Última actualización: 10 de noviembre de 2024

Anexo de seguridad

Este Anexo de Seguridad forma parte de Sus Condiciones con Interwave. Todos los términos en mayúscula utilizados pero no definidos en este Anexo de seguridad tienen el significado establecido en las Condiciones. Los servicios informáticos utilizados para ofrecer el Servicio se basan en la nube y se proporcionan a Interwave a través de uno o más proveedores de servicios en la nube y representan nuestro "Entorno en la nube".

1. AUDITORÍAS Y CERTIFICACIONES DE INTERWAVE.

1.1. El sistema de gestión de la seguridad de la información utilizado para prestar el Servicio será evaluado por auditores externos independientes, tal y como se describe en las auditorías y certificaciones ("Auditorías externas") existentes, con una periodicidad mínima anual.

1.2. Los informes de Auditoría de Terceros se ponen a su disposición tal y como se describe en la Sección 10.1.

1.3. En la medida en que Interwave decida interrumpir una Auditoría de Terceros, Interwave adoptará un marco equivalente reconocido por la industria.

2. ALOJAMIENTO DE DATOS Y CONTENIDOS DE CLIENTES.

2.1. Los Datos y Contenidos del Cliente serán almacenados y procesados por Interwave y sus proveedores en centros de datos ubicados en la región geográfica especificada en Su formulario de pedido actualmente operativo o según se acuerde de otro modo por escrito.

2.2. Puede solicitar que los Datos y Contenidos del Cliente se almacenen en una región geográfica específica distinta. Interwave hará todos los esfuerzos comercialmente razonables para que así sea, siempre que lo permitan nuestros proveedores de servicios en la nube subyacentes y siempre que se cumplan las leyes y normativas aplicables.

3. ENCRYPTION.

3.1. Interwave encripta los Datos y Contenidos del Cliente en reposo utilizando encriptación AES de 256 bits (o superior). Interwave utiliza Transport Layer Security 1.2 (o superior) para los Datos y Contenidos del Cliente en tránsito por redes públicas o no fiables.

3.2. Rotamos las claves de cifrado al menos una vez al año y utilizamos módulos de seguridad de hardware para salvaguardar las claves de cifrado críticas. Interwave separa lógicamente las claves de cifrado de los Datos y Contenidos del Cliente.

4. SEGURIDAD DE SISTEMAS Y REDES.

4.1. El acceso del personal de Interwave a nuestro Entorno en la Nube se realiza con un ID de usuario único y es coherente con el principio de mínimo privilegio. El acceso requiere una conexión segura,

autenticación multifactor y contraseñas que cumplan o superen los requisitos razonables de longitud y complejidad.

4.2. El personal de Interwave no accederá a los Datos o Contenidos del Cliente salvo (i) para prestar o dar soporte al Servicio o (ii) para cumplir la ley o una orden vinculante de un organismo gubernamental.

4.3. Al acceder a nuestro Entorno en la Nube, nuestro personal utilizará ordenadores portátiles proporcionados por la empresa que utilizan controles de seguridad que incluyen el cifrado y que también incluyen herramientas de detección y respuesta de puntos finales para supervisar y alertar de actividades sospechosas, código malicioso y gestión de vulnerabilidades, tal como se describe en la sección 4.7.

4.4. Nuestro Entorno en la nube utiliza herramientas de detección de amenazas estándar del sector con actualizaciones diarias de firmas, que se utilizan para supervisar y alertar de actividades sospechosas, malware potencial, virus y/o código informático malicioso (colectivamente, "Código malicioso"). Interwave no tiene la obligación de supervisar los Datos o Entradas del Cliente en busca de Código Malicioso.

4.5. Interwave contrata a un tercero independiente para realizar pruebas de penetración del Servicio al menos una vez al año. Los resultados resumidos de dichas pruebas de penetración se pueden poner a su disposición como se describe en la Sección 10.1 a petición suya, y contienen, como mínimo: (i) nombre de la organización de pruebas de penetración, (ii) fecha(s) de la prueba de penetración, (iii) alcance de la prueba de penetración, (iv) modo de prueba / enfoque de la prueba, y (v) breve resumen de los hallazgos.

4.6. Interwave utiliza herramientas automatizadas para escanear bases de datos de vulnerabilidades de acceso público (por ejemplo, National Vulnerability Database (NVD) o similares) en busca de vulnerabilidades en el software que pueda ser utilizado por nosotros. Puntuamos las vulnerabilidades de acuerdo con un sistema de clasificación interno que tiene en cuenta la probabilidad de un exploit y el impacto potencial de un exploit, similar al CVSS. Nos ocupamos oportunamente de las vulnerabilidades. Las de categoría "crítica" se abordan en un plazo máximo de 7 días, las de categoría "alta" en 30 días y las de categoría "media" en 90 días.

4.7. Interwave contratará a un tercero para realizar evaluaciones de seguridad a nivel de aplicación web en el Servicio al menos una vez al año. Dichas evaluaciones incluirán pruebas de las vulnerabilidades de seguridad pertinentes identificadas en el Proyecto abierto de seguridad de aplicaciones web (OWASP), incluidas la falsificación de solicitudes en sitios cruzados, la secuencia de comandos en sitios cruzados (XSS), la inyección SQL (SQLi), las vulnerabilidades de autenticación y autorización, y otras.

5. CONTROLES ADMINISTRATIVOS.

5.1. Interwave mantiene programas de concienciación y formación en materia de seguridad para su personal, incluso en el momento de la incorporación y, posteriormente, al menos una vez al año. Dicha formación de concienciación sobre seguridad incluye los siguientes temas (i) responsabilidades individuales en términos de seguridad de la información y privacidad de los datos, (ii) comprensión de nuestras políticas y normas de seguridad de TI, (iii) orientación sobre cómo proteger la información de las amenazas cibernéticas existentes y emergentes, como los correos electrónicos de phishing, y (iv) requisitos para mantener la seguridad de sus dispositivos, credenciales y cuentas.

5.2. Interwave forma a todos los desarrolladores de software en prácticas de desarrollo seguro adecuadas a su función al menos una vez al año. El contenido de la formación se ajusta en función de la evolución del panorama de amenazas y puede incluir el modelado de amenazas, los principios de diseño seguro, la prevención de ataques para eludir la autenticación y la autorización, la prevención de ataques de secuencias de comandos en sitios cruzados, la prevención de ataques de falsificación de solicitudes en sitios cruzados y la prevención del uso de bibliotecas vulnerables.

5.3. El personal de Interwave está obligado a firmar acuerdos de confidencialidad y a reconocer la responsabilidad de informar sobre incidentes de seguridad que afecten a los Datos y Contenidos del Cliente.

5.4. Interwave retira el acceso a los sistemas críticos (incluidos los sistemas que contienen Datos y Contenidos del Cliente) a todo el personal separado en el plazo de 1 día y retira el acceso a todos los sistemas en el plazo de 3 días. Además, Interwave revisa los privilegios de acceso de su personal a su entorno en la nube al menos trimestralmente.

5.5. Interwave revisa la información externa sobre amenazas, incluidos los anuncios de vulnerabilidades de US-Cert y otras fuentes fiables de informes sobre vulnerabilidades. Las vulnerabilidades anunciadas por U.S.-Cert calificadas como críticas o altas se priorizan para su reparación de acuerdo con la Sección 4.6.

5.6. Interwave llevará a cabo las siguientes comprobaciones de antecedentes para todo el personal con acceso a los Datos y Contenidos del Cliente, en la medida en que lo permita la legislación aplicable: (i) comprobación de identidad, (ii) comprobación del derecho a trabajar y (iii) comprobación de antecedentes penales.

5.7. Interwave revisa todas las cuentas con privilegios elevados (cuentas de "administrador" o "root") en sistemas que contengan o tengan acceso a Datos y Contenidos del Cliente al menos trimestralmente y reduce el acceso administrativo si ya no es necesario (en otras palabras, se siguen los principios de mínimo privilegio).

6. PROVEEDORES Y SUBPROCESADORES.

6.1. Interwave garantiza que cualquiera de sus proveedores que procese Datos o Contenido del Cliente mantenga medidas de seguridad coherentes con nuestras obligaciones en virtud del presente Anexo de Seguridad.

6.2. Interwave mantiene una lista de subprocesadores en AthenaAIService.com.

7. CONTROLES FÍSICOS DEL CENTRO DE DATOS.

7.1. Nuestro entorno en la nube es mantenido por uno o más proveedores de servicios en la nube. Nos aseguramos de que los centros de datos de nuestros proveedores de servicios en la nube cuenten con los controles apropiados auditados en virtud de sus auditorías y certificaciones de terceros. Cada proveedor de servicios en la nube tendrá una auditoría anual SOC 2 Tipo II y la certificación ISO 27001, o marcos equivalentes reconocidos por la industria. Dichos controles incluyen:

- El acceso físico a las instalaciones se controla en los puntos de entrada a los edificios;
- Los visitantes deben presentar un documento de identidad y registrarse;

- El acceso físico a los servidores se gestiona mediante dispositivos de control de acceso;
- Los privilegios de acceso físico se revisan periódicamente;
- Las instalaciones utilizan procedimientos de monitorización y respuesta a las alarmas;
- Las instalaciones utilizan CCTV;
- Las instalaciones disponen de sistemas adecuados de detección y protección contra incendios;
- Las instalaciones cuentan con sistemas de reserva y redundancia adecuados; y
- Las instalaciones disponen de sistemas de climatización adecuados.

7.2. Interwave no mantiene oficinas físicas salvo para fines corporativos y ejecutivos limitados. En ningún caso los Datos o Contenidos del Cliente se almacenan o alojan en dichas oficinas.

8. DETECCIÓN Y RESPUESTA A INCIDENTES.

8.1. Si Interwave tiene conocimiento de una infracción de seguridad que provoque la destrucción, pérdida, alteración, divulgación no autorizada o acceso a los Datos o Contenidos del Cliente (una "Incidencia de seguridad"), Interwave se lo notificará sin demora indebida y, en cualquier caso, en un plazo de 48 horas tras tener conocimiento de la misma. Se le notificará a la dirección de correo electrónico de aviso de seguridad indicada en Su formulario de pedido actualmente operativo o según Interwave determine apropiado.

8.2. En caso de que se produzca un incidente de seguridad según lo descrito anteriormente, Interwave tomará rápidamente las medidas razonables para contener, investigar y mitigar cualquier incidente de seguridad. Todos los registros que se determinen relevantes para un incidente de seguridad se conservarán durante al menos un año.

8.3. Interwave le proporcionará información oportuna sobre el Incidente de Seguridad, incluyendo la naturaleza y las consecuencias del Incidente de Seguridad, el estado de nuestra investigación y un punto de contacto del que se puede obtener información adicional. Interwave también compartirá información sobre las medidas adoptadas o propuestas por Interwave para mitigar o contener el Incidente de Seguridad una vez concluida la investigación sobre el Incidente de Seguridad. El Cliente reconoce que, debido a que el personal de Interwave puede no tener visibilidad del contenido de los Datos y Contenidos del Cliente, puede darse el caso de que no podamos proporcionar un análisis detallado del tipo de Datos y Contenidos del Cliente afectados por la Incidencia de Seguridad. Las comunicaciones en relación con un Incidente de Seguridad no se interpretarán como un reconocimiento por parte de Interwave de ninguna culpa o responsabilidad con respecto al Incidente de Seguridad.

9. REGISTRO DE AUDITORÍA.

9.1. Interwave creará, protegerá y conservará registros de auditoría del sistema de información en la medida necesaria para mantener la integridad, y permitirá la supervisión, el análisis, la investigación y la notificación de actividades ilegales, no autorizadas o inapropiadas del sistema de información. Las acciones de los usuarios humanos del sistema de información se pueden rastrear de forma exclusiva hasta dichos usuarios.

9.2. Los registros de auditoría se conservan un mínimo de 1 año y un máximo de 10 años. Los registros de auditoría están protegidos contra la manipulación.

10. DERECHOS DE AUDITORÍA DEL CLIENTE.

10.1. Previa solicitud, y sin coste adicional para Usted, Interwave le proporcionará a Usted y/o a Su representante de terceros debidamente cualificado (colectivamente, el "Auditor") acceso a la documentación razonablemente solicitada que demuestre nuestro cumplimiento de nuestras obligaciones en virtud del presente Anexo de Seguridad en forma de, según corresponda, (i) el informe de auditoría de Interwave, más los resúmenes de pruebas de penetración y diagramas de flujo de datos pertinentes, y (ii) una copia de nuestras certificaciónes, así como una declaración de aplicabilidad (colectivamente con las Auditorías de Terceros, los "Informes de Auditoría"). Cuando un Auditor sea un tercero, dicho tercero deberá firmar un acuerdo de confidencialidad por separado con Interwave antes de cualquier auditoría, prueba de penetración o revisión de los Informes de Auditoría, e Interwave podrá objetar por escrito a dicho tercero si, en opinión razonable de Interwave, el tercero no está debidamente cualificado. Cualquier objeción de este tipo requerirá que Usted designe a otro tercero para revisar dichos Informes de Auditoría. Interwave no será responsable de los gastos incurridos por un Auditor en relación con la revisión de los Informes de Auditoría.

10.2. Una vez al año, Usted podrá presentar cuestionarios de seguridad razonables (que no superen las 100 preguntas en total) y solicitudes de documentación de seguridad actualizada, e Interwave se compromete a proporcionar los resultados en el plazo oportuno y por cuenta de Interwave.

10.3. En caso de que se produzca un incidente de seguridad que afecte a los datos o al contenido del cliente, Interwave se compromete a contratar a un especialista forense independiente o a una empresa similar a su propio coste y, en la medida en que los datos o el contenido del cliente se vean afectados, Interwave le proporcionará los resultados de dicho informe a su debido tiempo.

11. RESPONSABILIDADES DEL CLIENTE.

11.1. Es su responsabilidad asegurarse de que está autorizado a utilizar cualquier Entrada o Datos de Cliente con el Servicio y de que su uso cumple con las obligaciones legales y reglamentarias pertinentes.

11.2. Usted es responsable de gestionar y proteger sus métodos de acceso al Servicio (por ejemplo, contraseña, conexiones SSO, buzones de correo electrónico para autenticación por código de correo electrónico, etc.). Las credenciales de usuario deben mantenerse confidenciales y no pueden compartirse con partes no autorizadas. Una misma cuenta no podrá ser compartida por varias personas. Debe informar inmediatamente de cualquier actividad sospechosa relacionada con su(s) cuenta(s) (por ejemplo, cuando crea razonablemente que las credenciales han sido comprometidas).

11.3. Usted es responsable de mantener actualizados y debidamente parcheados sus sistemas informáticos pertinentes (como el navegador que utiliza para acceder al Servicio).

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

12.1. Interwave mantiene planes de continuidad del negocio que detallan cómo se mantendrán las operaciones durante una interrupción imprevista del servicio. Esto incluye contingencias para procesos empresariales, activos, recursos humanos y socios comerciales, y cubre información, sistemas y servicios clave. Los planes de continuidad son aprobados por la alta dirección y revisados y probados anualmente.

V 1.00