ANEXO DE SEGURIDAD

1. OBJETO DEL ACUERDO: Este Anexo de Seguridad establece las medidas para proteger la información compartida entre BELLTECH y sus proveedores. Se aplica a todos los proveedores de BELLTECH y al personal involucrado en relaciones con proveedores.

2. PROPIEDAD DE LA INFORMACIÓN:

1. BELLTECH retiene la propiedad exclusiva de toda la información compartida con EL PROVEEDOR, incluyendo diseños, marcas y derechos de propiedad intelectual. Esto abarca estudios, informes y datos generados durante la ejecución del contrato.

2. El PROVEEDOR no puede reproducir ni comercializar la información, salvo estipulación en contrario.

3. El PROVEEDOR puede procesar cierta información para el servicio, pero debe garantizar su seguridad.

4. El PROVEEDOR debe conservar registros de las operaciones relacionadas con la información proporcionada por BELLTECH durante al menos cinco años.

3. RESTRICCIONES DEL SOFTWARE EMPLEADO:

1. En el evento en el cual EL PROVEEDOR tenga acceso al software de BELLTECH o de sus contratistas, El PROVEEDOR no reproducirá, distribuirá ni comercializará el software de BELLTECH ni permitirá acceso no autorizado al mismo. Se compromete a usar el software solo según las indicaciones de BELLTECH y a no modificarlo ni realizar ingeniería inversa. En caso de violación de derechos de propiedad intelectual, el PROVEEDOR indemnizará a BELLTECH por cualquier daño.

2. El PROVEEDOR usará software seguro para proteger la información de BELLTECH y permitirá pruebas de seguridad por parte de BELLTECH. Si el software no cumple con los requisitos de seguridad, BELLTECH se reserva el derecho de rechazar su uso.

3. Si el PROVEEDOR utiliza software gratuito o servicios en la nube, debe garantizar el soporte adecuado y la integración con los sistemas de autenticación de BELLTECH.

4. PROCEDIMIENTOS ANTE ALTERACIÓN O MANIPULACIÓN DE DISPOSITIVOS O INFORMACIÓN

1. En caso de que durante la ejecución del presente contrato, se evidencie: alteración o manipulación de equipos o información que es de propiedad de BELLTECH, utilizados en desarrollo del contrato u orden de compra, EL PROVEEDOR deberá informar dicha situación al encargado de EL CONTRATANTE, mencionado en el presente contrato, así al correo electrónico sig@belltech.la, aportando las pruebas que demuestren dicha eventualidad y las acciones tomadas para mitigar cualquier daño o perjuicio de BELLTECH.

2. Cuando se detecte manipulación o alteración de Software, Hardware o información de BELLTECH, EL PROVEEDOR cesará inmediatamente su uso y restringirá el acceso a contratistas y funcionarios.

3. EL PROVEEDOR deberá contar con los medios y procedimientos para recolectar, almacenar y suministrar la información requerida por BELLTECH, manteniendo la cadena de custodia según normativas legales.

4. EL PROVEEDOR será responsable ante BELLTECH, terceros y autoridades por el manejo adecuado de la información.

5. BELLTECH podrá recolectar la información si lo considera necesario.

6. EL PROVEEDOR deberá proporcionar registros de aplicación y datos según los requisitos de computación forense o análisis de seguridad.

5. PROCEDIMIENTOS DE ENTREGA Y DESTRUCCIÓN DE INFORMACIÓN POR EL PROVEEDOR.

1. Entrega de Información Física:

a. La entrega de documentos físicos de BELLTECH se realizará con evidencia de entrega, trazabilidad en sistemas de envío y recibo, o mediante medios tecnológicos.

b. Dependiendo del servicio, se pueden requerir procedimientos adicionales de entrega, informados por BELLTECH.

2. Entrega de Información Electrónica:

a. EL PROVEEDOR garantizará la seguridad de la información electrónica transmitida, evitando acceso o modificación no autorizada.

b. Se deben implementar sistemas de control y seguridad para certificar la integridad y restricción de acceso a la información.

3. Destrucción o Devolución de Información:

a. Al finalizar los servicios, EL PROVEEDOR debe devolver o destruir la información según lo indique BELLTECH.

b. La devolución o destrucción se realizará en un plazo de 30 días hábiles, previa autorización de BELLTECH.

c. Si no se otorga autorización, EL PROVEEDOR debe solicitar instrucciones dentro de los 60 días hábiles siguientes.

d. EL PROVEEDOR garantizará la confidencialidad durante el proceso de destrucción y suscribirá contratos de confidencialidad con los encargados de destruir la información.

La información en la nube se borrará de manera segura antes de entregar los recursos, definiendo los requisitos de almacenamiento y retención con BELLTECH.

6. CONTINUIDAD DE LOS SERVICIOS SUMINISTRADOS

1. EL PROVEEDOR debe tener un plan de continuidad para manejar incidentes internos y externos que puedan interrumpir los servicios.

2. El plan debe documentarse y revisarse cada 6 meses para garantizar su eficacia ante diversos escenarios.

3. Los colaboradores relevantes del proveedor serán informados sobre estos procedimientos.

ANEXO DE SEGURIDAD

4. BELLTECH tiene derecho a verificar la efectividad del plan, solicitando documentación y realizando visitas planificadas con anticipación.

5. El Plan de Continuidad del Negocio incluye políticas, estrategias, procedimientos y tareas para mantener la continuidad de los servicios.

7. NORMAS DE SEGURIDAD DE LA INFORMACIÓN: PROVEEDOR El PROVEEDOR deberá cumplir con las políticas de seguridad de BELLTECH establecidas en el "ANEXO POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN". Además, el PROVEEDOR proporcionará servicios siguiendo las mejores prácticas del sector y cumpliendo con las normas establecidas para garantizar la seguridad de la información. BELLTECH tendrá derecho a solicitar informes sobre los estándares aplicados por el PROVEEDOR.

8. SEGURIDAD DE LA INFORMACIÓN: Para asegurar la seguridad de la información EL PROVEEDOR debe:

1. Implementar un programa de seguridad de la información y ciberseguridad certificado por un auditor externo, Conforme a estándares internacionales como ISO 27001 u otros aplicables, incluyendo: **I.** Capacitación anual sobre seguridad. **II**. Protección anticipada contra amenazas. **III.** Gestión y respuesta a incidentes. **IV.** Pruebas de vulnerabilidad. **V.** Procesos para la prevención de fuga de información. **VI.** Mecanismos de control de acceso a la información.

2. Notificar a BELLTECH sobre modificaciones en los procedimientos de seguridad

9. SEGURIDAD EN LA NUBE (Solo aplica para contratación de servicios en Nube)

1. El PROVEEDOR debe cumplir con el estándar definido por BELLTECH para los servicios en la nube, garantizando la disponibilidad y modificación de la información, así como la gestión de incidentes de seguridad. La información debe alojarse en países con leyes de protección de datos.

2. Ambas partes deben tener responsables definidos para los incidentes de seguridad de la información. BELLTECH puede solicitar información en cualquier momento, y el PROVEEDOR debe atender estas solicitudes dentro de los plazos acordados.

3. El PROVEEDOR debe seguir el marco de referencia para la seguridad en la nube, incluyendo estándares como ISO/IEC 27017, ISO 27018, SSAE 16 SOC1, SOC2, SOC3, CSA STAR y PCI DSS si corresponde. Si no cuenta con estas certificaciones al momento de firmar el contrato, tiene un plazo máximo de doce meses para establecerlas, iniciando las gestiones en un plazo de sesenta días. Se debe validar cualquier excepción con las áreas de Seguridad de la Información.

10. GESTIÓN DE CAMBIOS EN SEGURIDAD DE LA INFORMACIÓN: EL PROVEEDOR deberá a informar a BELLTECH los cambios que puedan afectar la seguridad de la información frente a la prestación del servicio.

11. SEGURIDAD DE LOS ARCHIVOS DE INFORMACIÓN Y BASES DE DATOS: Para garantizar la seguridad de los archivos y bases de datos de BELLTECH, EL PROVEEDOR deberá:

1. Almacenar la información confidencial de BELLTECH en formato cifrado.

2. Colocar los servidores y repositorios de datos en áreas físicamente seguras.

3. Restringir el acceso físico y lógico según necesidad de negocio.

4. Proteger los accesos con una combinación de identificación de usuario y contraseña.

5. Registrar toda la actividad de acceso y transacciones.

6. Manejar copias de respaldo con estrictos controles de seguridad.

7. Utilizar herramientas de análisis de seguridad para revisar las configuraciones de las bases de datos.

8. Revisar periódicamente todos los controles de seguridad para asegurar su vigencia.

12. RESPALDO Y RECUPERACIÓN: Para cumplir con los requisitos de BELLTECH y las mejores prácticas de la industria para el respaldo y la recuperación, EL PROVEEDOR deberá:

1. Implementar medidas adecuadas de respaldo, incluido el almacenamiento seguro de los archivos fuera del sitio.

2. Facilitar la reanudación de aplicaciones críticas y actividades comerciales después de emergencias.

3. Mantener un plan de recuperación de desastres documentado y probarlo.