Celonis Information Security Annex

This Celonis Information Security Annex (the "Annex") sets forth the IT security and controls applicable to Celonis' provision of EMS (defined below) to You and is incorporated into and made part of the Agreement.

1. **Definitions.** All capitalized terms in this Annex have the meanings specified in the Agreement, except as otherwise provided below:

1.1 "EMS" means the Celonis Execution Management System, as made available to You under the Agreement.

1.2 "High Availability" means the elimination of single points of failure to enable applications to continue to operate even if one of the underlying IT components fails.

1.3 "Information Security Incident" means any (i) unauthorized access to, alteration of or damage to the EMS, or (ii) loss or unauthorized alteration of or damage to Customer Data or (iii) theft or unauthorized use, disclosure or acquisition of or access to any Customer Data.

1.4 "Malware" means any program or device (including any software, code or file) which is intended to prevent, impair or otherwise adversely affect the access to or operation, reliability or user experience of any computer software, hardware or network, telecommunications service, equipment or network or any other service or device, including without limitation worms, trojan horses, viruses, ransomware, trap doors and other similar malicious devices.

1.5 "Principle of Least Privilege" means allowing access for users (or processes acting on behalf of users) only as necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

2. **Our Obligations.**

2.1 We will comply with, and will cause Our employees to comply with, this Annex. As between You and Celonis, We are responsible for any failure of Our subcontractors to comply with any IT controls set forth in this Annex.

2.2. We will maintain Our comprehensive information security program in compliance with industry-recognized standards and applicable law. Our information security program includes appropriate administrative, technical, physical, organizational and operational safeguards and other security measures designed to (i) ensure the security and confidentiality of Customer Data, and (ii) protect against the threat of Information Security Incidents. Our information security program also

Celonis Anexo de seguridad de la información

El presente Celonis Anexo de seguridad de la información (el "Anexo") establece la seguridad informática y controles aplicables a la prestación de Celonis EMS (definido a continuación), por parte de Celonis a Usted; y se integra y forma parte del Contrato.

1. **Definitions.** Todos los términos que aparecen en mayúsculas en el presente Anexo tienen el significado que se especifica en el Contrato salvo que se disponga lo contrario a continuación:

1.1 "EMS" significa "Sistema de Gestión de Ejecución de Celonis" (Celonis Execution Management System), tal y como se pone a su disposición en virtud del Contrato.

1.2 "Alta Disponibilidad" significa la eliminación de puntos únicos de fallo para permitir que las aplicaciones sigan funcionando incluso si falla uno de los componentes informáticos subyacentes.

1.3 "Incidente de seguridad de la información" se refiere a cualquier (i) acceso no autorizado, alteración o daño al EMS, o (ii) pérdida o alteración no autorizada o daño a los Datos del Cliente o (iii) robo o uso no autorizado, divulgación o adquisición o acceso a cualquier Dato del Cliente.

1.4 "Malware" hace referencia a cualquier programa o dispositivo (incluido cualquier software, código o archivo) cuyo objetivo sea impedir, perjudicar o afectar negativamente de cualquier otro modo al acceso o funcionamiento, fiabilidad o experiencia de usuario de cualquier software, hardware o red informática, servicio, equipo o red de telecomunicaciones o cualquier otro servicio o dispositivo, incluidos, entre otros, gusanos, troyanos, virus, ransomware, puertas trampa y otros dispositivos maliciosos similares.

1.5 "Principio del menor privilegio" significa permitir el acceso a los usuarios (o a los procesos que actúan en nombre de los usuarios) sólo en la medida necesaria para llevar a cabo las tareas asignadas de acuerdo con las misiones y funciones empresariales de la organización.

2. Nuestras obligaciones.

2.1 Nosotros cumpliremos, y haremos que Nuestros empleados cumplan, el presente Anexo. En lo que respecta a Usted y Celonis, somos responsables de cualquier incumplimiento por parte de Nuestros subcontratistas de los controles informáticos establecidos en el presente Anexo.

2.2 Mantendremos Nuestro programa integral de seguridad de la información de conformidad con las normas reconocidas del sector y la legislación aplicable. Nuestro programa de seguridad de la información incluye salvaguardas administrativas, técnicas, físicas, organizativas y operativas adecuadas, así como otras medidas de seguridad diseñadas para (i) garantizar la seguridad y confidencialidad de los Datos del Cliente, y (ii) proteger contra la amenaza de Incidentes de Seguridad de la

includes a cybersecurity awareness program that informs and reminds staff of preventative measures to avoid inadvertent exposure of Customer Data or inadvertent exposure of EMS to unauthorized activity.

2.3 We will regularly test, review and update Our information security program, and will incorporate into EMS the improvements resulting from such updates.

3. Standards / Certifications.

3.1 We will maintain, and will provide to You upon request and subject to confidentiality requirements, any then-available attestations of compliance with certifications and other standards including:

i. SOC 1, Type 2;
ii. SOC2, Type 2;
iii. ISO 27001:2013;
iv. ISO 27701:2019;
v. TISAX; and
vi. ISO 9001:2015

3.2 You may view Our current list of certifications and compliance status at http://trust.celonis.com/.

3. Encryption.

4.1 We will provide encryption for Your connection to EMS with a minimum encryption level equivalent to AES-128 (or then-current industry equivalent).

4.2 We will encrypt all Customer Data residing on backups with a minimum encryption level equivalent to AES-256.

4.3 We will ensure that remote access to EMS is only via a secured connection with a minimum encryption level equivalent to AES-128.

4.4 We will encrypt Customer Data at rest with a minimum AES-256 bit encryption. Data will be encrypted, whether the storage device is powered on or off.

4.5 We will store system secrets, including but not limited to encryption keys, certificates, passwords, hashes, connection strings, and other secrets in an appropriate secure service. We will not store system secrets in configuration files or in source code. We will ensure that access to system secrets follows the Principle of Least Privilege.

4.6 We will encrypt all passwords with a minimum encryption level equivalent to AES-256

4.7 If You have purchased a private cloud instance, We will support use of encryption keys supplied by You (bring or hold Your own encryption key) and will provide a means of allowing You to rotate the key as documented in Our then-current product documentation.

4. Controls.

4.1. EMS.

i. EMS is hosted on platforms provided by infrastructure as a service cloud providers. We will have in place, maintain, and use appropriate information security measures, including physical,

Información. Nuestro programa de seguridad de la información también incluye un programa de concienciación sobre ciberseguridad que informa y recuerda al personal las medidas preventivas para evitar la exposición inadvertida de los Datos del Cliente o la exposición inadvertida del EMS a actividades no autorizadas.

2.3 Comprobaremos, revisaremos y actualizaremos periódicamente Nuestro programa de seguridad de la información, e incorporaremos al EMS las mejoras resultantes de dichas actualizaciones.

Chapter 3 Normas / Certificaciones.

3.1 Mantendremos, y le proporcionaremos a Usted, cuando lo solicite y sujeto a obligaciones de confidencialidad, cualquier certificado de cumplimiento de certificaciones y otras normas disponibles en ese momento, incluyendo:

i. SOC 1, Tipo 2;
ii. SOC2, Tipo 2;
iii. ISO 27001:2013;
iv. ISO 27701:2019;
v. TISAX; y
vi. ISO 9001:2015

3.2 Puede consultar Nuestra lista actual de certificaciones y estado de cumplimiento en http://trust.celonis.com/.

4. Cifrado (Encriptación)

4.1 Proporcionaremos cifrados para Su conexión a EMS con un nivel de cifrado mínimo equivalente a AES-128 (o equivalente en la industria en ese momento).

4.2 Cifraremos todos los Datos del Cliente que residan en copias de seguridad con un nivel de cifrado mínimo equivalente a AES-256.

4.3 Nos aseguraremos de que el acceso remoto a EMS se realice únicamente a través de una conexión segura con un nivel de cifrado mínimo equivalente a AES-128.

4.4 Cifraremos los Datos del Cliente en reposo con un nivel mínimo de cifrado AES-256 bits. Los datos se cifrarán tanto si el dispositivo de almacenamiento está encendido como apagado.

4.5 Almacenaremos los secretos del sistema, incluidos, entre otros, claves de cifrado, certificados, contraseñas, hashes, cadenas de conexión y otros secretos en un servicio seguro adecuado. No almacenaremos secretos del sistema en archivos de configuración ni en código fuente. Nos aseguraremos de que el acceso a los secretos del sistema siga el Principio del Mínimo Privilegio.

4.6 Cifraremos todas las contraseñas con un nivel de cifrado mínimo equivalente a AES-256.

4.7 Si ha adquirido una instancia de nube privada, apoyaremos el uso de claves de cifrado suministradas por Usted (traiga o conserve su propia clave de cifrado) y proporcionaremos un medio que le permita rotar la clave, tal y como se documenta en nuestra documentación del producto vigente en ese momento.

5. Controles.

5.1. EMS.

i. EMS está alojado en plataformas proporcionadas por proveedores de infraestructura como servicio en la nube. Estableceremos, mantendremos y utilizaremos

technical, and administrative controls, to prevent unauthorized access to EMS.

ii. We will maintain appropriate separation between EMS and Our internal business network.
iii. Our support staff (including subcontractors) will use secure access methods to access EMS for support services.

iv. We monitor EMS for indicators of unauthorized activity or compromise and have a dedicated security operations organization. We will retain logs of detection and blocking events for a minimum of one (1) year unless applicable law requires retention for a different period.

v. We will follow a secure development process to systematically reduce the frequency and severity of vulnerabilities in code.
vi. We will utilize industry standard safeguards against Malware and malicious activity in EMS.
vii. We will not knowingly introduce Malware into EMS.

viii. We will implement and maintain up-to-date security controls to protect EMS against industry known threats, such as the "OWASP Top 10" threats, via secure coding practices and appropriate technical controls.

ix. We will harden EMS by removing unnecessary software and utilities, turning off unneeded EMS instances, and closing extraneous network communication ports.

5.2 Operating System/Applications
i. We will implement and maintain up-to-date change management procedures for EMS which include Our testing, certification, and approval processes specifically related to standard bug fixes, updates, security patches, and upgrades made available to You.

5.3 Backups.

i. We will perform and continuously maintain secure replication of a primary production site's Customer Data in near real-time to geo-diverse active sites within the same country as the primary production site. Encryption of and access to Customer Data for the replicated sites must comply with this Annex.
ii. We have and will maintain a business continuity and/or disaster recovery plan in relation to the provision of EMS. The disaster recovery plan is tested at least annually.
iii. EMS leverages backups of its application and analytics data. The automated backup system is configured to perform daily incremental data backups of production databases, which are retained for 30 days.

5.4 Authentication/Authorization/Access.

medidas de seguridad de la información adecuadas, incluidos controles físicos, técnicos y administrativos, para impedir el acceso no autorizado a EMS.
ii. Mantendremos una separación adecuada entre el EMS y Nuestra red empresarial interna.
iii. Nuestro personal de soporte (incluidos los subcontratistas) utilizarán métodos de acceso seguros para acceder al EMS para los servicios de soporte.
iv. Monitoreamos el EMS en busca de indicadores de actividad no autorizada o de riesgo y contamos con una organización de operaciones de seguridad especializada. Conservaremos los registros de eventos de detección y bloqueo durante un mínimo de un (1) año, a menos que la legislación aplicable exija su conservación durante un periodo diferente.
v. Seguiremos un proceso de desarrollo seguro para reducir sistemáticamente la frecuencia y gravedad de las vulnerabilidades del código.
vi. Utilizaremos salvaguardas estándar del sector contra el malware y la actividad maliciosa en el EMS.
vii. No introduciremos malware en el EMS de manera intencionada.
viii. Implementaremos y mantendremos controles de seguridad actualizados para proteger el EMS contra las amenazas conocidas de la industria, como las amenazas "OWASP Top 10", a través de prácticas de codificación seguras y controles técnicos apropiados.
ix. Fortaleceremos el EMS eliminando el software y las herramientas innecesarias, desactivando las instancias del EMS que no sean imprescindibles y cerrando los puertos de comunicación de red superfluos.

5.2 Sistema operativo/aplicaciones.
i. Implantaremos y mantendremos procedimientos actualizados de gestión de cambios para el EMS que incluyan Nuestros procesos de prueba, certificación y aprobación específicamente relacionados con correcciones de errores, actualizaciones, parches de seguridad y mejoras estándar que se pongan a Su disposición.

5.3 Copias de seguridad.
i. Realizaremos y mantendremos continuamente una replicación segura de los Datos del Cliente de un centro de producción primario en tiempo casi real a centros activos geodiversos dentro del mismo país que el centro de producción primario. El cifrado y acceso a Datos del Cliente para los sitios replicados deben cumplir con este Anexo.
ii. Disponemos y mantendremos un plan de continuidad de negocio y/o de recuperación en caso de desastre en relación con el suministro del EMS. El plan de recuperación en caso de catástrofe se comprobará al menos una vez al año.
iii. EMS realiza copias de seguridad de sus aplicaciones y datos analíticos. El sistema automatizado de copias de seguridad está configurado para realizar copias de seguridad incrementales diarias de las bases de datos de producción, que se conservan durante 30 días.

5.4 Autenticación/Autorización/Acceso.

i. We will require multifactor authentication for all staff when gaining access to EMS, except where it is not technically possible.
ii. Supported authentication methods for Your Users are documented in Celonis product documentation.
iii. We will provide You with the option of multifactor authentication as documented in our product documentation.
iv. We will limit the number of Our support staff (including subcontractors) with persistent access to Customer Data according to the Principle of Least Privilege.
v. We will maintain an activity log of system access tracing such access back to specific employees of Ours who: (i) access the EMS infrastructure, (ii) perform system and application administration support, or (iii) use administrator or other privileged access on a central log server. We will implement and maintain a backup regime on the central log server. The retention period for such logs will be twelve (12) months. The activity log will include date and time, ID of who performed the action, resource accessed, event identifier, and event information. Log files will be immutable and inaccessible to administrators of the servers and resources being logged. We will regularly review logs related to the use of privileged access or anomalous security events (such as abnormal access attempts, critical data changes) to identify any irregularities.

5.5 Data Center Security.

i. EMS information-processing systems and supporting infrastructure will be located in data center facilities that meet Our requirements for physical security and provide an appropriate level of protection against unauthorized physical access, damage, and interference, which may include:

a. Physical access controls at building ingress points;
b. Identity controls of all visitors prior to sign-in;
c. Access control devices managing physical access to servers;
d. Regular review of physical access privileges;
e. Comprehensive monitor and alarm response procedures;
f. CCTV surveillance;
g. Appropriate fire detection and prevention systems;
h. Appropriate power redundancy and backup systems; and
i. Appropriate climate control systems.

5.6 Administrative Controls.

i. Exigiremos la autenticación multifactor a todo el personal cuando obtenga acceso a EMS, excepto cuando no sea técnicamente posible.
ii. Los métodos de autenticación admitidos para sus usuarios están documentados en la Documentación de Producto Celonis.
iii. Le proporcionaremos la opción de autenticación multifactor tal y como se documenta en la Documentación de Producto de Celonis.
iv. Limitaremos el número de Nuestro personal de soporte (incluidos los subcontratistas) con acceso persistente a los Datos de Cliente de acuerdo con el Principio de Mínimo Privilegio.
v. Mantendremos un registro de actividad del acceso al sistema que rastree dicho acceso hasta empleados específicos Nuestros que: (i) accedan a la infraestructura del EMS, (ii) realicen soporte de administración de sistemas y aplicaciones, o (iii) utilicen el acceso de administrador u otro acceso privilegiado en un servidor de registro central. Implementaremos y mantendremos un régimen de copias de seguridad en el servidor central de registros. El periodo de conservación de dichos registros será de doce (12) meses. El registro de actividad incluirá la fecha y hora, el identificador de quien realizó la acción, el recurso al que se accedió, el identificador del evento y la información del evento. Los archivos de registro serán inmutables e inaccesibles para los administradores de los servidores y recursos registrados. Revisaremos periódicamente los registros relacionados con el uso de accesos privilegiados o eventos de seguridad anómalos (como intentos de acceso anómalos, cambios de datos críticos) para identificar cualquier irregularidad.

5.5 Seguridad del Centro de Datos.

i. Los sistemas de procesamiento de información del EMS y la infraestructura de apoyo se ubicarán en instalaciones de centros de datos que cumplan Nuestros requisitos de seguridad física y proporcionen un nivel adecuado de protección contra el acceso físico no autorizado, daños e interferencias, que pueden incluir:
a. Controles de acceso físico en los puntos de entrada al edificio;
b. Controles de identidad de todos los visitantes antes de iniciar sesión;
c. Dispositivos de control de acceso que gestionen el acceso físico a los servidores;
d. Revisión periódica de los privilegios de acceso físico;
e. Procedimientos exhaustivos de monitorización y respuesta a alarmas;
f. Vigilancia por circuito cerrado de televisión;
g. Sistemas adecuados de detección y prevención de incendios;
h. Sistemas adecuados de redundancia y reserva de energía; y
i. Sistemas de climatización adecuados.

5.6 Controles administrativos.

i. We will, to the extent legally permitted and in accordance with Our internal policies and processes, perform industry standard background checks on Our employees and subcontractors with access to Customer Data.
ii. Our employees are required to gain and maintain certification within Our security awareness and training program.

6. Data Deletion.

6.1 On expiry of Your Subscription Term or termination of the Agreement for any reason, and at Your request, We will either (i) securely destroy or render unreadable, undecipherable, or unrecoverable or (ii) deliver to You or Your designees all Customer Data or Confidential Information in Our possession, custody, or control.

7. Security Assessment and Testing

7.1 We will conduct, or commission third parties to conduct, at Our expense, vulnerability assessments and penetration testing of EMS at least annually. Such assessments and testing will be limited to validating Our compliance with the security requirements herein and identifying security vulnerabilities, if any, of EMS. On request, We will share a confidential summary of any relevant findings from such assessments and testing.

7.2 You may, at Your own expense, conduct security assessments of Your EMS applications, but only in accordance with Our "Guidelines for Security Assessment by Customers". The following activities are expressly prohibited:

i. Denial of service (DoS). You are expressly prohibited from utilizing any tools or services in a manner that performs DoS attacks or simulations of such against any EMS asset;
ii. Resource request flooding (e.g. HTTP request flooding, Login request flooding, API request flooding);
iii. Protocol flooding (e.g. SYN flooding, ICMP flooding, UDP flooding);
iv. Scanning or testing assets belonging to any other customer;
v. Gaining access to any data that is not wholly-owned by You;
vi. Performing automated testing of services that generate significant amounts of traffic; and
vii. Attempting phishing or other social engineering attacks against Our employees.

7.3 We will mitigate and remediate any confirmed zero-day vulnerabilities detected or identified in EMS through patching, decommissioning or compensating controls.

8. Information Security Incident Detection and Response

i. En la medida en que la ley lo permita y de conformidad con Nuestras políticas y procesos internos, realizaremos comprobaciones de antecedentes estándar del sector a Nuestros empleados y subcontratistas con acceso a los Datos del cliente.
ii. Se exige a nuestros empleados que obtengan y mantengan una certificación dentro de nuestro programa de concienciación y formación en materia de seguridad.

6. Eliminación de datos.

6.1 A la expiración del Periodo de Suscripción o a la terminación del Contrato por cualquier motivo, y a petición suya, (i) destruiremos de forma segura o haremos ilegibles, indescifrables o irrecuperables o (ii) le entregaremos a usted o a las personas que usted designe todos los Datos del Cliente o la Información Confidencial que estén en nuestra posesión, custodia o control.

7. Evaluación y pruebas de seguridad

7.1 Realizaremos, o encargaremos a terceros que realicen, a nuestra costa, evaluaciones de vulnerabilidad y pruebas de penetración del EMS al menos una vez al año. Dichas evaluaciones y pruebas se limitarán a validar nuestro cumplimiento de los requisitos de seguridad del presente documento y a identificar las vulnerabilidades de seguridad, si las hubiera, del EMS. Previa solicitud, compartiremos un resumen confidencial de cualquier resultado relevante de dichas evaluaciones y pruebas.

7.2 Usted puede, a sus expensas, llevar a cabo evaluaciones de seguridad de sus aplicaciones del EMS, pero sólo de acuerdo con nuestras "Directrices para la evaluación de seguridad por parte de los Clientes". Las siguientes actividades están expresamente prohibidas

i. Denegación de servicio (DoS). Queda expresamente prohibido el uso de herramientas o servicios que realicen ataques de denegación de servicio o simulaciones de los mismos contra cualquier activo del EMS;
ii. Saturación de solicitudes de recursos (por ejemplo, saturación de solicitudes HTTP, saturación de solicitudes de inicio de sesión, saturación de solicitudes API);
iii. Saturación de protocolo (por ejemplo, saturación SYN, saturación ICMP, saturación UDP);
iv. Escaneo o comprobación de activos pertenecientes a cualquier otro cliente;
v. Obtener acceso a cualquier dato que no le pertenezca en su totalidad;
vi. Realizar pruebas automatizadas de servicios que generen cantidades significativas de tráfico; y
vii. Intentar suplantación de identidad u otros ataques de ingeniería social contra nuestros empleados.

7.3 Mitigaremos y remediaremos cualquier vulnerabilidad confirmada de día cero detectada o identificada en EMS mediante parches, desmantelamiento o controles compensatorios.

8. Detección y respuesta a incidentes de seguridad de la información

8.1. Notice of Incident. In the event We become aware of any confirmed Information Security Incident affecting Your data, We will notify You without undue delay. Such notice will summarize in reasonable detail a description of the nature of the breach, the likely consequences and the measures taken to address the breach. We will also advise details of a contact point where further information can be obtained.

8.2 Notice of Disclosure. We will provide You with copies of any public disclosure, filings, communications, general notices, press releases, or reports related to any Information Security Incident ("Communications"). Where the content of any such Communications identifies or may reasonably identify You, We will seek Your approval prior to the disclosure of such information, where permitted by law.

8.3 We will provide reasonable assistance with regards to any legal reporting requirements in response to any actual or suspected unauthorized access to EMS.

8.1 Notificación de incidentes. En caso de que tengamos conocimiento de cualquier Incidente de Seguridad de la Información confirmado que afecte a sus datos, se lo notificaremos sin demora indebida. Dicha notificación resumirá de forma razonablemente detallada una descripción de la naturaleza de la infracción, las consecuencias probables y las medidas adoptadas para hacer frente a la infracción. También le indicaremos un punto de contacto en el que puede obtener más información.

8.2 Notificación de divulgación. Le proporcionaremos copias de cualquier divulgación pública, presentación, comunicación, aviso general, comunicado de prensa o informe relacionado con cualquier Incidente de Seguridad de la Información ("Comunicaciones"). Cuando el contenido de cualquiera de dichas Comunicaciones le identifique o pueda identificarle razonablemente, solicitaremos su aprobación antes de divulgar dicha información, siempre que la ley lo permita.

8.3 Proporcionaremos asistencia razonable con respecto a cualquier requisito legal de notificación en respuesta a cualquier acceso no autorizado real o sospechado a EMS.

9. Customer Responsibilities

9.1 You must take all reasonable steps to ensure appropriate administrative, technical, physical, organizational and operational safeguards are implemented and enforced for all areas under Your control, including but not limited to:

i. Ensuring that Customer Data for which HIPAA, FedRAMP or similar elevated security requirements apply is uploaded only to EMS instances specifically designated as appropriate for such data;
ii. Ensuring that payment card information is not uploaded or otherwise published to any EMS environment;
iii. Implementing all appropriate customer-configurable security controls to protect Your Customer Data;
iv. Implementing source system and Customer Data backups and appropriate data hygiene controls;
v. Ensuring any anonymization or pseudonymization tools (including those made available by Celonis) are configured properly;
vi. Safeguarding against Malware and other malicious activity, including without limitation scanning Your systems and Customer Data with current versions of industry-standard antivirus software and leveraging adequate firewall technologies;
vii. Monitor and update the status page to indicate incidents affecting availability (status.celonis.com). We will provide updates during the duration of the incident;
viii. Managing and protecting Your User roles and credentials; and
ix. Managing and protecting any encryption keys held by You to ensure the integrity, availability and confidentiality of the key and the Customer Data secured with such key.

9.2 All Customer Data must be subject to a regular backup cycle consistent with the nature of data being processed to ensure that data can be recovered in the event of any data loss, for which Celonis is not responsible. Recovery from backups shall be tested by You at least annually.

9. Responsabilidades del cliente

9.1 Debe tomar todas las medidas razonables para garantizar que se implementan y aplican las salvaguardas administrativas, técnicas, físicas, organizativas y operativas adecuadas para todas las áreas bajo su control, incluidas, entre otras, las siguientes

i. Garantizar que los Datos del Cliente a los que se apliquen los requisitos de seguridad elevados de HIPAA, FedRAMP o similares se carguen únicamente en las instancias de EMS designadas específicamente como apropiadas para dichos datos;
ii. Garantizar que la información de las tarjetas de pago no se cargue ni se publique de otro modo en ningún entorno de EMS;
iii. Implementar todos los controles de seguridad apropiados configurables por el cliente para proteger Sus Datos de Cliente;
iv. Implementar copias de seguridad del sistema fuente y de los Datos del Cliente, así como controles adecuados de higiene de datos;
v. Garantizar que todas las herramientas de anonimización o pseudonimización (incluidas las que Celonis pone a su disposición) estén configuradas correctamente;
vi. Protegerse contra el malware y otras actividades maliciosas, incluyendo, sin limitación, el escaneo de Sus sistemas y Datos de Cliente con versiones actualizadas de software antivirus estándar del sector y el uso de tecnologías de cortafuegos adecuadas;
vii. Supervisar y actualizar la página de estado para indicar las incidencias que afecten a la disponibilidad (status.celonis.com). Proporcionaremos actualizaciones mientras dure el incidente;
viii. Gestionar y proteger sus funciones y credenciales de usuario; y
ix. Gestionar y proteger las claves de cifrado que Usted posea para garantizar la integridad, disponibilidad y confidencialidad de la clave y de los Datos del cliente protegidos con dicha clave.

9.2 Todos los Datos de Cliente deben someterse a un ciclo regular de copias de seguridad coherente con la naturaleza de los datos que se procesan para garantizar que los datos puedan recuperarse en caso de pérdida de datos, de la que Celonis no es responsable. El Cliente deberá comprobar la recuperación de las copias de seguridad al menos una vez al año.