



## **AVISO SUSTITUTORIO DE VIOLACIÓN DE DATOS**

### **De conformidad con las leyes federales y estatales, se proporciona este aviso sustitutorio**

El Departamento de Servicios de Salud del Condado de Los Ángeles (DHS, por sus siglas en inglés) sufrió un ataque cibernético malicioso que puede afectar la privacidad parcial de su identificación personal y/o de su información de salud. El 20 de junio de 2024, se enviaron avisos a las direcciones físicas conocidas de las personas potencialmente afectadas. Este aviso proporciona información sobre el ataque cibernético y es nuestra respuesta para aquellas personas de las que no teníamos suficiente información para notificar por correo. El DHS toma este incidente en serio, estamos trabajando y cooperando con las fuerzas del orden en este asunto.

### **¿Qué pasó**

El 6 de febrero de 2024, el DHS fue víctima de un ataque cibernético. En concreto, un hacker burló las medidas de seguridad multifactoriales de autenticación de la cuenta de Microsoft 365 de un empleado a través de un método comúnmente conocido como "spam de notificaciones push". Creemos que el ataque cibernético pudo haber permitido al atacante acceso a cierta información personal. Debido a la investigación en curso por parte de las fuerzas del orden, nos indicaron que deberíamos retrasar la notificación de este incidente a las partes afectadas, ya que el aviso público pudo haber obstaculizado su investigación. Para comunicar este asunto de manera proactiva proporcionamos información detallada sobre los pasos que puede seguir para proteger su información personal. Además, hemos implementado medidas de seguridad mejoradas para evitar que estas vuelvan a ocurrir en el futuro. Su privacidad y seguridad son de suma importancia para nosotros; estamos comprometidos en mantener los más altos estándares de protección de su información.

### **¿Qué información estuvo involucrada?**

La información identificada en la cuenta de correo electrónico potencialmente comprometida puede haber incluido su nombre y apellido, fecha de nacimiento, domicilio, número de teléfono, dirección de correo electrónico, número de Seguro Social, identificación emitida por el gobierno, número de registro médico, información del seguro médico (plan de salud y número de miembro) y/o información médica (por ejemplo, diagnóstico / afección, medicamentos, tratamiento, fechas de servicio).

Cada individuo puede haber sido afectado de manera diferente y no todos los elementos mencionados estaban presentes en el caso de cada individuo.

### **Lo que estamos haciendo**

El DHS ha implementado numerosas mejoras para reducir nuestra exposición a ataques similares por correo electrónico en el futuro. Al descubrir el ataque de phishing, actuamos con rapidez para desactivar la cuenta de correo electrónico afectada, restablecer y volver a crear una imagen de los dispositivos del usuario, bloqueamos los sitios web que se identificaron como parte de la campaña de phishing y pusimos en cuarentena todos los correos electrónicos entrantes sospechosos. Las fuerzas del orden fueron notificadas al descubrir el ataque de phishing e iniciaron una investigación delictiva. Además, se distribuyeron notificaciones a todos los miembros de la fuerza laboral del DHS para que tomen conciencia y

que estén atentos cuando revisen sus correos electrónicos, especialmente aquellos que incluyan enlaces o archivos adjuntos.

Luego de determinar que la cuenta se había visto comprometida, iniciamos una revisión exhaustiva, con la ayuda de una empresa forense líder en la industria, para identificar cualquier información personal o de salud personal que pudo haber sido afectada, e implementamos controles adicionales para minimizar el riesgo de futuros ataques de phishing contra las cuentas de correo electrónico del DHS.

Además, mejoramos la capacitación para identificar y responder a los ataques de phishing como parte del programa continuo de crear conciencia sobre la seguridad cibernética del DHS.

Además de notificar a las personas potencialmente afectadas por este incidente, hemos notificado a la Oficina de Derechos Civiles del Departamento de Salud y Servicios Humanos de los Estados Unidos, al Departamento de Salud Pública de California, a la Oficina del Fiscal General del Estado y a otras agencias según lo exija la ley y/o el contrato.

Buscamos mantenernos a la vanguardia de las amenazas continuas que avanzan rápidamente contra los grandes sistemas de datos. El DHS permanece vigilante en sus esfuerzos por proteger la información confidencial y continúa fortaleciendo su programa de privacidad y seguridad de la información para implementar medidas de salvaguarda y así prevenir y/o reducir los ataques cibernéticos.

### **Lo que usted puede hacer**

Si bien el DHS no puede confirmar que su información haya sido utilizada indebidamente, alentamos a los pacientes a revisar el contenido y la exactitud de la información de su registro médico con su profesional de la salud, y que permanezca atento a cualquier actividad sospechosa en cualquiera de sus cuentas.

Para ayudar a aliviar las preocupaciones y restaurar su confianza después de este incidente, hemos contratado los servicios de Kroll para proporcionarle monitoreo de identidad durante un año sin costo alguno. Kroll es un líder mundial en mitigación y respuesta a riesgos, y su equipo tiene amplia experiencia ayudando a las personas que han sufrido una exposición involuntaria de sus datos confidenciales.

Para obtener información adicional, consulte "Pasos que puede tomar para protegerse contra el robo de identidad y el fraude", publicado en este sitio web: <https://dhs.lacounty.gov>. Si cree que su información personal se está utilizando de manera indebida, también puede comunicarse con la policía local para presentar un informe policial.

### **Para más información**

Entendemos que puede tener preguntas sobre este incidente que no se mencionan en esta carta. Hemos establecido un centro dedicado de llamadas que está disponible de forma gratuita en los Estados Unidos en 1-866-898-8099 de 6:00 a.m. a 5:00 p.m., horario del Pacífico (excepto los fines de semana y los principales días festivos de los Estados Unidos). También puede visitar el siguiente sitio web para obtener más información: <https://dhs.lacounty.gov>.