HOSPITAL
Los Madroños

Estimados proveedores,

En cumplimiento del artículo 34 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD), Silvia Beatriz, S.L. (en adelante, "el hospital" u "Hospital Los Madroños") les informa de que el pasado 07 de marzo de 2025 detectamos una **brecha de seguridad** en nuestros sistemas. Esta brecha se debió a un **ataque de tipo ransomware**, atribuido al grupo **Qilin**, que logró cifrar (encriptar) nuestros sistemas informáticos y **extraer copias no autorizadas de datos** almacenados en ellos.

Por este motivo, un número no determinado de datos de carácter personal han sido afectados.

Lamentamos profundamente lo ocurrido y queremos brindarles información clara sobre lo sucedido, las medidas tomadas y cómo proteger sus datos.

1. **Naturaleza de la brecha de seguridad:** el ataque ransomware **Qilin** infectó la red interna del hospital, **bloqueando temporalmente el acceso** a la información al cifrarla. Adicionalmente, los atacantes **extrajeron datos confidenciales** durante el incidente, que, posteriormente, **han publicado en su blog** sin que actualmente hayamos podido determinar con precisión su alcance. En resumen, se produjo tanto la **encriptación** de nuestros archivos como la **exfiltración** de información y **publicación**.

2. **Datos personales afectados:** tras un análisis exhaustivo, confirmamos que los datos de proveedores comprometidos por esta brecha pueden incluir:

    - **Información de cuenta bancaria:** los números de cuenta (IBAN) que nuestros proveedores nos han facilitado para la gestión de pagos y facturas. Estos datos financieros estuvieron accesibles a los atacantes. Si bien un IBAN por sí solo no permite retirar dinero, su divulgación indebida puede facilitar intentos de fraude (por ejemplo, falsificación de domiciliaciones bancarias o suplantación en comunicaciones de pago).

    - **Personas de contacto y sus datos:** los nombres y apellidos de las personas de contacto que figuran en nuestras fichas de proveedor, junto con sus datos de identificación profesional y de contacto (tales como cargo, número de teléfono corporativo, dirección de correo electrónico de trabajo y, en algunos casos, DNI/NIF si nos fue proporcionado para contratos). Esta información de contacto podría ser utilizada indebidamente por terceros para intentar engaños o comunicaciones fraudulentas dirigidas a su empresa.

      Es importante señalar que **no se han comprometido datos comerciales sensibles** (por ejemplo, detalles de contratos, precios, propiedad intelectual, etc.) más allá de los mencionados datos de cuenta y contactos. El alcance se ha limitado a información administrativa básica necesaria para nuestra relación comercial. Aun así, entendemos que la privacidad de estos datos es crucial y por ello estamos actuando con máxima diligencia.

3. **Medidas adoptadas por el hospital:** tan pronto como tuvimos conocimiento del incidente, activamos nuestro **protocolo de respuesta ante brechas de seguridad**. A

continuación, detallamos las principales medidas implementadas para resolver la situación y mitigar el impacto:

- **Aislamiento y contención:** desconectamos de inmediato los sistemas afectados para impedir la propagación del ransomware a otros sistemas del hospital. Esto limitó el alcance del ataque y protegió datos adicionales.

- **Equipo de respuesta especializado:** nuestros técnicos de informática, junto con expertos externos en ciberseguridad, trabajaron intensivamente para **eliminar el malware** de la red y asegurar cada equipo. Paralelamente, estamos llevando a cabo una **investigación forense** para determinar con precisión cómo ocurrió el ataque y qué información fue accedida.

- **Recuperación de datos:** estamos restaurando los sistemas e historiales desde **copias de seguridad seguras**. Gracias a estas copias de respaldo, hemos podido **recuperar la mayoría de la información cifrada** y reanudar los servicios clínicos con normalidad, minimizando la interrupción en la atención sanitaria.

- **Notificación a autoridades:** hemos informado puntualmente de la brecha a las autoridades competentes. En concreto, se notificó a la Agencia Española de Protección de Datos (AEPD) y se presentó denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado. Estas entidades están al tanto del incidente y colaboran con nosotros en las investigaciones.

- **Refuerzo de la seguridad:** como medida preventiva adicional, el hospital ha **reforzado sus medidas de seguridad**. Esto incluye actualizar y **fortalecer los sistemas de protección** (firewalls, antivirus, sistemas de detección), aplicar parches de software, y establecer protocolos adicionales de **monitorización 24/7** para detectar cualquier actividad anómala de inmediato. También hemos recordado y mejorado nuestras políticas internas de contraseñas y formación al personal en materia de ciberseguridad.

- **Asistencia a los empleados afectados:** reconocemos la inquietud que este incidente pueda generar. Por ello, hemos habilitado recursos específicos para **asesorar y apoyar a los empleados** en la protección de sus datos personales. Nuestro departamento de Recursos Humanos, junto con el Delegado de Protección de Datos, atenderá individualmente cualquier caso en que un empleado pueda haber sufrido consecuencias derivadas de esta brecha, brindando orientación sobre cómo proceder.

4. **Impacto que puede suponer esta brecha de seguridad:** en base a esta brecha de seguridad, se podrían generar consecuencias tales como, menoscabo en sus derechos fundamentales (salud y privacidad), suplantación de identidad o fraude, entre otros.

Con estas acciones, Hospital Los Madroños buscamos resolver la situación lo antes posible y **prevenir que algo así vuelva a ocurrir**. Les aseguramos que la atención médica continúa brindándose con normalidad y que la seguridad de sus datos es ahora, más que nunca, nuestra prioridad.

HOSPITAL
Los Madroños

Recomendaciones para proteger sus datos personales: entendemos su preocupación y recomendamos encarecidamente tomar **medidas de precaución adicionales** para proteger su información personal:

- **Supervisión de cuentas bancarias:** aunque el conocimiento de un número de cuenta bancaria por terceros no autoriza movimientos, **vigilen de cerca los movimientos** en la cuenta cuyo IBAN nos han proporcionado. Revise periódicamente los extractos bancarios de su empresa para detectar posibles domiciliaciones o cargos no reconocidos. Si observaran alguna actividad extraña (por ejemplo, un adeudo que su empresa no esperaba), **infórmenlo de inmediato a su entidad bancaria** para su anulación y tomen nota de los detalles, y, si procede, solicitar la devolución del importe. Además, según lo establecido en el Real Decreto-Ley 19/2018, el usuario bancario dispone de un plazo de trece (13) meses desde la fecha del cargo para solicitar la devolución de recibos no autorizados.

  Mantener este control durante los próximos meses es recomendable como medida preventiva.

  Aprovechamos para informarle que, en lo relativo los datos de cuenta bancaria que de acuerdo con la Directiva de Servicios de Pago (PSD2), la Directiva (UE) 2015/2366 y el Real Decreto-Ley 19/2018 de servicios de pago, el uso de una cuenta corriente como medio de pago requiere una autenticación reforzada del cliente. Esto dificulta que los ciberdelincuentes puedan utilizar las cuentas bancarias para realizar pagos sin autorización. Por ello, conforme a la normativa bancaria, no pueden realizarse cargos en cuentas bancarias sin el consentimiento expreso del titular.

- **Verificación de comunicaciones financieras:** estén alerta ante **posibles intentos de fraude o suplantación** relacionados con pagos. Por ejemplo, si reciben correos o llamadas supuestamente del hospital solicitando **cambios de cuenta bancaria para los pagos** o indicando **modificaciones inesperadas en los acuerdos de facturación**, por favor **verifiquen dicha comunicación por vías oficiales** antes de actuar. Del mismo modo, si alguien contacta en nombre de su empresa pidiendo al hospital redirigir pagos a una cuenta diferente, nosotros aplicaremos esta cautela y les llamaremos para confirmar. Esta doble verificación mutua nos ayudará a frustrar intentos de fraude que aprovechen la información filtrada.

- **Protección de las cuentas de sus empleados de contacto:** si las personas de contacto de su organización tienen credenciales de acceso a plataformas compartidas con el hospital (por ejemplo, portales de proveedores, sistemas de pedido en línea, etc.), **recomienden a dichos empleados cambiar sus contraseñas** por seguridad. Asegúrense de que utilicen contraseñas robustas y, si es posible, habiliten la autenticación en dos pasos en esas plataformas. Esto reducirá la posibilidad de accesos indebidos si algún ciberdelincuente intenta usar la información obtenida para infiltrarse en sistemas de colaboración entre nuestras entidades.

- **Cautela con correos y llamadas sospechosas:** dado que los datos de contacto se vieron comprometidos, existe la posibilidad de que los atacantes u otros terceros malintencionados intenten **engañar a sus empleados** de contacto. Podrían recibir correos falsos aparentando provenir del hospital (con remitentes similares a los nuestros) o incluso llamadas telefónicas fraudulentas. Si algún mensaje les resulta fuera de lugar o pide información sensible, **tomen medidas de verificación**: por ejemplo, contacten con su interlocutor habitual en el hospital por la vía ya conocida para confirmar la solicitud. Insistimos en que **nuestro hospital nunca les pedirá**

información confidencial por medios inseguros. Ante la menor duda, consulten con nosotros directamente antes de responder.

- **Notifiquen incidentes o sospechas:** si su empresa o personal detecta algún intento de estafa, suplantación o uso indebido de la información (derivado de esta brecha u otra circunstancia), por favor **háganoslo saber de inmediato**. Pueden contactar a nuestro equipo (ver abajo) para informar de cualquier actividad sospechosa relacionada. Asimismo, consideren **informar a las autoridades** si llegan a concretarse intentos de fraude contra su empresa. Compartir esta información nos permitirá alertar a otros proveedores y reforzar las medidas conjuntas de seguridad.

Contacto para dudas y asistencia: Ponemos a su disposición **nuestros canales de contacto** para cualquier pregunta, aclaración o necesidad de apoyo relacionado con esta brecha de seguridad. Pueden comunicarse con el **Delegado de Protección de Datos del Hospital** o con el equipo de seguridad de la información a través de:

- Correo electrónico: **dpo@lmh.es**
- Teléfono gratuito de asistencia: **918 16 35 26**

No duden en contactarnos; estamos aquí para ayudarles en todo lo que necesiten.

Nuestro objetivo es **proteger su privacidad** y atender sus inquietudes con total transparencia.

Finalmente, expresamos nuestras **sinceras disculpas por los inconvenientes** que esta situación pueda ocasionarles. Sabemos que confían en nosotros para manejar sus datos de manera segura, y lamentamos profundamente que haya ocurrido este incidente a pesar de las medidas de protección con las que contábamos. Vamos a continuar trabajando arduamente para mejorar nuestros sistemas de seguridad y evitar que algo similar vuelva a suceder.

Transparencia y comunicación pública: Con el fin de garantizar que esta información llegue a todos los afectados, les informamos que **este comunicado también ha sido publicado en periódicos de tirada nacional** como El Mundo, La Razón y 20 Minutos con fecha 14 y 15 de marzo. De esta manera, reforzamos nuestro compromiso con la transparencia y la rápida difusión de la información importante.

Atentamente,

La Dirección del Hospital Los Madroños.