la empresa CENCOSUD.

Que de acuerdo a lo dispuesto por la Resolución AAIP N° 30 del 14 de mayo de 2018, ante ausencia del titular de la AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA y a los efectos de garantizar el normal desenvolvimiento del Organismo, se ha encomendado la atención del despacho y la resolución de los asuntos concernientes a la competencia del mismo, al Sr. Director Nacional de Protección de Datos Personales, Dr. Eduardo Hernán CIMATO, delegándose la firma correspondiente.

Que la presente medida se dicta en virtud de las atribuciones conferidas por los artículos 19 de la Ley Nº 27.275, por el artículo 29, inciso 1, apartado f) de la Ley N° 25.326 y la Resolución Nº 30/18.

Por ello,

EL DIRECTOR NACIONAL DE PROTECCION DE DATOS PERSONALES DE LA

AGENCIA DE ACCESO A LA INFORMACION PÚBLICA

RESUELVE:

ARTICULO 1.- Aplicase a la empresa CENCOSUD S.A., CUIT Nº 30-59036076-3, con domicilio en Suipacha 1111, Piso 18 de la Ciudad Autónoma de Buenos Aires, la sanción contemplada en artículo 31 de la Ley N° 25.326, normas reglamentarias y complementarias; consistente en una multa por la suma de PESOS

DOSCIENTOS NOVENTA MIL ($ 290.000,00), por haber incurrido en DOS (2) infracciones graves y DOS (2) infracciones muy graves, de acuerdo con el detalle expresado en los considerandos de la medida.

ARTICULO 2.- Notifíquese a la firma CENCOSUD S.A. haciéndole saber que la presente Resolución agota la vía administrativa, quedando expedita la acción judicial, la que deberá interponerse dentro de los NOVENTA (90) días hábiles judiciales de notificado el acto. Asimismo, podrá deducir recurso de reconsideración dentro del plazo de DIEZ (10) días, de acuerdo con lo normado por el artículo 84 del Decreto N° 1759/72, T.O. 2017.

ARTÍCULO 3º.- Hágase saber a la interesada que el 23 de abril de 2020, esta AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA dictó la Resolución N° 83, mediante la cual estableció el criterio de declarar inadmisibles los recursos de alzada, en consonancia con la Ley N° 27.483 que en su artículo 1° aprobó el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, suscripto en la ciudad de Estrasburgo, República Francesa, el día 28 de enero de 1981, y el Protocolo Adicional al Convenio, suscripto en la ciudad de Estrasburgo, República Francesa, el día 8 de noviembre de 2001.

ARTÍCULO 4°.- Tómese nota en el REGISTRO DE INFRACTORES LEY N° 25.326 y cumplido, archívese.

Digitally signed by CIMATO Eduardo Hernan
Date: 2021.09.17 11:02:43 ART
Location: Ciudad Autónoma de Buenos Aires

Eduardo Hernán Cimato
Director Nacional
Dirección Nacional de Protección de Datos Personales
Agencia de Acceso a la Información Pública

Digitally signed by Gestion Documental Electronica
Date: 2021.09.17 11:03:08 -03:00