aruba.it

Aruba - Soluciones Cloud

Anexo A
ISO 27001:2017

14.04.2023

Anexo A - ISO 27001:2017 Aspectos de seguridad del Cloud del Grupo Aruba			
Área de control		**Nuestros controles**	**Herramientas y funcionalidades a disposición del Cliente**
A.5	**Políticas de seguridad de la información**	**Políticas del Sistema de Gestión de Seguridad de la Información** (SGSI) - El Grupo Aruba ha definido el enfoque adoptado por la organización para la gestión de sus objetivos de Seguridad de la Información dentro de una Política corporativa específica. Este documento ha sido aprobado por la Dirección y publicado en la intranet de la empresa. Para respaldar esta Política, existen políticas y procedimientos adicionales para temas específicos que definen el Sistema de Gestión de Seguridad de la Información del Grupo Aruba.	
A.6	**Organización de la seguridad de la información**	**Roles y Responsabilidades** - Dentro del ámbito de responsabilidad como proveedor de servicios en la nube, tal como se define en la página dedicada al modelo de responsabilidad compartida, el Grupo Aruba ha definido las figuras, los roles, las competencias y las responsabilidades relacionadas con los procesos, según los principios de Segregation of Duties, Least Privilege y Dual Control. **Segregation of Duties (SoD)** - Como parte de los procesos operativos de los Servicios, diferentes personas llevan a cabo diferentes procedimientos, de modo que ninguna persona individual tiene el control de todo el proceso. **Least Privilege** - Los permisos de acceso a locales, aparatos, datos, funcionalidades, etc., se conceden al personal encargado de los servicios, según el principio del "least privilege", es decir, en la medida necesaria para que dichos recursos puedan desempeñar las tareas que se les asignan, pero no más allá. **Dual Control** - Los procedimientos más críticos desde el punto de vista de la seguridad requieren la participación de al menos dos personas.	**Roles y Responsabilidades** - La descripción general del servicio está disponible dentro de la Knowledge Base (KB), en la página dedicada a la descripción general del servicio, junto con la tabla con los lugares de prestación de los servicios y la tabla del modelo de responsabilidad compartida entre el Grupo Aruba como proveedor de servicios en la nube y sus clientes.
A.7	**Seguridad de los recursos humanos**	**Formación del personal** - Los empleados del Servicio tienen la competencia y la experiencia adecuadas y se les proporciona formación específica para cada actualización importante del sistema. **Conciencia (Awareness)** - Periódicamente, se sensibiliza al personal sobre los temas de seguridad, sobre el cibercrimen en general y sobre	**Formación y concienciación** – El Grupo Aruba proporciona una Knowledge Base que contiene información relacionada con los servicios del Grupo Aruba. Contiene información sobre los servicios, guías, tutoriales, documentación sobre la interfaz de programación de aplicaciones (API), el glosario y el registro de cambios de los servicios.

Anexo A - ISO 27001:2017 Aspectos de seguridad del Cloud del Grupo Aruba			
Área de control		**Nuestros controles**	**Herramientas y funcionalidades a disposición del Cliente**
		las mejores prácticas a adoptar, mediante cursos de formación específicos. **Non Disclosure Agreement (NDA)** - Se requiere que los nuevos empleados firmen un acuerdo de confidencialidad para proteger el know-how y otra información confidencial de la empresa.	
A.8	**Gestión de activos**	**Asset Inventory** - Hay un inventario actualizado de activos, que incluye las máquinas virtuales y físicas que proporcionan los servicios y su ubicación física dentro de la infraestructura del Grupo Aruba. Cada vez que se instala una nueva máquina dentro de la infraestructura, se actualiza el inventario de activos. Además, para verificar posibles desfases, diariamente se realizan escaneos automáticos en las redes para detectar posibles nuevos activos. Dentro del inventario hay una categorización de los activos en la que se describen sus características: por ejemplo, el tipo de máquina (virtual o física), la infraestructura a la que pertenece, la propiedad interna, etc. **Handling of Assets** - También hay procedimientos internos que definen y formalizan las actividades relacionadas con la preparación de las nuevas máquinas y la gestión de las mismas (por ejemplo, cómo realizar un cambio, cómo actualizar los sistemas, etc.). **Gestión de las configuraciones** - Se define la lista de los componentes del Sistema para permitir la identificación de los componentes individuales de hardware y software y, respectivamente, de su modelo o de su versión. **Mantenimiento y asistencia** - Los componentes hardware (HW) más importantes para la continuidad del servicio están cubiertos por contratos de mantenimiento que garantizan la reparación o sustitución en tiempos adecuadamente rápidos por parte del proveedor, o bien se conservan en almacén componentes idénticos que pueden ser puestos en funcionamiento en caso de necesidad. Por lo que respecta a los software (SW) comerciales, se prevén contratos de asistencia correspondientes que garantizan la asistencia técnica del proveedor en caso de funcionamiento anómalo.	**Propiedad de los activos** - Dentro de la lógica de responsabilidad compartida, el Grupo Aruba ha identificado, para cada servicio, las respectivas atribuciones de propiedad con respecto a la infraestructura, licencias, direcciones IP, software proporcionado por el Grupo Aruba, software, datos y contenidos introducidos por el cliente. La información sobre la propiedad de los activos de servicios está disponible para los clientes dentro de la KB pública en la página dedicada a ello. **Eliminación de datos** - A través de la técnica del disk wipe en entorno Cloud, para los servicios VPS (Smart), PRO y Private Cloud, el cliente tiene la posibilidad de eliminar definitivamente los datos contenidos en su máquina y hacer imposible su recuperación. La página dedicada de la KB muestra los pasos operativos. **Etiquetado** - Los servicios del Grupo Aruba permiten a los clientes nombrar y clasificar los activos bajo su control. Las guías publicadas en Knowledge Base proporcionan orientación precisa sobre cómo realizar estas operaciones y cuáles son las limitaciones.

Anexo A - ISO 27001:2017 Aspectos de seguridad del Cloud del Grupo Aruba			
Área de control		**Nuestros controles**	**Herramientas y funcionalidades a disposición del Cliente**
		Eliminación - El Grupo Aruba garantiza la implementación de procedimientos específicos de eliminación y destrucción de los componentes de hardware desechados, tanto para los centros de datos extranjeros de coubicación como para los centros de datos propios, con el fin de garantizar que por cada almacenamiento que haya alcanzado el final de su vida útil y que deba ser reemplazado y eliminado, se eliminen todos los datos contenidos en el mismo de forma completa y definitiva.	
A.9	**Control de los accesos**	**Gestión de accesos lógicos**- Antes de acceder a los sistemas internos, se solicita al personal autorizado que se identifique (mediante nombre de usuario, contraseña y/o tarjeta inteligente). El personal del Grupo Aruba solo puede acceder, previa autenticación, a los recursos (por ejemplo, sistemas, datos) para los que ha sido autorizado explícitamente, según las necesidades reales del cargo desempeñado. La gestión de usuarios se realiza a través del controlador de dominio Active Directory (AD). Para garantizar el principio de "Segregation of Duty", los accesos lógicos al entorno de producción se gestionan a través de AD en un dominio dedicado, en cuyo interior hay usuarios con privilegios y permisos diferentes según el rol de trabajo de cada uno, respetando el principio de privilegio mínimo. Todos los usuarios son nominales, por lo que no hay usuarios de grupo y/o compartidos y se someten periódicamente a una verificación independiente por parte del Departamento de Seguridad. **Política de contraseñas** - De acuerdo con las políticas de seguridad del grupo y de conformidad con la legislación sobre privacidad ("medidas mínimas", medidas del Garante), se aplica una política segura de gestión de contraseñas. Después de la creación de un usuario, está previsto el cambio de contraseña obligatorio en el primer inicio de sesión y, posteriormente, el cambio de contraseña obligatorio periódico después de un intervalo de tiempo definido.	**Gestión de los accesos lógicos** - El cliente tiene garantizada en todo momento la posibilidad de registrar, modificar, suspender, reactivar y cancelar sus perfiles de usuario, así como de gestionar sus aspectos comerciales (créditos, umbrales, perfiles asociados, etc.). A nivel de permisos, cada cliente tiene la posibilidad de gestionar sus activos desde el punto de vista administrativo estableciendo niveles de seguridad y gestión de los permisos de acceso. En concreto, los clientes tienen la posibilidad, dependiendo del servicio, de: • Asignar una o varias máquinas virtuales a sus usuarios, haciendo uso del sistema de contabilidad dentro de la máquina virtual. • Para los servicios de Cloud Object Storage, Cloud Backup puede crear credenciales únicas para asignarlas a grupos de recursos independientes. • Para el servicio Virtual Private Cloud, es posible crear conjuntos de usuarios técnicos con diferentes permisos dentro del panel de control técnico. • Para los clientes asociados, siempre es posible definir los conjuntos de operaciones permitidas a los usuarios mediante reglas de elaboración de perfiles correspondientes. Los permisos están organizados de manera jerárquica.
A.10	**Cifrado**	**Canal seguro TLS** - Los flujos de datos hacia/desde los sistemas están protegidos por canal seguro TLS,	**Controles criptográficos**: sugerimos que los clientes adopten un enfoque basado en el riesgo e implementen controles

Anexo A - ISO 27001:2017 Aspectos de seguridad del Cloud del Grupo Aruba			
Área de control		**Nuestros controles**	**Herramientas y funcionalidades a disposición del Cliente**
		mediante una configuración adecuada en los servidores, para garantizar: • La verificación del servidor; • El cifrado de la sesión con un algoritmo de cifrado simétrico considerado suficientemente seguro. Esto se aplica tanto a los flujos generados de forma interactiva (navegación web) como a los generados automáticamente (por ejemplo, consulta de servicios web). Como algoritmo de cifrado simétrico, hoy en día se utiliza principalmente AES. La versión de TLS habilitada es la más alta posible, teniendo en cuenta las capacidades de los software cliente. Los certificados SSL Server instalados en los servidores expuestos en Internet son emitidos por una CA reconocida como fiable por los principales navegadores y sistemas operativos. Los detalles de los certificados en uso en los paneles en la nube y los protocolos utilizados en la red pública están disponibles en KB en la página dedicada a los certificados utilizados en los paneles Cloud. **Cifrado de datos en reposo** - Los datos "en reposo" más críticos para la seguridad, como contraseñas, semillas de tokens OTP y otros datos que deben mantenerse confidenciales para garantizar la fiabilidad de los procesos, se almacenan mediante cifrado simétrico, utilizando un algoritmo que se considera suficientemente seguro. En lo que respecta más concretamente a la protección de credenciales, las contraseñas se almacenan en el repositorio en modo "hashata" no reversible (huella o resumen de datos), mediante el uso del algoritmo de hashing SHA-512.	criptográficos adicionales en sus áreas de responsabilidad (ver tabla del modelo de responsabilidad compartida) en caso de que los datos procesados dentro del servicio del Grupo Aruba sean particularmente confidenciales. **Aruba Cloud Backup – Cifrado** - El servicio Cloud Backup ofrece la posibilidad de cifrar los datos almacenados como copia de seguridad incluso antes de la transferencia con una contraseña segura (estándar AES-256).
A.11	**Seguridad física y ambiental**	**Data Center**- Los sistemas para la prestación del Servicio Cloud se encuentran en el Data Center de Arezzo IT1 e IT2, situados respectivamente en Via Gobetti 96 y Via Ramelli 8, y los Data Centers IT3 DCA y DCB de Ponte San Pietro (BG) en Via San Clemente 53. Además de los data centers italianos, el Grupo Aruba cuenta con una red internacional de	

Anexo A - ISO 27001:2017 Aspectos de seguridad del Cloud del Grupo Aruba			
Área de control		**Nuestros controles**	**Herramientas y funcionalidades a disposición del Cliente**
		infraestructuras, tanto propias como pertenecientes a socios cualificados: • Data center CZ1, ubicado en Ktiš (República Checa), que pertenece a la red internacional de data centers propiedad de la Organización. • Data center FR1, ubicado en París (Francia), que pertenece a la red de data centers asociados. • Data center DE1, ubicado en Frankfurt (Alemania), que pertenece a la red de data centers asociados. • Data center UK1, ubicado en Londres (Reino Unido), que pertenece a la red de data centers asociados. • Data center PL1, ubicado en Varsovia (Polonia), que pertenece a la red de data centers asociados. **Edificios antisísmicos** - Los Data Centers del Grupo Aruba cumplen con la normativa antisísmica. **Control de accesos físicos** -Solo pueden acceder a los edificios aquellas personas que realmente lo necesiten registrándose previamente en la recepción. El acceso a las salas técnicas solo está permitido a los empleados autorizados, previa identificación con su tarjeta de identificación y el PIN correspondiente. El sistema de gestión de acceso ofrece la posibilidad de habilitar y deshabilitar las tarjetas personales según las áreas, los horarios y otros parámetros, para garantizar así la máxima seguridad de los entornos y la fluidez necesaria de los accesos. **Sistemas antiintrusión** - En los centros de datos y oficinas hay rejillas, ventanas de protección antibalas, puertas blindadas, puertas motorizadas (antiintrusión pasiva) y sistemas de CCTV y/o VMD (antiintrusión activa) instalados. El sistema de alarmas antiintrusión por zonas funciona de forma totalmente automática. Los data centers están divididos internamente en varias zonas, regidas por sistemas antiintrusión. Además, en todas las zonas están instalados sensores de movimiento capaces de detectar la presencia de personas; en las zonas sensibles (salas de datos, power center, almacenes) también hay	

Anexo A - ISO 27001:2017 Aspectos de seguridad del Cloud del Grupo Aruba			
Área de control		**Nuestros controles**	**Herramientas y funcionalidades a disposición del Cliente**
		sensores que detectan la apertura de las puertas y se utiliza la credencial para entrar y salir. **Sistema de extinción de incendios** - Este sistema respeta las normas legales y los estándares técnicos de referencia. Todas las plantas de los edificios cuentan con sensores de detección de incendios. **Sistema antiinundación** - Hay instalados sistemas de detección de líquidos y antiinundación. Los edificios también están ubicados en zonas llanas y en una posición elevada respecto al nivel del campo. **Sistema de suministro eléctrico** - Este sistema está presente en los Data Centers por partida doble en todos los niveles (grupos de transformación, power center, UPS, grupos electrógenos, cuadros de distribución, etc.) para garantizar la continuidad del suministro eléctrico en todas las condiciones previsibles. Incluye también las medidas destinadas a contener el efecto de descargas eléctricas de origen atmosférico, picos de la red eléctrica, etc. **Sistema de ventilación y aire acondicionado (HVAC)** - Garantiza condiciones ambientales y microclimáticas óptimas para el correcto funcionamiento de los servidores alojados en los Data Centers. **Conexión a Internet** - En los edificios hay conexión suficiente, con una capacidad de al menos el doble del mínimo necesario. **Control Room e Facility Operation Center (FOC)** - Los Data Centers están supervisados las 24 horas del día, los 365 días del año, por personal informático cualificado que garantiza la supervisión constante de la infraestructura y los servicios y la intervención en caso de necesidad. **Seguro** - La compañía ha firmado una póliza de seguros para cubrir los riesgos no previstos por las medidas de seguridad restantes.	
A.12	**Productos**	**Procedimientos operativos** - Los procedimientos que prescriben comportamientos operativos están documentados y disponibles y son conocidos por el personal involucrado. **Refuerzo de los servidores** - Los servidores que alojan componentes críticos para la seguridad de los servicios se someten a intervenciones	**Copias de seguridad** - Los servicios cloud ofrecidos por el Grupo Aruba permiten a los clientes crear y configurar sus propias copias de seguridad automatizadas a través de la solución Cloud Backup y Bare Metal Backup, eligiendo sus propias políticas en términos de cifrado, periodicidad, tipo

Anexo A - ISO 27001:2017 Aspectos de seguridad del Cloud del Grupo Aruba			
Área de control		**Nuestros controles**	**Herramientas y funcionalidades a disposición del Cliente**
		sistemáticas destinadas a reducir la superficie de ataque, tales como: eliminación de software innecesario, desactivación de servicios/protocolos innecesarios, instalación de parches de seguridad recomendados por los proveedores, aplicación de políticas para la complejidad de las contraseñas, habilitación de los registros de seguridad, etc. **Protección contra Distribuided Denial of Service (DDoS)-** Existe un sistema que analiza los datos entrantes para detectar el tráfico anómalo y, cuando es posible, bloquear los paquetes potencialmente maliciosos. **Seguimiento (logging)** - Se recopilan y almacenan los registros de los servidores de infraestructura para el acceso privilegiado a los sistemas de acuerdo con los requisitos legales. El equipo de seguridad verifica periódicamente estos registros mediante auditorías internas. Se ponen a disposición de los clientes los registros de aplicación de las operaciones realizadas durante el uso de los servicios. Del mismo modo, el trabajo de los Administradores del Sistema es objeto, al menos una vez al año, de una verificación por parte de los responsables del tratamiento, con el fin de controlar el cumplimiento de las medidas organizativas, técnicas y de seguridad relativas al tratamiento de datos personales previstas por las normas vigentes. **Monitoreo y Alerta** - Los sistemas críticos del Servicio están controlados por un sistema de monitoreo supervisado de manera continua. El sistema tiene la capacidad de generar "alertas", en forma de mensajes de correo electrónico o SMS, que permiten informar rápidamente al personal sobre un posible incidente o mal servicio, de modo que las acciones correctivas necesarias puedan implementarse lo antes posible. **Backup (parte dentro de la competencia del Grupo Aruba)** - Los componentes funcionales para la prestación del servicio , la gestión de los usuarios y los demás componentes arquitectónicos del servicio siguen los procedimientos de backup definidos a nivel empresarial que se verifican y prueban periódicamente. **Antivirus** - Todos los equipos de la red del Grupo Aruba están controlados, monitorizados y	(completo o incremental) y otras necesidades específicas. El servicio opcional de **Disaster Recovery as a Service (DRaaS)** también permite probar los procedimientos de conmutación por error sin interrupciones. Todos los procedimientos de gestión de los servicios de copias de seguridad y restauración se realizan de forma autónoma por los usuarios y están descritos en la Knowledge Base (KB) del servicio en la página dedicada a ello, donde se describen también los diversos métodos que pueden ser utilizados para hacer copia de seguridad de los datos propios. No se hace ninguna otra copia de seguridad de los datos más allá de las definidas de forma independiente por los usuarios. **Registro** – El Grupo Aruba pone a disposición de los clientes los logs aplicativos que producen durante el uso de los servicios. • Cloud PRO: el usuario puede consultar registros para llevar a cabo operaciones en máquinas virtuales como creación, eliminación, almacenamiento, restauración, encendido, apagado, restablecimiento, cambio de contraseña, cambio de características, creación y eliminación y restauración de instantáneas. • Cloud VPS (SMART): el usuario puede consultar logs para operaciones en máquinas virtuales como creación, cancelación, encendido, apagado, restablecimiento, actualización. • Virtual Switch: el usuario puede consultar registros para operaciones en Virtual Switch como compra y eliminación y cambios de características. • IP públicas: el usuario puede consultar los registros para llevar a cabo operaciones de IP públicas, como la compra y eliminación de una IP pública, la gestión y los cambios en reverseDNS. • Balanceadores: el usuario puede consultar los registros para llevar a cabo

Anexo A - ISO 27001:2017 Aspectos de seguridad del Cloud del Grupo Aruba			
Área de control		**Nuestros controles**	**Herramientas y funcionalidades a disposición del Cliente**
		protegidos por sistemas EDR. La tecnología EDR (Endpoint Detection and Response) es capaz de monitorizar en tiempo real y de forma proactiva las amenazas conocidas y desconocidas que afectan a todos los endpoints y servidores empresariales. Un grupo especializado con cobertura H24 se ocupa de analizar los acontecimientos inusuales e intervenir rápidamente. **Proceso de gestión de vulnerabilidades** - Todo el perímetro del Grupo Aruba es escaneado regularmente por herramientas automáticas y por profesionales cualificados del sector con el fin de identificar cualquier posible vulnerabilidad, incluso potencial. Cada problema identificado se comunica inmediatamente al grupo correspondiente, iniciando un ciclo de resolución del problema que puede terminar con una nueva versión o con una mitigación (por ejemplo, parches virtuales). Para comprobar su eficacia, se lleva a cabo un nuevo análisis para asegurarse de que la vulnerabilidad haya desaparecido. **Capacity Management y Change Management** - Con el fin de garantizar la correcta entrega/prestación del servicio, el Grupo Aruba considera fundamental supervisar los recursos disponibles, analizar las capacidades y adoptar las medidas adecuadas para el uso óptimo de los mismos y para garantizar el uso normal de los servicios. Los niveles de conectividad, los niveles de ocupación de los recursos, el espacio en disco y el tamaño de la infraestructura son monitoreados con herramientas específicas por el grupo de operadores pertenecientes a la Control Room 24/7/365, cuya tarea también se extiende al monitoreo de cualquier anomalía. Las herramientas de monitorización permiten configurar controles específicos para cada servicio, detectando las anomalías y permitiendo anticipar las necesidades de cambio. Los cambios necesarios en las actividades de seguimiento y gestión de la capacidad se gestionan de forma controlada para permitir la verificación de los resultados y el seguimiento de las actividades llevadas a cabo.	operaciones en los balanceadores, como la creación, la modificación, la cancelación, la activación o desactivación del balanceador, la adición de modificaciones y la eliminación de reglas. • Almacenamiento unificado: el usuario puede consultar los registros para llevar a cabo operaciones en los Virtual Switch, como la compra y eliminación y los cambios en las características. • Servicio FTP: el usuario puede consultar registros para llevar a cabo operaciones en cuentas FTP como activación y eliminación y modificación de espacio. • Virtual Private Cloud: el usuario puede consultar los registros para llevar a cabo operaciones en su Private Cloud, como creación, eliminación y modificación de los recursos. • Cloud Backup: el usuario puede consultar registros para llevar a cabo operaciones en sus cuentas de copias de seguridad relacionadas con la creación, cancelación y modificaciones del plan, cambio o restablecimiento de contraseña. • Cloud Monitoring: el usuario puede consultar los registros para llevar a cabo operaciones en sus servicios de monitoreo y los controles relacionados, como la creación de un plan de monitoreo o la adición de un nuevo control, la eliminación de un plan de monitoreo o control, los cambios en el plan de monitoreo o en un solo control. • Cloud Object Storage: el usuario puede consultar registros para llevar a cabo operaciones en sus cuentas de Object Storage relacionadas con la creación, eliminación y cambios en el plan, cambio o restablecimiento de contraseñas. • Domain Center: el usuario puede consultar registros para llevar a cabo operaciones en sus propios dominios y DNS relacionadas con la adición de nuevo dominio, cancelación de dominio y cambios en los datos relacionados con el dominio, creación de DNS, cancelación de DNS, cambios en cualquier registro DNS.

Anexo A - ISO 27001:2017 Aspectos de seguridad del Cloud del Grupo Aruba			
Área de control		**Nuestros controles**	**Herramientas y funcionalidades a disposición del Cliente**
		Actualizaciones y parcheo - En todos los sistemas se realiza periódicamente la actualización y el parcheo mediante herramientas centralizadas y siguiendo procedimientos internos que prevén un test previo en los entornos de desarrollo. Una vez superada esta fase, se ejecuta la aplicación en el entorno de producción. **Sincronización** - Todos los sistemas Cloud utilizan el sistema NTP para sincronizar sus relojes y mantener la coherencia de los eventos. La fuente autorizada para la sincronización del reloj es INRiM (http://www.inrim.it). La zona horaria en todos los sistemas utilizados es CEST, excepto en el Reino Unido, donde se utiliza GMT. Todas las máquinas virtuales suministradas tienen una zona horaria basada en CEST y utilizan la fuente de sincronización del host en el que residen como fuente de sincronización de reloj. **Multicliente y eliminación segura de datos** – El Grupo Aruba ofrece un sistema multicliente que permite separar las instancias de clientes individuales entre sí y separar las instancias de clientes de las instancias de Cloud Service Provider. El panel cloud público ha sido desarrollado expresamente por el Grupo Aruba en modalidad multicliente siguiendo las directrices para la programación segura y solo permite el acceso y la administración de la infraestructura Cloud propia. Además, para los servicios PRO, VPS y Virtual Private Cloud, y siempre que se utilice un software externo, el multicliente está garantizado directamente por los sistemas de virtualización utilizados. A la finalización del servicio, o al agotamiento del crédito, según lo definido contractualmente, el Grupo Aruba procede a la cancelación y eliminación definitiva de los datos de los servicios Cloud según lo descrito en la página dedicada a lo que sucede cuando se agota el crédito. La cancelación, dependiendo del servicio, puede ocurrir a través de API, paneles técnicos, scripts o software específicos. El Grupo Aruba gestiona la eliminación periódica de los archivos temporales de sus sistemas cloud con un proceso definido.	• Jelastic Cloud: el usuario puede consultar registros para llevar a cabo operaciones en sus cuentas de Jelastic Cloud relacionadas con la creación, cancelación y cambios de planes, cambio o restablecimiento de contraseñas. • Database as a Service (DBaaS): el usuario puede consultar registros para llevar a cabo operaciones en sus cuentas de "Database as a Service" relacionadas con la creación, cancelación y modificaciones del plan, cambio o restablecimiento de contraseña, copia de seguridad y restauración de bases de datos y reinicio de instancias. **Capacity Management** - En lo que respecta a la gestión de la capacidad del cliente, el Grupo Aruba permite al cliente controlar constantemente el consumo de los recursos económicos y técnicos a su disposición, lo que también le permite realizar previsiones. Además, durante la fase de adquisición del servicio se describen los casos en los que existen límites a la capacidad de expansión de los recursos. **Sincronización**- Cuando se considera que la sincronización de los relojes puede ser un problema para el cliente, se proporciona información detallada en la Knowledge Base pública (por ejemplo, en la página de operaciones del cronograma) o en los paneles de administración. **Multicliente** Cloud PRO. La arquitectura multicliente está garantizada: • Por el panel cloud público desarrollado expresamente en modo multicliente por el Grupo Aruba y las API públicas autenticadas. Estas soluciones solo permiten el acceso y la administración de su infraestructura Cloud. • Por el sistema de virtualización Hyper-V, Vmware o Openstack. El cliente solo tiene acceso a sus máquinas virtuales (VM) que los hipervisores subyacentes mantienen aisladas lógicamente de las

Anexo A - ISO 27001:2017 Aspectos de seguridad del Cloud del Grupo Aruba			
Área de control		**Nuestros controles**	**Herramientas y funcionalidades a disposición del Cliente**
			demás. Las VM proporcionadas al cliente se instalan con herramientas de control de acceso cuyas credenciales las elige directamente el cliente en la fase de creación. Las herramientas de acceso que se incluyen con las máquinas son SSH para entornos Linux y RDP para entornos Windows. Las redes públicas se comparten entre los clientes, pero en todas las máquinas disponibles hay un firewall perimetral para uso del cliente. Además de esto, el cliente tiene la opción de comprar el servicio Virtual Switch que consiste en proporcionar una VLAN dedicada y no compartida con otros clientes en la que el cliente puede interconectar sus máquinas para la máxima segregación. Cloud VPS (SMART). La arquitectura multicliente está garantizada: • Por el panel cloud público desarrollado expresamente en modo multicliente por el Grupo Aruba y las API públicas autenticadas. Estas soluciones solo permiten el acceso y la administración de su infraestructura Cloud. • Por el sistema de virtualización Vmware y Opesnstack. El cliente solo tiene acceso a sus máquinas virtuales que los hipervisores subyacentes mantienen aisladas lógicamente de las demás. Las VM proporcionadas al cliente se instalan con herramientas de control de acceso cuyas credenciales las elige directamente el cliente en la fase de creación. Las herramientas de acceso que se incluyen con las máquinas son SSH para entornos Linux y RDP para entornos Windows. Las redes públicas se comparten entre los clientes, pero en todas las máquinas disponibles hay un firewall perimetral para uso del cliente. Virtual Switch y Hybrid Link: estos son recursos dedicados a un solo cliente. El multicliente está garantizado por el panel cloud público desarrollado expresamente en modo multicliente por el Grupo Aruba y las API públicas autenticadas. Estas

Anexo A - ISO 27001:2017 Aspectos de seguridad del Cloud del Grupo Aruba			
Área de control		**Nuestros controles**	**Herramientas y funcionalidades a disposición del Cliente**
			soluciones solo permiten el acceso y la administración de su infraestructura Cloud. Virtual Private Cloud. La arquitectura multicliente está garantizada: • Por el panel vCloud Director, desarrollado expresamente en modo multicliente por VMware. Este panel solo permite el acceso y la administración de su infraestructura Cloud. • Por el sistema de virtualización VMware. El cliente solo tiene acceso a su Virtual Datacenter VM que los hipervisores subyacentes mantienen aislados lógicamente de los demás. Las VM proporcionadas al cliente se instalan con herramientas de control de acceso cuyas credenciales las elige directamente el cliente en la fase de creación. Las herramientas de acceso que se incluyen con las máquinas son SSH para entornos Linux y RDP para entornos Windows. En cada Virtual Datacenter proporcionado, se proporciona un software de firewall perimetral (NSX Edge) que permite el aislamiento de su Virtual Datacenter de los demás y permite al cliente configurar las reglas de seguridad óptimas para su propósito. El cliente tiene la posibilidad de crear de forma independiente redes privadas específicas y no compartidas por otros clientes para configurar su propia arquitectura. Bajo demanda, también se pueden proporcionar redes públicas específicas y no compartidas con otros clientes. Bare Metal Backup. La arquitectura multicliente está garantizada: • Por el panel cloud público desarrollado expresamente en modo multicliente por el Grupo Aruba y las API públicas autenticadas. Estas soluciones solo permiten el acceso y la administración de su infraestructura Cloud. • Por el panel de gestión de Veeam. El cliente solo tiene acceso a sus datos de copia de seguridad y no tiene ninguna posibilidad de ver o controlar los

Anexo A - ISO 27001:2017 Aspectos de seguridad del Cloud del Grupo Aruba			
Área de control		**Nuestros controles**	**Herramientas y funcionalidades a disposición del Cliente**
			sistemas de copia de seguridad de otros clientes. Disaster Recovery. La arquitectura multicliente está garantizada: • Por el panel cloud público desarrollado expresamente en modo multicliente por el Grupo Aruba y las API públicas autenticadas. Estas soluciones solo permiten el acceso y la administración de su infraestructura Cloud. • Por el panel de gestión de Zerto, Veeam, VMWare VCAV. El cliente solo tiene acceso a su conjunto de datos y no tiene ninguna posibilidad de ver o consultar los sistemas de Disaster recovery (DR) de otros clientes. Cloud Backup (Evault/Commvault). La arquitectura multicliente está garantizada: • Por el panel cloud público desarrollado expresamente en modo multicliente por el Grupo Aruba y las API públicas autenticadas. Estas soluciones solo permiten el acceso y la administración de su infraestructura Cloud. • Por el sistema de copia de seguridad Evault o Commvault. El cliente solo tiene acceso a sus datos de copia de seguridad y no tiene ninguna posibilidad de ver o controlar los sistemas de copia de seguridad de otros clientes. Cloud Monitoring: el multicliente está garantizado por el panel cloud público desarrollado expresamente en modalidad multicliente por el Grupo Aruba y por las API públicas autenticadas. Estas soluciones solo permiten el acceso y la administración de su infraestructura Cloud. Cloud Object Storage. La arquitectura multicliente está garantizada: • Por el panel cloud público desarrollado expresamente en modo multicliente por el Grupo Aruba y las API públicas autenticadas. Estas soluciones solo permiten el acceso y la administración de su infraestructura Cloud.

Anexo A - ISO 27001:2017 Aspectos de seguridad del Cloud del Grupo Aruba			
Área de control		**Nuestros controles**	**Herramientas y funcionalidades a disposición del Cliente**
			• Por el sistema de Identity and Access Management de Scality y CEPH . El cliente solo tiene acceso a su cuenta de almacenamiento y no tiene ninguna posibilidad de ver o consultar las cuentas de otros clientes. IaaS para SAP HANA. La arquitectura multicliente y la separación están garantizadas gracias a varias medidas: • Una VPN SSL específica que permite al cliente acceder al sistema de gestión de la plataforma. • Una cuenta única en el sistema de virtualización de VMware que le permite acceder solo a las máquinas virtuales del cliente. • La separación que proporciona la red específica puesta a disposición del cliente y no compartida con otros clientes. • Las herramientas internas suministradas con la VM que permiten la creación de múltiples perfiles de usuario y administrativos. Domain Center. El multicliente está garantizado por el panel cloud público desarrollado expresamente en modo multicliente por el Grupo Aruba y las API públicas autenticadas. Estas soluciones solo permiten el acceso y la administración de su infraestructura Cloud. Jelastic Cloud. La arquitectura multicliente está garantizada de dos modos: • Por el panel cloud público desarrollado expresamente en modo multicliente por el Grupo Aruba y las API públicas autenticadas. Estas soluciones solo permiten el acceso y la administración de su infraestructura Cloud. • Desde el sistema de Jelastic, el cliente sólo tiene acceso a su cuenta de jelastic y no tiene posibilidad alguna de ver o consultar cuentas de otros clientes.

Anexo A - ISO 27001:2017 Aspectos de seguridad del Cloud del Grupo Aruba			
Área de control		**Nuestros controles**	**Herramientas y funcionalidades a disposición del Cliente**
			Database as a service (DBaaS): la arquitectura multicliente está garantizada por el panel cloud público desarrollado expresamente en modo multicliente por el Grupo Aruba y las API públicas autenticadas. Estas soluciones solo permiten el acceso y la administración de su infraestructura Cloud.
A.13	**Seguridad de las comunicaciones**	**Firewall e IPS**. Los portales web expuestos para los servicios están protegidos por el firewall del data center del servicio cloud y protegidos por IPS. En cuanto a los servicios informáticos, todas las máquinas virtuales proporcionadas por el Grupo Aruba están modeladas y disponibles en forma de imágenes. Estas imágenes son producidas y probadas por los técnicos del Grupo Aruba y en particular, después de haber instalado el Sistema Operativo y efectuado la primera configuración, se habilita el sistema de firewall concediendo los privilegios mínimos posibles y abriendo sólo las puertas necesarias. **Virtual Private Network (VPN)** - El acceso remoto a la red (LAN) de la empresa solo está permitido al personal autorizado que lo necesite; el acceso remoto solo es posible a través de una VPN que garantiza confidencialidad de la comunicación, autenticación fuerte del servidor y autenticación fuerte (de dos factores) del usuario.	**Firewall** - El cliente es administrador de su propio servidor y, por lo tanto, tiene la capacidad de cambiar la configuración del firewall. Las guías y tutoriales de KB proporcionan información sobre cómo separar y proteger la seguridad de la red y configurar un firewall en el propio Aruba Cloud. **Virtual Switch** - El cliente tiene la posibilidad de adquirir el servicio de Virtual Switch que consiste en el suministro de una VLAN específica y no compartida con otros clientes sobre la cual el cliente puede interconectar sus máquinas para la máxima separación y la posibilidad de crear autónomamente redes privadas específicas y no compartidas por otros clientes para configurar su propia arquitectura (Virtual Private Cloud). Bajo demanda, también se pueden proporcionar redes públicas específicas y no compartidas con otros clientes. **Ubicación geográfica de los datos para garantizar la seguridad y el cumplimiento** - Los servicios prestados por el Grupo Aruba pueden opcionalmente servicios que se pueden activar en un datacenter o en una región (que coincide con un país). El cliente tiene la posibilidad de indicar el Datacenter o los Datacenter dentro de los cuales se activarán sus servicios y se transferirán sus datos; para los servicios regionales, los clientes tienen la posibilidad de seleccionar el país dentro del cual se activará el servicio.

Anexo A - ISO 27001:2017 Aspectos de seguridad del Cloud del Grupo Aruba			
Área de control		**Nuestros controles**	**Herramientas y funcionalidades a disposición del Cliente**
			En ningún caso el Grupo Aruba traslada sistemas o contenidos fuera de las localidades geográficas (DC o regiones) configuradas por sus clientes.
A.14	**Adquisición, desarrollo y mantenimiento de sistemas**	**Gestión de cambios** - Los cambios en el software de aplicación se someten a evaluación y aprobación antes de ser realizados; después se someten a pruebas antes de ser subidos a producción con el fin de verificar la correcta implementación de las nuevas funciones y la ausencia de regresiones. Además, todo el software desarrollado está administrado por un sistema de versionado.	**Gestión de cambios** – El Grupo Aruba pone a disposición de los clientes un changelog (como se detalla en la página dedicada en la KB) para comunicar las versiones, correcciones, correcciones y actualizaciones de los servicios ofrecidos.
A.15	**Relaciones con los proveedores**	**Gestión de proveedores** - La política empresarial que regula las relaciones con los proveedores establece que, para una correcta definición y gestión de las relaciones con cada nuevo proveedor, se tengan siempre en cuenta los siguientes aspectos, con especial atención a la seguridad de la información: • Evaluación del riesgo e investigaciones preliminares que deben llevarse a cabo para la valoración completa de un nuevo proveedor; • Selección de las cláusulas contractuales con el fin de evaluar si los contratos estándar cubren los riesgos identificados o si es necesario añadir o modificar cláusulas concretas; • Control de los accesos a la información, para proporcionar el acceso al proveedor según la lógica del "Need-to-know" y, por lo tanto, solo a los datos y a las informaciones que son efectivamente requeridas y necesarias para el desarrollo de la propia actividad; • Control de los accesos a los sistemas del Grupo Aruba a través de usuarios específicos, en caso de que el suministro rquiera que el proveedor acceda a los sistemas, utilizando una Private Network (VPN) y un sistema específico de detection response y virtual desktop infrastructure (VDI) suministrados por el propio Grupo Aruba; • Seguimiento de los inclumplimientos para el correcto desarrollo de los controles con el fin de poder verificar el cumplimiento del proveedor	

Anexo A - ISO 27001:2017 Aspectos de seguridad del Cloud del Grupo Aruba			
Área de control		**Nuestros controles**	**Herramientas y funcionalidades a disposición del Cliente**
		con respecto a los requisitos contractuales acordados y a la seguridad de la información. Además, los suministros externos necesarios para el desarrollo, el mantenimiento y la prestación del Servicio están sujetos a controles destinados a mitigar el riesgo de incidentes de seguridad causados por material no conforme o por acciones inadecuadas por parte de los proveedores. Todos los proveedores de servicios profesionales están obligados a firmar un acuerdo de confidencialidad (NDA). Los modelos contractuales utilizados por el Grupo Aruba para la prestación del servicio prevén la posibilidad de que el Grupo Aruba recurra a terceros para el desarrollo de sus actividades. Esta colaboración se basa en el compromiso, contractualmente previsto con eventuales subcontratistas, por parte del Grupo Aruba de verificar que éstos, según el tipo de servicio prestado, estén en condiciones de respetar los mismos requisitos y niveles de seguridad a los que se compromete el Grupo Aruba. El Grupo Aruba tiene una lista de subcontratistas de servicios que está disponible a petición de los clientes. Asimismo, en caso de incorporación de nuevos subcontratistas, el Grupo Aruba se compromete a comunicarlo a sus clientes con la suficiente antelación para permitir su oposición o desistimiento.	
A.16	**Gestión de incidentes de seguridad de la información**	**Proceso de gestión de incidentes de seguridad de la información** - El Grupo Aruba ha identificado y documentado dentro de una política específica su enfoque estructurado y programático para la gestión de eventos y/o incidentes de seguridad de la información que puedan ocurrir dentro del alcance operativo de las empresas del Grupo Aruba, aplicando la guía ISO 27035 en su flujo de gestión de incidentes de seguridad de la información. Este proceso se implementa mediante un plan específico que regula las medidas operativas que deben implementarse en caso de que se detecten incidentes de seguridad de la información. Se ha definido un flujo de gestión de incidentes y se han identificado las responsabilidades relacionadas con su aplicación, tanto en términos de gestión y	

Anexo A - ISO 27001:2017 Aspectos de seguridad del Cloud del Grupo Aruba			
Área de control		**Nuestros controles**	**Herramientas y funcionalidades a disposición del Cliente**
		resolución de incidentes como de apoyo estratégico para la adopción oportuna de las decisiones necesarias para hacer frente a los incidentes de seguridad más importantes (por ejemplo, incidentes mayores, incidentes desconocidos, Data Breach). También se han definido tiempos y disposiciones para la preparación y el envío de las comunicaciones relativas a los incidentes de seguridad de la información a autoridades, clientes y terceros.	
A.17	**Aspectos relativos a la seguridad de la información en la gestión de la continuidad operativa**	**Procedimiento de gestión de desastres** – El Grupo Aruba ha formalizado un Plan de Business Continuity, una Política y procedimientos específicos de BC relativos a los servicios esenciales para el funcionamiento de los Data Centers (suministro eléctrico, aire acondicionado y conexión). Los data centers están certificados ISO 27001 y en ellos se implementan las principales medidas para garantizar la seguridad física y la continuidad operativa de las instalaciones. Concretamente, los Data Centers IT1, IT3 DCA y DCB del Grupo Aruba cumplen con el nivel máximo nivel (Rating 4) entre los establecidos por la normativa ANSI TIA 942-B-2017. Este resultado, que indica la capacidad de evitar interrupciones en los servicios incluso en caso de averías graves (tolerancia a fallos), se ha logrado gracias a una serie de medidas de diseño e implementación que han abarcado todos los aspectos del data center: selección del sitio, aspectos arquitectónicos, seguridad física, sistemas contra incendios, instalaciones eléctricas, instalaciones mecánicas y red de datos. Un centro de datos de Rating 4 (anteriormente Tier 4) cuenta con componentes redundantes siempre activos, además de rutas de suministro eléctrico y enfriamiento de hardware con múltiples vías. Por último, los data centers están diseñados para resistir averías en cualquier punto del sistema sin causar tiempo de inactividad y están protegidos contra eventos físicos, incluyendo desastres naturales (por ejemplo, incendios, inundaciones,	**Disaster Recovery as a Service (DRaaS)** – El Grupo Aruba ofrece el servicio Disaster Recovery as a Service diseñado para garantizar la business continuity de las empresas, lo que permite replicar y restaurar rápidamente el acceso y la funcionalidad de la infraestructura informática después de una interrupción debido a un ataque cibernético, una avería o un desastre. A través de un panel web de autoservicio, en una conexión segura, el cliente puede crear de forma independiente directivas y políticas de Disaster Recovery, seleccionando la fuente (sitio principal) y el destino (sitio secundario) y eligiendo entre su propia infraestructura virtual VMware on-premise y/o data center del Grupo Aruba habilitados para el servicio Virtual Private Cloud.

Anexo A - ISO 27001:2017 Aspectos de seguridad del Cloud del Grupo Aruba			
Área de control		**Nuestros controles**	**Herramientas y funcionalidades a disposición del Cliente**
		terremotos, etc.). Los Data Centers IT3 DCA y DCB del Grupo Aruba están certificados ISO/IEC 22237, un estándar internacional de referencia para todo el ciclo de vida del sata center, desde la concepción estratégica hasta la implementación y puesta en funcionamiento, en línea con las normas ANSI/TIA 942 (estándar estadounidense) y EN 50600 (estándar europeo). El entorno cloud está compuesto por una infraestructura de múltiples data centers, cuyos servicios están interconectados a través de una red IPSEC de alta velocidad y protección. Dado que la estructura está diseñada para ser multi-data center, está naturalmente preparada para la Disaster Recovery, ya que todos los data centers son independientes entre sí desde el punto de vista lógico. Las máquinas virtuales de los clientes no están sujetas a Disaster Recovery geográficos, ya que se proporcionan a los propios clientes todas las herramientas necesarias para construir a medida sus sistemas y procedimientos de Disaster Recovery.	
A.18	**Cumplimiento**	**Protección de datos personales** - Todos los servicios prestados se gestionan en pleno cumplimiento de la legislación vigente en materia de protección de datos personales de acuerdo con el Reglamento de la UE 2016/679 ("GDPR"), el Decreto Legislativo 196/2003, así como el Decreto Legislativo 101/2018, y las Medidas de la Autoridad Garante para la protección de datos personales. **Revisión** (**auditoría**) - Los eventos registrados con el seguimiento, en particular aquellos que podrían indicar una amenaza a la seguridad, se analizan periódicamente. **Inspecciones internas** - El responsable de las verificaciones y de las inspecciones (auditoría) asegura la verificación del cumplimiento del servicio cloud con lo previsto en el presente documento y en las normas vigentes con una periodicidad al menos anual.	

HISTORIAL DE VERSIONES

VERSIÓN 1.1 DEL 14/04/2023	***NATURALEZA DE LAS MODIFICACIONES: Actualizados los controles A.12, A.13, A.17***

VERSIÓN 1.0 DEL 01/01/2022	***NATURALEZA DE LAS MODIFICACIONES: Primera emisión***