Anexo de Protección de Datos ("Anexo") a la Orden de Pedido

1 El presente Anexo de Protección de Datos se aplica en relación con la Orden de Pedido (incluidos los Términos y Condiciones de Viajes de Negocios y/o los Términos y Condiciones de los Servicios de Reuniones y Eventos, según proceda) (conjuntamente, el "Acuerdo") entre Reed & Mackay España S.A.U. ("R&M") (Registrada en España con el nº A-08649477) con domicilio social en Calle Carretas 14, 8 H-I, 28012, Madrid, y usted, el Cliente. Los términos definidos que se utilicen en otras partes del Contrato tendrán el mismo significado en el presente Anexo. Cuando R&M procese Datos, R&M:

1.1 utilizará los Datos únicamente para:

(a) cumplir sus obligaciones en virtud del presente Acuerdo y tratar dichos Datos de conformidad con las instrucciones escritas del Cliente; y/o

(b) cumplir con la Legislación de Protección de Datos o las leyes de cualquier otro estado miembro de la Unión Europea (siempre que R&M haya informado al Cliente de dicho requisito antes del tratamiento correspondiente (a menos que la Ley Pertinente prohíba dicha notificación));

1.2 con sujeción a los Párrafos 2, 4 y 5 (inclusive) de este Anexo, implementará y mantendrá medidas técnicas y organizativas apropiadas para proteger los Datos tratados en relación con este Acuerdo de la destrucción accidental o ilegal, pérdida, alteración, divulgación o acceso no autorizados y tomará todas las medidas requeridas por él de conformidad con el Artículo 32 del GDPR ("seguridad del trataamiento");

1.3 tomará todas las medidas razonables para garantizar la fiabilidad de cualquiera de los Empleados de R&M o Personal que tenga acceso a los Datos tratados en relación con el presente Acuerdo y se asegurará de que todos dichos Empleados de R&M o Personal estén sujetos a obligaciones exigibles de confidencialidad;

1.4 teniendo en cuenta la naturaleza del tratamiento, asistirá al Cliente mediante medidas técnicas y organizativas adecuadas, en la medida de lo posible, para el cumplimiento de la obligación del Cliente de responder a las solicitudes de los interesados que ejerzan sus derechos en virtud del Capítulo III delGDPR;

1.5 ayudará al Cliente a garantizar el cumplimiento por parte del Cliente de sus obligaciones en virtud de los artículos 32 a 36 del GDPR ("seguridad del tratamiento", "notificación de violación de datos personales...", "evaluación del impacto de la protección de datos" y "consulta previa"), teniendo en cuenta la naturaleza del tratamiento y la información de que dispone R&M;

1.6 notificará al Cliente sin demora indebida, y en cualquier caso en el plazo de 48 horas, cualquier violación de la seguridad que provoque la destrucción accidental o ilícita, la pérdida, la alteración, la difusión o el acceso no autorizados a los Datos tratados por R&M en relación con el presente Acuerdo;

1.7 pondrá a disposición del Cliente, en un plazo razonable tras la notificación del Cliente, toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente Anexo y permitir y contribuir a las auditorías, incluidas las inspecciones, llevadas a cabo por el Cliente o por otro auditor autorizado por el Cliente, siempre que dichas auditorías y/o inspecciones se produzcan únicamente en una (1) ocasión en un periodo de doce (12) meses, que dichas inspecciones y/o auditorías se limiten estrictamente a las disposiciones de R&M para el cumplimiento del presente Anexo, que dichas inspecciones y/o auditorías se lleven a cabo en horario laboral normal y que el Cliente (o el tercero pertinente que lleve a cabo dicha auditoría) notifique a R&M dicha auditoría y/o inspección con una antelación razonable y por escrito, y el alcance de dicha auditoría y/o inspección se acuerde con R&M antes de su inicio;

1.8 tendrá derecho a transferir Datos fuera del Espacio Económico Europeo siempre que se establezcan las salvaguardias adecuadas en virtud de la Legislación de Protección de Datos, incluyendo, sin limitación, cuando proceda: (a) para las transferencias de Datos desde el Espacio Económico Europeo las Cláusulas Contractuales Tipo de la UE estén en vigor; (b) para las transferencias de Datos desde el Reino Unido, la Adenda del Reino Unido en vigor, siempre que esto siga siendo un mecanismo de transferencia válido en virtud del GDPR del Reino Unido; (c) cualquier otro mecanismo de transferencia válido esté en vigor en virtud de la Legislación de Protección de Datos. Para evitar cualquier duda y con sujeción al apartado 4 siguiente, el Cliente reconoce y acepta que R&M no está obligado a suscribir ninguna cláusula contractual estándar (incluidas, entre otras, las Cláusulas Contractuales Tipo de la UE o la Adenda del Reino Unido) u otros acuerdos con los Proveedores de Servicios;

1.9 notificar inmediatamente al Cliente, si en opinión de R&M, cualquier instrucción o dirección del Cliente infringe la Legislación de Protección de Datos u otra legislación aplicable sobre protección de datos de la Unión Europea o los Estados miembros; y

1.10 a elección del Cliente, eliminar o devolver al Cliente todos los Datos cuando los Servicios dejen de prestarse al Cliente, y eliminar todas las copias existentes en ese momento (a menos que la legislación aplicable exija que R&M las conserve).

2 El Cliente reconoce y acepta, y procurará que los Viajeros y Usuarios reconozcan y acepten, que es necesario para que R&M proporcione Datos a Proveedores de Servicios (estén o no dentro del EEE) con el fin de prestar Servicios.

3 El Cliente reconoce y acepta que R&M estará autorizada a utilizar Subencargados del Tratamiento en relación con el tratamiento de Datos en nombre del Cliente para la prestación de los Servicios en virtud del presente Acuerdo. La lista de Subencargados del Tratamiento utilizados por R&M está disponible aquí. R&M seguirá siendo responsable de los actos u omisiones de sus Subencargados del Tratamiento. R&M se asegurará de tener un contrato por escrito con los Subencargados del Tratamiento que contenga condiciones para la protección de los Datos que no sean menos protectoras que las condiciones establecidas en el presente Anexo. R&M informará al Cliente de cualquier cambio en la lista de Subencargados del Tratamiento, incluida la adición de nuevos Subencargados del Tratamiento. Si el Cliente se opone a un cambio en la lista de Subencargados del Tratamiento, el Cliente deberá notificar a R&M por escrito dentro de los 15 días posteriores a la publicación de la lista actualizada de Subencargados del Tratamiento. Si el Cliente proporciona a R&M dicha notificación, siempre que sea posible, R&M cumplirá con sus obligaciones en virtud de este Acuerdo sin el tratamiento de Datos en relación con este Acuerdo por parte de los nuevos Subencargados del Tratamiento. Sin embargo, si no es razonablemente factible que R&M cumpla con sus obligaciones en virtud de este Acuerdo sin el tratamiento de Datos en relación con este Acuerdo por parte de los nuevos Subencargados del Tratamiento, R&M notificará al Cliente de ello, y el Cliente tendrá derecho a rescindir este Acuerdo con treinta (30) días de anticipación notificación por escrito a R&M. En el caso de que el Cliente no se oponga a cualquier cambio o adición a la lista de Subencargados del Tratamiento dentro de los 15 días posteriores a la publicación de la lista actualizada por parte de R&M, se considerará que el Cliente ha aprobado cualquier cambio y/o adición a la lista de Subencargados del Tratamiento. R&M sigue siendo responsable de cualquier acto u omisión de sus Subencargados del Tratamiento. R&M se asegurará de tener un contrato escrito con los Subencargados del Tratamiento que contenga términos para la protección de Datos que no sean menos protectores que los términos establecidos en este Anexo.

4 Sin perjuicio de lo dispuesto en el apartado 2 anterior, y sin perjuicio de cualquier otra disposición del presente Acuerdo, el Cliente:

(a) consiente por la presente que R&M transfiera los Datos a cualquier Proveedor de Servicios (esté o no dentro del EEE o del Reino Unido) a efectos de la prestación de los Servicios de conformidad con el presente Acuerdo; y

(b) se asegurará de que los Viajeros y los Usuarios hayan dado, cuando sea necesario, su consentimiento para que R&M transfiera los Datos de los Viajeros y de los Usuarios a los Proveedores de Servicios con el fin de prestar los Servicios de conformidad con el presente Acuerdo.

5 A la luz del párrafo 2 anterior, R&M hará todo lo posible por ayudar al Cliente a responder ante cualquier incumplimiento (ya sea por acción u omisión) por parte de un Proveedor de Servicios en el tratamiento de los Datos de acuerdo con los métodos apropiados y estándar del sector, pero R&M no tendrá ninguna responsabilidad ante el Cliente, cualquier miembro del Grupo del Cliente o cualquier Viajero o Usuario (ya sea contractual, extracontractual (incluida la negligencia o el incumplimiento de obligaciones legales), falso testimonio o de otro tipo) que surja de o en relación con el tratamiento, uso, uso indebido, pérdida, daño o corrupción de Datos por parte de cualquier Proveedor de Servicios, o que infrinja de otro modo los derechos de una persona en relación con los Datos.

6 Sin perjuicio de lo dispuesto en los apartados 2, 4 y 5 anteriores (inclusive) del presente Anexo, el Cliente se asegurará de que se han establecido todas las bases legales necesarias, incluida, en su caso, la obtención del consentimiento, y proporcionará a los Viajeros y Usuarios toda la información necesaria para que los Datos puedan ser facilitados legalmente a R&M de conformidad con la Legislación de Protección de Datos.

7 El Cliente reconoce y acepta que el Anexo 1 del presente Anexo contiene determinados detalles relativos al tratamiento de Datos por parte de R&M en virtud del presente Acuerdo.

8 El Cliente reconoce y acepta que correrá con los gastos y reembolsará a R&M los costes y gastos razonables en que incurra R&M para prestar la asistencia descrita en los apartados 1.4 y 1.5 anteriores.

9 Si fuera necesario para el cumplimiento de la Legislación de Protección de Datos y salvo que lo prohíba la legislación aplicable, R&M deberá: (i) informar al Cliente sin demora indebida de cualquier solicitud, orden o demanda similar por parte de un tribunal, autoridad competente, aplicación de la ley u otro organismo gubernamental ("Solicitud de Aplicación de la Ley") relacionada con el tratamiento de Datos en virtud del presente Acuerdo y proporcionar al Cliente la oportunidad de oponerse a cualquier Solicitud de Aplicación de la Ley; y (ii) tomar todas las medidas razonables para evitar la divulgación de cualquier Dato procesado por R&M en virtud del presente Acuerdo en respuesta a una Solicitud de Aplicación de la Ley sin el consentimiento expreso previo por escrito del Cliente.

Anexo 1

Actividades de tratamiento de datos

Categorías de datos	Datos del viajero y/o de la persona que reserva: título, nombre, segundo nombre, apellidos, nombre conocido (si es diferente), sexo, fecha, lugar y país de nacimiento, país de residencia, nacionalidad, estado civil; ubicación del viajero: destinos y lugares del viaje. Información de la empresa: nombre de la empresa, departamento, centro de costes, número de cuenta, cargo, número de empleado Principales datos de contacto: direcciones (particular, oficinas, etc.), números de teléfono, fax, teléfono móvil y dirección de correo electrónico. Información sobre la agencia de viajes/PA: nombre, número de teléfono, dirección de correo electrónico Métodos de pago - tipo de tarjeta, número de tarjeta, fecha de caducidad, preferencias de uso, débito/crédito, personal/empresarial Documentos Pasaporte - país del pasaporte, país de expedición, número de pasaporte, nombre, segundo nombre, apellidos, fecha de expedición, fecha de caducidad, datos biométricos (sí/no) Visado (incluidos ESTA, Redress, Schengen, permiso de trabajo, Global Entry).: país de visado, país de expedición, tipo de visado, número de documento, fecha de expedición y fecha de caducidad TSA - Número TSA, fecha de inicio, fecha de caducidad Permisos de conducción - país, número de permiso, nombre, segundo nombre, apellidos, fecha de inicio, fecha de caducidad, provisional (sí/no), internacional (sí/no) Documentos de identidad - país, número de documento de identidad, nombre, segundo nombre, apellidos, fecha de inicio, fecha de caducidad Vacunas, Covid e información sanitaria necesaria para las reservas Preferencias de viaje Avión - tipo de asiento, aeropuerto de origen, preferencia de facturación en línea, tipo de comida Coche - categoría, estilo, transmisión, combustible/aire, navegador por satélite (sí/no), Ferrocarril - asignación de asientos, tipo de comida Eurostar - número de vagón, número de asiento, tipo de asiento, asignación de asiento, tipo de comida Hotel - fumadores/no fumadores, tipo de habitación preferida Requisitos de accesibilidad para el viaje Afiliaciones - tarjetas de fidelidad - tipo de servicio, proveedor, número de afiliación, fecha de caducidad, estatus, nivel Aficiones personales
Categorías de interesados	Empleados e invitados del cliente, y otras personas para las que el cliente requiera desplazamientos
Operaciones de tratamiento	Prestación de servicios relacionados con los viajes
Propósitos	Prestación de servicios relacionados con los viajes
Duración	Finanzas - duración del contrato + 7 años Perfiles: duración del contrato, revisión anual y supresión a petición del cliente

Anexo 2

Medidas técnicas y organizativas, incluidas las medidas técnicas y organizativas para garantizar la seguridad de los datos

Descripción de las medidas técnicas y organizativas aplicadas por el importador o importadores de datos (incluidas las certificaciones) pertinentes para garantizar un nivel de adecuado, teniendo en cuenta la naturaleza, el alcance, el contexto y la finalidad del tratamiento, as í como los riesgos para los derechos y libertades de las personas f ísicas.

Versión 2.4 - Enero de 2023 (actualizada periódicamente por R&M)

DEFINICIONES

"Personal" se refiere a los empleados, contratistas o consultores de Reed & Mackay que participan en el servicio que Reed & Mackay presta a sus clientes.

"Datos" significa los datos del Cliente proporcionado a Reed & Mackay por el Cliente (Controlador de Datos) de conformidad con cualquier Acuerdo de Procesamiento de Datos, Cláusulas Contractuales Estándar y/o contratos entre el Cliente y Reed & Mackay.

INTRODUCCIÓN

El Equipo Ejecutivo de Reed & Mackay reconoce la importancia de la Seguridad de la Información, y mantener los más altos estándares de confidencialidad, integridad y disponibilidad de la información interna, de clientes y proveedores es fundamental para nuestra Visión "Ser la empresa de viajes, asesoría y eventos más valorada, recomendada y emprendedora del mundo".

Tal y como se describe en este documento, Reed & Mackay mantiene un conjunto de Medidas de Seguridad Técnicas y Organizativas en línea con las Mejores Prácticas y Estándares de la Industria y Certificaciones que mantenemos para mitigar los riesgos para los datos, los activos de información, el servicio, el rendimiento, la confianza del cliente u otras áreas del negocio que puedan resultar de un fallo en la Seguridad de la Información.

1. CERTIFICACIONES

1.1. Reed & Mackay mantiene ISO/IEC 27001, la norma internacional para la Gestión de la Seguridad de la Información,las certificaciones ISO 22301 - Gestión de la Continuidad del Negocio, ISO 9001 - Gestión de la Calidad, e ISO 14001 - Gestión Medioambiental. también cuenta con la certificación PCI-DSS Reed & Mackay , que también es un requisito previo para la concesión de licencias de la IATA y que, por consiguiente, Reed & Mackay se toma muy en serio. - The Payment Card Industry - Data Security Standard

1.2. Las certificaciones se mantienen mediante un programa de auditorías externas e internas, que incluyen auditorías internas periódicas y externas anuales, y actividades continuas de mejora.

2. SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

2.1. Las Políticas de Seguridad de la Información de establecen una dirección clara para la Seguridad de la Información y demuestran el apoyo y el compromiso con la gestión de la Seguridad de la Información en toda la empresa. Reed & Mackay

2.2. La seguridad de la información se gestiona mediante un estricto conjunto de controles, que incluyen políticas, procesos, procedimientos, software y funciones de hardware que constituyen el Sistema de Gestión de la Seguridad de la Información (SGSI) de Reed & Mackay Estos controles se supervisan, revisan y, en caso necesario, se mejoran para garantizar el cumplimiento de los objetivos específicos de seguridad y de negocio.

2.3. Todo el personal recibe un programa de iniciación y formación completo y obligatorio al incorporarse a la empresa, así como una actualización anual del cumplimiento, que incluye la seguridad de la información y la protección de datos.

2.4. La responsabilidad última en materia de seguridad de la información recae en el Director de Seguridad de la Información del Grupo, pero esta responsabilidad se ejerce a través de la función designada de Jefe de Seguridad de la Información, que es el principal responsable de la seguridad de la información, la gestión de los riesgos de seguridad de la información y de los incidentes de seguridad en Reed & Mackay y actúa como punto central de contacto en materia de seguridad de la información tanto para el personal como para las organizaciones externas.

2.5. Los Jefes de Departamento son responsables de la aplicación de las políticas de seguridad de la información en sus áreas de actividad y del cumplimiento de las mismas por parte de su personal. Todo el personal es responsable de la seguridad de la información, garantizando el cumplimiento de las políticas, procesos y procedimientos pertinentes de la empresa, la concienciación general sobre la importancia de la seguridad de la información y los riesgos potenciales, y la notificación de cualquier incidente, suceso o posible deficiencia.

3. SEGURIDAD DE LOS RECURSOS HUMANOS

3.1. Reed & Mackay colabora estrechamente con nuestras agencias de contratación para garantizar que se cumplan en nuestro nombre los requisitos de selección previa a la contratación.

3.2. Reed & Mackay utiliza los servicios de una empresa externa de selección de empleados para llevar a cabo la investigación de antecedentes de acuerdo con la Norma Básica de Seguridad del Personal (BPSS) del Gobierno del Reino Unido en todo el personal, independientemente de su función.

3.3. En los contratos del personal existen cláusulas de confidencialidad que protegen adecuadamente la confidencialidad de los Datos.

3.4. Existe un proceso disciplinario para tratar el incumplimiento de las políticas y requisitos de seguridad.

3.5. En caso de cese de la relación laboral, se revoca el acceso del personal en su último día laborable y el cesante devuelve todo el equipo y la propiedad intelectual.

4. GESTIÓN DE ACTIVOS Y SEGURIDAD DE LOS DATOS

4.1. Se identifican los activos asociados a la información y las instalaciones de tratamiento de la información y se mantiene un inventario de activos.

4.2. La información y los datos se clasifican y gestionan de acuerdo con una Política de Clasificación de la Información y Gestión de Datos aprobada por la dirección.
4.3. Sólo los dispositivos de confianza tienen acceso a los recursos de la red corporativa de Reed & Mackay. Entre ellos se incluyen los ordenadores conectados al dominio de Reed & Mackay y los dispositivos móviles que se han registrado en Reed & Mackay la solución de gestión de dispositivos móviles de y cumplen las políticas de seguridad.
4.4. Los requisitos de los controles de seguridad para dispositivos móviles personales y emitidos por Reed & Mackay se definen en la política de dispositivos móviles y personales. Los controles incluyen, entre otros, cifrado, borrado remoto y puertos USB deshabilitados.
4.5. Todos los terminales están encriptados. Los puertos USB y el uso de soportes extraíbles están restringidos.
4.6. Se aplican medidas técnicas de DLP, así como una política de Clear Desk & Clear Screen para mitigar el riesgo de fuga de datos y divulgación involuntaria de los Datos.
4.7. Existe una Política de Retención de Datos y un Calendario de Retención de Datos para definir los requisitos de retención de datos en línea con el GDPR y la Ley de Protección de Datos, así como los requisitos de eliminación segura de datos confidenciales en soportes físicos o electrónicos según las normas / mejores prácticas de seguridad reconocidas de la industria de TI (por ejemplo, normas aprobadas por CESG o DOD).
4.8. Los soportes que contienen cualquier información se destruyen utilizando medios seguros de eliminación de acuerdo con las normas de destrucción de datos aprobadas por WEEE (Waste Electrical and Electronic Equipment) y CESG (Communications Electronics Security Group). Operaciones de TI mantiene registros.
4.9. La documentación se destruye de forma segura utilizando trituradoras de corte transversal o recurriendo a terceros autorizados que presten servicios conforme a la norma de trituración de seguridad BS EN 15713 y al nivel de seguridad DIN P-3, como mínimo, adecuado para documentos confidenciales.

5. CONTROL DE ACCESO

5.1. Existe un modelo de control de acceso basado en funciones que asigna funciones a las personas en función de su trabajo y de la necesidad de conocerlas.
5.2. Se siguen los principios de separación de funciones y mínimo privilegio, y el acceso privilegiado se concede previa aprobación documentada de la alta dirección.
5.3. Los derechos administrativos de TI privilegiados se proporcionan a través de un ID de usuario separado (cuenta elevada) del ID de usuario normal del usuario.
5.4. Supervisamos todos los eventos asociados al inicio de sesión en servidores y estaciones de trabajo con cuentas administrativas, así como los cambios/modificaciones en los grupos de privilegios.
5.5. Las revisiones de los derechos de acceso se llevan a cabo periódicamente con una frecuencia que depende de la criticidad del activo de información y que varía entre trimestral y anualmente.
5.6. La política de contraseñas de Reed & Mackay se define del siguiente modo: Las contraseñas deben contener un mínimo de 12 caracteres, al menos una letra mayúscula, una letra minúscula y un número o carácter especial. Las contraseñas deben evitar los caracteres internacionales (no ASCII), no deben incluir palabras del diccionario ni información sobre el usuario (como el ID de usuario, nombres de familiares, fecha de nacimiento, etc.), deben cambiarse al menos una vez cada 90 días y no pueden ser iguales a las 24 contraseñas utilizadas anteriormente.
5.7. Las cuentas de usuario se bloquean después de 5 intentos de inicio de sesión no válidos y permanecerán bloqueadas hasta que un administrador o el usuario las desbloquee (esto último mediante autoservicio y autenticación multifactor).
5.8. La autenticación multifactor se aplica a todos los usuarios y cuentas administrativas de Reed & Mackay.

6. CRYPTOGRAFÍA

6.1. Tal y como se define en Reed & Mackayla Política de Criptografía de , se emplean controles criptográficos para proteger los datos confidenciales tanto en tránsito como en reposo.
6.2. El cifrado en dispositivos móviles se aplica a través de las políticas de Microsoft Intune Endpoint Manager
6.3. El cifrado de la base de datos PII se realiza a través de Thales CipherTrust (cifrado AES de 256 bits, tokenización de datos y servicios de cifrado).
6.4. El cifrado de la base de datos se realiza mediante el cifrado transparente de datos (TDE) AES-256.
6.5. Todo el tráfico desde y hacia nuestras aplicaciones de cara al público (sitios web y aplicación móvil) utiliza certificados HTTPS emitidos por GlobalSign Certificate Authority y cifrados con TLS 1.2 o superior.
6.6. Todas las copias de seguridad están encriptadas.

7. SEGURIDAD DE LAS OPERACIONES

7.1. Los cambios en los entornos de producción se controlan de acuerdo Reed & Mackaycon la política de gestión de cambios informáticos de .
7.2. Controles de detección, prevención y recuperación de programas maliciosos para protegerse mediante una solución antimalware de última generación.
7.3. Existe un proceso integral de gestión de parches. Los parches y las actualizaciones de seguridad se despliegan mensualmente, o con mayor frecuencia si se identifica un riesgo significativo para la seguridad. La gestión de parches está sujeta al control de cambios informáticos y al proceso de gestión de cambios informáticos.
7.4. Existe un programa técnico de gestión de vulnerabilidades que incluye un programa continuo de corrección. Las vulnerabilidades se detectan mediante escaneos internos y externos de la infraestructura, escaneos trimestrales PCI-DSS ASV y pruebas de penetración.
7.5. Existe un amplio programa anual de pruebas de penetración, realizado por expertos independientes acreditados por CREST.

8. REGISTRO, SUPERVISIÓN Y GESTIÓN DE INCIDENTES DE SEGURIDAD

8.1. Los registros de eventos que registran las actividades de los usuarios, las excepciones, los fallos y los eventos de seguridad de la información se generan, se conservan, se protegen de la manipulación y se revisan periódicamente.

8.2. Existe un servicio de Centro de Operaciones de Seguridad (SOC) 24 horas al día, 7 días a la semana, a través de un proveedor externo de confianza de servicios de seguridad gestionados, que incluye supervisión, recopilación y análisis de registros, gestión de eventos e información de seguridad (SIEM), respuesta y mitigación de incidentes de seguridad y capacidades de análisis forense para comprender la causa de los incidentes de seguridad y los métodos para reducir o eliminar posibles áreas de ataque.

8.3. Los incidentes de seguridad observados o presuntos se notifican de forma centralizada, se registran automáticamente y son objeto de seguimiento por parte del Equipo de Respuesta a Incidentes de Seguridad, en consonancia con el Plan de Respuesta a Incidentes de Seguridad de la Información y el Proceso de Gestión de la Vulneración de Datos, si procede.

9. SEGURIDAD EN LA NUBE

9.1. La plataforma de gestión de viajes y la infraestructura de servidores de están alojadas Microsoft Azure Reed & Mackay en el centro de datos de en el sur del Reino Unido.

9.2. MS Azure está configurado para cifrar la información en reposo independientemente del medio de almacenamiento, ya sea un disco gestionado conectado a una máquina virtual, una cuenta de almacenamiento que contenga datos de telemetría o código fuente de aplicaciones, o un servicio de base de datos de plataforma como Microsoft SQL.

9.3. Existe una política de seguridad en la nube aprobada por la dirección para definir los requisitos de seguridad en la nube.

9.4. Existe una solución de gestión de la postura de seguridad en la nube para supervisar y gestionar la gobernanza en todos Reed & Mackaylos activos y servicios basados en Microsoft Azure de , incluida la visualización y evaluación de la postura de seguridad, la detección de errores de configuración y la aplicación de las mejores prácticas de seguridad y los marcos de cumplimiento.

9.5. Los grupos de seguridad de red de Microsoft y los dispositivos de cortafuegos virtuales Checkpoint de nueva generación protegen nuestro entorno en el perímetro con la prevención de intrusiones activada.

10. SEGURIDAD FÍSICA

10.1. De acuerdo con nuestra Política de Seguridad Física y Medioambiental, se aplican medidas de seguridad física y medioambiental adecuadas para evitar el acceso físico no autorizado, los daños y las interferencias en los datos, locales e instalaciones de tratamiento. Existen los siguientes controles:

10.1.1. Oficina central:
Recepción del edificio atendida 24x7, la recepción de la oficina de Reed & Mackay funciona durante el horario de oficina. CCTV en todos los puntos de acceso al edificio, con cobertura de la mayoría de las zonas comunes y de las zonas de entrada y salida del edificio. A la sala de comunicaciones informáticas se accede mediante un sistema de tarjeta magnética y un teclado. La entrada está restringida a las personas autorizadas que tengan una necesidad profesional.

10.1.2. Oficinas regionales:
En las oficinas regionales se aplican los mismos controles que en la sede central, con algunas excepciones. Nuestras oficinas más pequeñas no disponen de una recepción con personal las 24 horas del día, los 7 días de la semana, ni de un sistema de tarjetas de acceso, pero nuestra política de seguridad física y medioambiental establece controles compensatorios para garantizar que la seguridad física de estas oficinas sea adecuada.

10.2. A los visitantes sólo se les permite el acceso para fines específicos y autorizados, y siempre están supervisados/acompañados mientras se encuentran en las oficinas de Reed & Mackay. Se mantienen registros de visitantes para todos los accesos físicos a las oficinas de Reed & Mackay, salas de servidores y centros de datos que albergan equipos informáticos y activos de información de Reed & Mackay.

11. SEGURIDAD DE LAS COMUNICACIONES Y LAS REDES

11.1. Las redes se gestionan mediante controles de seguridad adecuados, como la segmentación de la red, la gestión del acceso a la red, cortafuegos, normas de configuración y registro y supervisión.

11.2. Existen procedimientos y controles de transferencia de información para proteger la transferencia de datos utilizando todo tipo de medios de comunicación.

11.3. Nuestro protocolo de transferencia de datos recomendado para los intercambios regulares de datos (por ejemplo, archivos de datos, fuentes de recursos humanos) consiste en establecer una conexión SFTP entre organizaciones.

12. DESARROLLO DE SOFTWARE

12.1. El desarrollo interno de software sigue la metodología de ciclo de vida Agile/Sprint y las mejores prácticas de OWASP.

12.2. Existe una política SDLC (ciclo de vida del desarrollo de software) que incluye análisis y especificaciones de requisitos, seguridad por diseño, principios de ingeniería segura, entorno de desarrollo seguro, soporte de aplicaciones, control de calidad, pruebas, implementación, formación y revisión posterior a la implementación.

12.3. La integración del inicio de sesión único está disponible en nuestras aplicaciones orientadas al cliente. Se admiten soluciones basadas en SAML 2.0, como ADFS, azure AD y OKTA; también pueden admitirse otras opciones de terceros, pero pueden requerir desarrollo y pruebas.

12.4. Los sistemas de desarrollo, prueba y producción están separados. Los datos anónimos se utilizan con fines de prueba en entornos que no son de producción.

12.5. Los datos de los clientes se segregan utilizando identificadores únicos asignados en el momento de la creación de la cuenta. La segregación se garantiza mediante el uso de identificadores únicos, por ejemplo, corporativosidentificadores, de viajero identificadorese identificadores cuentade.

13. RELACIONES CON LOS PROVEEDORES

13.1. Los nuevos proveedores directos (incluidos los subprocesadores de datos) se someten a un proceso de diligencia debida que abarca la seguridad de la información, la protección de datos, la continuidad de las actividades, la gobernanza empresarial y la calidad, la salud y la seguridad, el medio ambiente, la igualdad de oportunidades, la diversidad, la lucha contra el soborno y la corrupción, la esclavitud moderna y el trabajo infantil, las prácticas empresariales éticas y la responsabilidad social de las empresas, así como una verificación de crédito, una revisión de las políticas, certificaciones, informes de auditoría independientes, pruebas de penetración independientes (incluido el seguimiento de las medidas correctoras), etc., según proceda.

13.2. Los proveedores están sujetos a cláusulas de confidencialidad y derecho de auditoría en sus contratos.
13.3. Los proveedores principios de funcionamiento de los proveedores de y los proveedores de productos/servicios que interactúan con los sistemas de información de R&M o procesan datos personales están obligados contractualmente a aceptar nuestros requisitos de seguridad de la información para proveedores.están obligados a cumplir Reed & Mackay los
13.4. Los proveedores son revisados periódicamente. La naturaleza, el alcance y la frecuencia de esta revisión dependen de varios factores, entre ellos el producto/servicio suministrado y del proveedorla criticidad .
13.5. Las capacidades de resistencia y recuperación de los proveedores críticos se revisan formalmente cada año como parte de nuestro Análisis de Impacto en el Negocio (BIA) de nuestras capacidades de recuperación de BC.

14. CONTINUIDAD DE LA ACTIVIDAD Y RECUPERACIÓN EN CASO DE CATÁSTROFE

14.1. En línea con nuestra certificación ISO 22301, los Planes de Continuidad de Negocio, incluido Reed & Mackayel Plan de Gestión de Crisis de , se revisan formalmente de forma anual, o con mayor frecuencia si es necesario (por ejemplo, si se produce un cambio significativo).
14.2. Existe un programa continuo de ejercicios y pruebas de continuidad de la actividad, que consiste en ejercicios de escenarios basados en la oficina y pruebas de recuperación física en el sitio.
14.3. Anualmente se realiza un Análisis de Impacto en el Negocio para definir la cantidad de interrupción que el negocio puede tolerar en sus actividades clave; el nivel mínimo de estas actividades necesario para su funcionamiento; y los recursos y dependencias necesarios para reanudar las actividades.
14.4. La plataforma de gestión de viajes de Reed & Mackay está alojada en Microsoft Azure, que ofrece altos grados de redundancia y resistencia.
14.5. Un servicio de copia de seguridad en línea de terceros para garantizar que la información crítica contenida en las máquinas virtuales y las cuentas de almacenamiento se almacena de forma segura e independiente del entorno Azure y está disponible para su restauración en caso de pérdida accidental o corrupción.
14.6. Nuestra base de datos patentada, que incluye todos los datos de contabilidad, clientes e informes, es objeto de una copia de seguridad completa diaria y de copias de seguridad incrementales a lo largo del día. El RPO es de 1 hora y el RTO de 3 horas. Los servidores son objeto de una copia de seguridad diaria "incremental para siempre". El RPO es de 1 día y el RTO de 4 horas. Nuestro RTO global es de 4 horas.
14.7. Las copias de seguridad se cifran y se comprueban periódicamente.

15. RIESGO PARA LA SEGURIDAD DE LA INFORMACIÓN

15.1. El pensamiento y la conciencia basados en el riesgo se incorporan Reed & al sistema de gestión de Mackay y a los procesos que lo sustentan.
15.2. El Programa de Gestión de Riesgos para la Seguridad de la Información forma parte del Marco Corporativo de Gestión de Riesgos y abarca la identificación y evaluación de los riesgos para la Seguridad de la Información derivados tanto de diversas actividades periódicas como de cambios planificados y no planificados. Los riesgos identificados se priorizan, tratan / aceptan y aprueban oportunamente.
15.3. Las actividades del programa de gestión de la seguridad de la información de Reed & Mackay se priorizan en función de los riesgos identificados y de su impacto en los servicios prestados a los clientes.