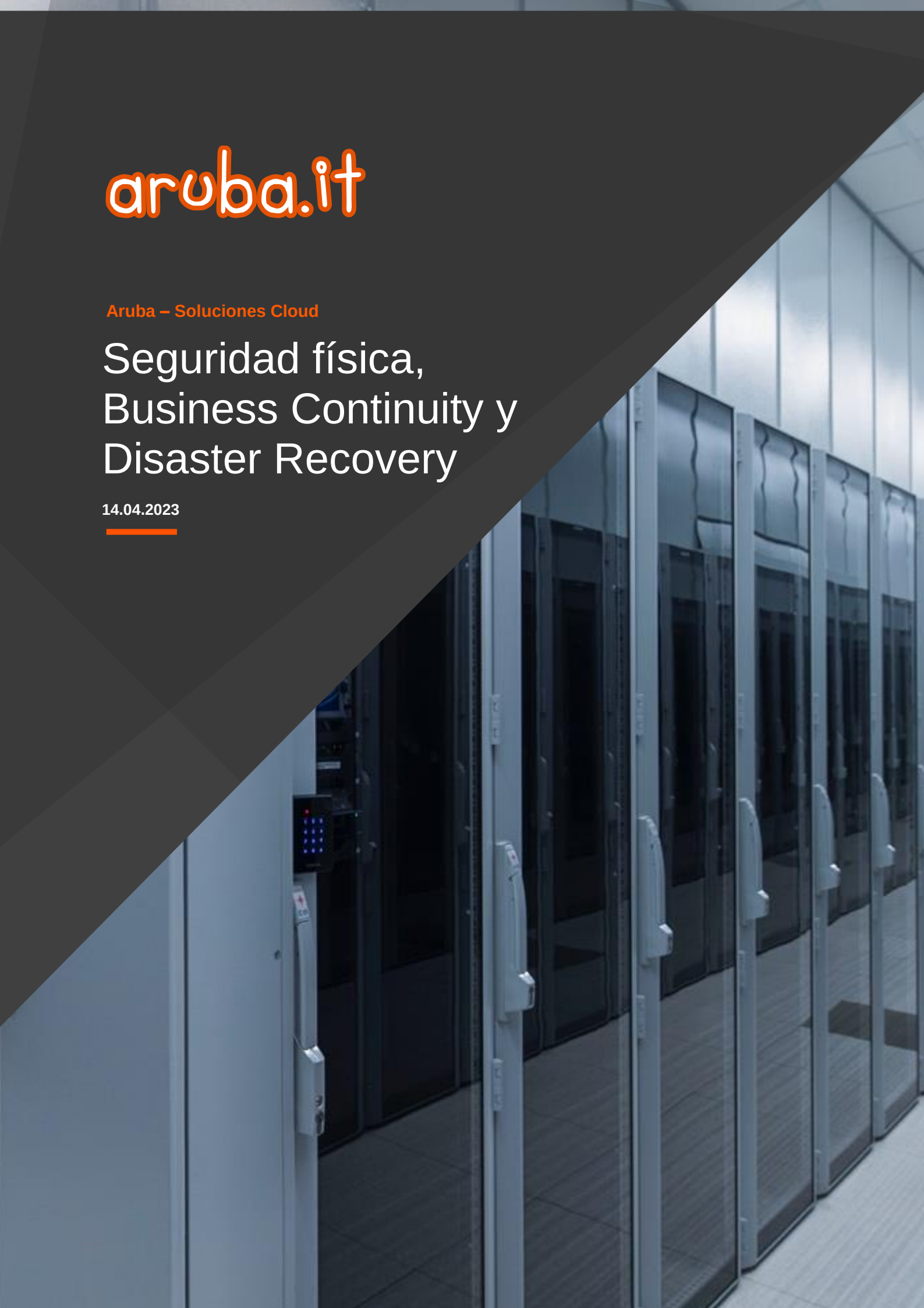
aruba.it

Aruba – Soluciones Cloud

Seguridad física, Business Continuity y Disaster Recovery

14.04.2023



ÍNDICE

Aruba S.p.A.
Via San Clemente 53 - 24036 Ponte San Pietro (BG) - CIF: 01573850516

1 HOUSING DE LOS SISTEMAS Y SEGURIDAD INFORMÁTICA

En Italia, todos los sistemas informáticos utilizados para la prestación de los servicios Cloud del Grupo Aruba se encuentran en los dos data centers de Arezzo IT1 e IT2, ubicados respectivamente en Via Gobetti 96 y Via Ramelli 8, así como los data centers IT3 DCA y DCB de Ponte San Pietro (BG), ubicados en Via San Clemente 53.

Figura 1 – Data Center IT1

Figura 2 – Data Center IT2

Figura 3 – Campus IT3

Además de los data centers italianos, para la prestación de los servicios Cloud, el Grupo Aruba cuenta con una red internacional de infraestructuras, tanto propias como de socios cualificados y, en particular:

- 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.

Figura 4 – Red internacional de data centers de los servicios Cloud

Para cumplir con los estrictos estándares de calidad, todos los data centers cuentan con la certificación ISO 9001.

En el siguiente apartado se explican las principales medidas de seguridad física que se han adoptado.

1.1 Descripción de medidas de seguridad física

Los data centers cuentan con la certificación ISO 27001 y en ellos se implementan las principales medidas destinadas a garantizar la seguridad física de las estructuras.

1.1.1 Tier 4*/Rating 4

Los data centers IT1, IT3 DCA y DCB del Grupo Aruba cumplen con el nivel más alto (Rating 4) entre los previstos por la norma ANSI TIA 942-B-2017. Este resultado, que indica la capacidad de los servicios para evitar interrupciones incluso en presencia de averías graves (tolerancia a los fallos), se ha obtenido gracias a la adopción de una serie de medidas de diseño y realización que afectan a todos los aspectos del data center: elección de la ubicación, aspectos arquitectónicos, seguridad física, sistemas antiincendios, instalación eléctrica, instalación mecánica y red de datos.

Un data center de Rating 4 (antes Tier 4) tiene componentes redundantes siempre activos, además de vías múltiples de alimentación y enfriamiento del hardware.

Los data centers están equipados para soportar una avería en un punto cualquiera de la planta sin causar un periodo de inactividad y están protegidos en caso de incidentes físicos, incluyendo entre otros las catástrofes naturales (p. ej. incendios, inundaciones, terremotos, etc.).

1.1.2 ISO/IEC 22237

Los data centers IT3 DCA y DCB del Grupo Aruba están certificados ISO/IEC 22237, que es un estándar internacional de referencia para todo el ciclo de vida de un data 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). La norma, llamada “Data centre facilities and infrastructures”, consta de siete partes: General concepts, Building construction, Power distribution, Environmental control, Telecommunications cabling infrastructure, Security systems y Management and operational information.

1.1.3 Monitorización 24 horas al día

Todos los data centers están monitorizados por un equipo técnico durante las 24 horas del día, los 365 días del año.

Además, los data centers asociados están gestionados a distancia por el equipo técnico de la Control Room de Aruba S.p.A..

Además de la vigilancia local, los data centers propietarios disponen de un sistema BMS (Building Management System) que avisa en tiempo real en caso de eventos relevantes y permite a los técnicos gestionar todas las instalaciones en remoto.

1.1.4 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.

Para los data centers propietarios, 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.

Algunos de los data centers asociados, como FR1, DE1 y UK1, cuentan con un sistema de control de acceso biométrico.

1.1.5 Sistemas antiintrusión

Todos los data centers cuentan con rejillas, ventanas de protección antibalas, puertas blindadas, puertas motorizadas (antiintrusión pasiva) e instalación de sistemas de CCTV y VMD (antiintrusión activa).

Además, en todas las zonas de los data centers propietarios se instalan sensores de movimiento que detectan la presencia de personas; en las zonas sensibles (salas de datos, Power Centers, almacenes) también hay sensores que detectan la apertura de puertas.

1.1.6 Sistema antiincendio, antiinundaciones y edificios antisísmicos

Todos los data centers cumplen con la normativa antisísmica. Además, hay sistemas de detección y extinción de incendios automáticos con gases inertes, inofensivos para las personas y para los sistemas informáticos e instalaciones de detección de inundaciones.

Además, los edificios están ubicados en zonas de llanura y en una posición elevada respecto al nivel del campo.

1.1.7 Sistemas de aire acondicionado redundantes

El sistema de climatización en las salas de datos y de equipamiento tecnológico se realiza mediante módulos múltiples redundantes que garantizan el funcionamiento de estas incluso en caso de varias averías simultáneas.

El sistema de climatización está protegido por un sistema UPS con baterías y generadores eléctricos de emergencia para garantizar la continuidad del servicio.

1.1.8 Alimentación y redundancia de los Power Centers

Para sus servicios, el Grupo Aruba utiliza exclusivamente servidores y sistemas dotados de alimentación doble. A la salida de cada Power Center se encuentran dispositivos STS (Static Transfer Switch) para garantizar la continuidad de alimentación eléctrica de las dos líneas presentes, garantizando así el funcionamiento a los servidores y a los sistemas que no dispongan de alimentador doble.

La alimentación suministrada a los servidores es completamente redundante gracias a dos Power Centers independientes. Cada uno de los Power Centers tiene la capacidad de alimentar las salas de datos de los data centers propietarios, incluso en carga completa, y está dotado de sistemas (UPS) de conversión doble y altísima eficiencia energética (redundancia de tipo 2N + 1 para IT1, IT2 e IT3 y de tipo 2N para CZ1).

Los sistemas de alimentación de los data centers asociados también son completamente redundantes y están dotados de sistemas (UPS) de doble conversión.

Para obtener más información sobre las características técnicas de los data center en análisis, consultar la página web: «Nuestros data centers».

2 BUSINESS CONTINUITY Y DISASTER RECOVERY

2.1 Introducción

El objetivo de este capítulo es describir el procedimiento de Disaster Recovery y Business Continuity puesto en marcha para garantizar su implementación en relación con los servicios Cloud del Grupo Aruba.

El negocio de todas las empresas y las actividades relacionadas con este, dependen estrictamente de la disponibilidad de estructuras y recursos específicos de los procesos de soporte. En general, el impacto derivado de la falta de disponibilidad del servicio crece a medida que persiste la interrupción de acuerdo con una tendencia exponencial, por lo que la capacidad de la empresa para operar puede verse comprometida de forma definitiva en poco tiempo.

Para garantizar la continuidad de los Procesos de Negocio es extremadamente importante proteger todos los recursos que contribuyen a la prestación de los servicios más críticos: información, personas e infraestructuras, tecnologías, redes de comunicación, etc.

El Grupo Aruba ha decidido dotarse de un programa de gestión de Business Continuity empresarial para analizar y gestionar los impactos en las operaciones frente a algunos escenarios de desastre y, en consecuencia, identificar las soluciones de recovery para fomentar la continuidad operativa.

Estas soluciones tienen como objetivo la restauración de los servicios esenciales tanto desde el punto de vista organizativo, como logístico e informático.

2.2 Plan de Business Continuity

El Plan de Business Continuity (en adelante denominado «BCP») o «Plan de Continuidad Operativa» es el conjunto de normas y procedimientos que (prefigurando uno o más escenarios de indisponibilidad capaces de interrumpir el funcionamiento normal de cualquier sistema organizado) define las responsabilidades, establece las actividades y proporciona las herramientas para gestionar la interrupción y conseguir un estado suficiente de funcionalidad operativa en el sistema.

El objetivo del BCP es asegurar la recuperación de los procesos críticos dentro de plazos tolerables y predeterminados para cada proceso.

Todo el entorno de producción relacionado con los servicios Cloud está protegido por el BCP empresarial, con pruebas de Business Continuity en la infraestructura que se programan anualmente.

Dicho Plan tiene la función de guiar al Grupo Aruba en la gestión y en la mediación de eventuales riesgos identificados aplicando la metodología de «Gestión del Riesgo para la Seguridad de la Información», descrita detalladamente en el capítulo específico.

El BCP también define y enumera las acciones que deben tomarse antes, durante y después de un estado de emergencia para garantizar la continuidad del servicio. Proporciona indicaciones y, cuando sea posible, instrucciones detalladas para garantizar la continuidad de los servicios críticos del Grupo Aruba, incluso en presencia de eventos no deseados que puedan causar la interrupción prolongada de los sistemas informáticos.

2.3 Disaster Recovery

El entorno Cloud está compuesto por una infraestructura de numerosos datacenter, cuyos servicios están interconectados por una red IPSEC de gran ancho de banda y de alta protección.

Cada data center ofrece numerosos tipos de servicios, entre los que se incluyen:

- Cloud Computing
- Jelastic Cloud
- Data Base as a Service
- Virtual Private Cloud – VPC
- Cloud Object Storage
- Domain Center
- Cloud Monitoring
- Cloud Backup

Además, cada data center cuenta con una estructura formada por las siguientes máquinas básicas:

- Domain Controller
- Balanceador LVS
- Front-End
- WCF (Microsoft Webservice)
- Aprovisionamient
- Contabilidad para la facturación
- Base de datos
- Hypervisor hosts
- Cloud Storage hosts
- Cloud Monitoring hosts
- Cloud Private hosts
- Cloud backup hosts

La estructura, que está pensada para diversos data centers, está predispuesta para el Disaster Recovery ya que todos los data centers son independientes entre ellos desde el punto de vista lógico.

Cabe destacar que las máquinas virtualizadas de los Clientes no están sujetas a Disaster Recovery geográfico, pues todos los Clientes disponen de las herramientas necesarias para construir los sistemas y los procedimientos de Disaster Recovery a medida.

Aruba S.p.A.
Via San Clemente 53 - 24036 Ponte San Pietro (BG) - CIF: 01573850516

HISTORIAL DE VERSIONES

VERSIÓN 1.1 DEL 14/04/2023	***NATURALEZA DE LAS MODIFICACIONES: Agregado: certificación ISO/IEC 22237 y Campus IT3 haciendo referencia a DCA y DCB; actualizada la lista de servicios Cloud***
VERSIÓN 1.0 DEL 01/01/2022	***NATURALEZA DE LAS MODIFICACIONES: Primera emisión***