Security Policy Cloud Services

Policy di sicurezza per servizi cloud

Revisione	Data	Redazione	Verifica	Approvazione	TLP
00	03/03/2025	Compliance	CISO	CEO	VERDE

Distribuzione

Indice

1. INTRODUZIONE

Il cloud computing offre numerosi potenziali benefici alle aziende che lo utilizzano, tra cui scalabilità, elasticità, alte prestazioni, minori carichi di lavoro per la sua gestione insieme a efficienza in termini di costi, agilità, tempi di immissione sul mercato più rapidi e nuove opportunità di innovazione.
Comprendere, gestire e controllare i rischi che riguardano principalmente le tematiche di riservatezza, sicurezza e resilienza legati all'adozione e/o all'erogazione di servizi in cloud è fondamentale per garantire una corretta gestione della sicurezza di tutte le tipologie di informazioni impattate.

2. SCOPO E CAMPO DI APPLICAZIONE

Il presente documento definisce le politiche aziendali specifiche, parti integranti della politica generale del SGSI definita da BDP, relativamente ai servizi cloud per la protezione dei dati, inclusi i dati personali, applicando le best practices definite dagli standard ISO 27017 e ISO 27018.
Lo scopo di questa politica pertanto è quello di descrivere i principi generali di sicurezza nell'ambito dei servizi in cloud che BDP ha deciso di applicare, al fine di garantire una sicurezza delle informazioni, conservate e/o gestite su piattaforme in cloud, di livello superiore o almeno pari ai principi espressi nella sua politica generale di sicurezza e conformi alla normativa vigente.

3. PERIMETRO ORGANIZZATIVO

La presente policy si applica a tutto il personale dipendente di BDP e a tutti i soggetti che collaborano con la stessa.
Nello specifico si applica a tutti i processi e a tutte le risorse che di volta in volta sono coinvolte nella gestione delle informazioni trattate dalla società.
È importante considerare che nel documento i termini "fornitori di servizi cloud" o "CSP", possono acquistare una duplice valenza a seconda del contesto, essendo BDP sia cliente che fornitrice di servizi in cloud.
Nel momento in cui la policy verrà applicata a servizi di cui BDP è cliente, con i suddetti termini ci si riferirà ai fornitori di tali servizi. Quando invece verrà applicata ai servizi erogati da BDP ai suoi clienti, ci si riferirà alla stessa BDP.

4. TERMINI E DEFINIZIONI

Asset o bene – qualsiasi risorsa che abbia un valore per l'organizzazione, sia essa materiale o immateriale (beni fisici, software, informazioni e dati…);
Cloud – insieme di servizi ICT accessibili on demand e/o in modalità self-service basati su risorse anche hardware remote, in rete e condivise, caratterizzati da rapida scalabilità e dalla misurabilità dei livelli di performance, garantendo in questo modo anche la possibilità di essere fruiti e pagati in base al consumo;
Cloud privato – piattaforma basata su cloud gestita internamente per erogare servizi e non aperta alla disponibilità di soggetti terzi;
Cloud pubblico – piattaforma basata su cloud che eroga servizi a più soggetti non connessi tra di loro;
Cloud ibrido – soluzione tecnologica che prevede l'impiego combinato di Cloud Pubblico e Cloud Privato;
CSP – (Cloud Service Provider) un'entità (privata o pubblica) che fornisce piattaforme, infrastrutture, applicazioni, servizi di sicurezza o di archiviazione basati su cloud a un'altra entità/organizzazione solitamente a pagamento;
Disponibilità – proprietà per la quale le informazioni sono rese accessibili e utilizzabili su richiesta di un'entità autorizzata;
IaaS – (Infrastructure-as-a-Service) infrastruttura erogata in modalità di servizio. Risorse hardware virtualizzate vengono messe a disposizione, affinché l'utilizzatore possa creare e gestire, secondo le proprie esigenze, una propria infrastruttura sul cloud senza preoccuparsi di dove siano allocate le risorse;
Integrità – Proprietà per la quale l'accuratezza e la completezza degli asset è salvaguardata;
Log - Il log è un sistema di registrazione di avvenimenti significativi. I file che contengono queste annotazioni sono detti file di log e potrebbero essere identificati anche come i file delle registrazioni, per cui il log non è altro che un registro;
Responsabile del Trattamento - la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
Riservatezza – Proprietà per la quale le informazioni non sono rese disponibili o divulgate a individui, entità o processi non autorizzati;
Snapshot – Copia dello stato di una macchina virtuale in un determinato momento;
Titolare del Trattamento - la persona fisica o giuridica, l'autorità pubblica o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione Europea o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

VM (*virtual machine*)– Le macchine virtuali sono software, creati all'interno di un ambiente digitale, che offrono le stesse funzionalità dei computer fisici.

5. CONTESTO REGOLATORIO DI RIFERIMENTO

- ISO 27001:2013 – Sistemi di gestione per la sicurezza delle informazioni – Requisiti
- ISO 27017:2021 – Codice di pratica per i controlli di sicurezza delle informazioni per i servizi in cloud basati su ISO / IEC 27002
- ISO 27018:2020 – Codice di pratica per la protezione delle informazioni personali (PII) trattati in cloud pubblici in qualità di responsabili del trattamento
- Regolamento UE 679/2016 (noto come GDPR) e legislazione nazionale.

Quali normative speciali, per clienti che operano in determinati settori merceologici, si richiamano il Regolamento UE Digital Operational Resilience Act (DORA) e il Regolamento noto come "AI Act", oltre alle leggi di attuazione della Direttiva NIS2 nel cui ambito di applicazione BDP rientra.

6. POLITICA DI SICUREZZA DI GESTIONE SERVIZI CLOUD

BDP eroga servizi di cloud computing in modalità SaaS (Software-as-a-Service), un metodo per la distribuzione di applicazioni software tramite Internet, nel quale i provider di servizi cloud ospitano e gestiscono tali applicazioni software per consentire l'uso delle stesse ai propri clienti attraverso i loro dispositivi.
BDP in qualità di cliente utilizza due tipologie di infrastruttura con due diverse modalità contrattuali, che sono uno *IaaS* (Infrastructure as a service) e un *housing*, nel quale le macchine fisiche e gli apparati BDP vengono inseriti all'interno di uno spazio fisico locato dal fornitore.
I clienti finali di BDP sono persone giuridiche che utilizzano le piattaforme messe a disposizione in SaaS per gestire i loro Contact Center ad uso interno o per mettere a disposizione di aziende terze servizi di Contact Center professionali. BDP offre ai clienti finali, che quindi in base a quanto evidenziato sopra possono essere o titolari o responsabili del trattamento dei dati personali, servizi che prevedono uno scambio di informazioni tra il software BDP installato volontariamente sui pc degli operatori di Contact Center e le infrastrutture IT ad hoc con architettura cloud attraverso le quali si rende fruibile il software sviluppato da BDP.
Nell'ambito dell'erogazione e/o gestione di servizi cloud BDP prende in considerazione i requisiti di seguito descritti.

- **Gestione del Cloud**: lo spostamento di dati nel cloud richiede una definizione specifica di ruoli e responsabilità all'interno dell'organizzazione e/o nei confronti dei suoi fornitori. Per questo motivo sono definiti puntualmente i ruoli tanto relativamente all'erogazione del servizio quanto alla gestione delle relazioni con i fornitori di servizi cloud. Il personale coinvolto in tale gestione è formato sulle tecnologie cloud e su eventuali specifiche disposizioni in materia di trattamento di dati personali.
- **Virtualizzazione e separazione**: Nel cloud computing, la maggior parte dei controlli di separazione logica vengono gestiti attraverso l'utilizzo di apparati virtuali e la segmentazione e l'integrità dei dati viene garantita attraverso controlli logici. BDP opera per garantire, nell'ambiente virtuale, un livello di sicurezza della separazione dei sistemi almeno analogo a quello degli ambienti fisici.
- **Gestione delle identità digitali**: la gestione delle identità digitali è una componente essenziale per garantire la sicurezza dei dati nel cloud computing. BDP garantisce una loro corretta gestione durante tutto il ciclo di vita dei dati e durante tutta la durata dei processi e trattamenti.

- **Gestione dei Log**: BDP dispone delle necessarie informazioni relative ai log di monitoraggio e garantisce l'accesso ai soli utenti autorizzati.
- **Sicurezza delle applicazioni**: il cloud è, in genere, un ambiente aperto e questo aspetto aumenta significativamente l'esposizione agli attacchi. Per questa ragione BDP sottopone a controlli specifici le applicazioni web che si interfacciano con ambienti cloud.
- **Disaster Recovery**: sui dati conservati in Cloud, BDP effettua verifiche puntuali e predispone configurazioni specifiche al fine di garantire il loro recupero anche nel caso in cui si verifichino dei problemi.
- **Indagini informatiche**: le autorità competenti possono richiedere l'accesso ad informazioni specifiche nell'ambito di attività d'indagine. Come per i dati archiviati internamente, BDP ha delle procedure condivise con il fornitore quando i dati sono archiviati da un CSP.
- **Requisiti contrattuali**: prima di trasferire i dati a terzi BDP effettua un'analisi del fornitore CSP e verifica che le clausole contrattuali siano adeguate agli standard di riferimento e agli impegni presi verso i propri clienti finali.
- **Trattamento dei dati personali**: i ruoli e le responsabilità nell'ambito del trattamento dei dati personali conservati su cloud sono chiaramente definiti e rispettano quanto previsto dal Regolamento UE 679/2016.

Nel seguito vengono descritte le principali attività necessarie per recepire i requisiti sopra riportati.

7. GESTIONE DEL CLOUD

7.1 Ruoli e responsabilità per la sicurezza delle informazioni

Per consentire un'efficace attività di gestione dei servizi cloud BDP assicura che:

- Il personale con responsabilità dirette relativamente ai servizi su cloud sia formato sulle tecnologie cloud e sulle disposizioni in materia di trattamento di dati personali.
- Nel caso di acquisizione di servizi cloud sul mercato, sulla gestione dei fornitori sono definiti e documentati i diversi ruoli e responsabilità per il personale responsabile della gestione del servizio cloud, sono formalizzati i requisiti per assicurare il livello del servizio erogato, laddove possibile sono inoltre sottoscritti NDA a garanzia della sicurezza e riservatezza delle informazioni.
- I ruoli di riferimento sono condivisi anche con i clienti quando BDP opera in qualità di CSP. In tal caso è definito e condiviso con i clienti un processo di escalation verso il gruppo responsabile della gestione dei servizi cloud.

L'identità del Responsabile del trattamento è la seguente:
Base Digitale Platform S.p.A.
Indirizzo sede legale e operativa: Via 5 Maggio, 81 - 16147 Genova (GE)
Altre sedi operative: Corso G. Mazzini, 33 – Novara
Via Montefeltro, 6 Milano
e-mail legal.bdp@basedigitalegroup.com Telefono: +39 0103747811
Sito internet www.basedigitaleplatform.com

Il controllo della gestione in sicurezza dell'infrastruttura Cloud è assicurato da un team di tecnici specialisti composto da risorse interne all'organizzazione BDP e da fornitori esterni qualificati.
Per informazioni di dettaglio:

- Responsabile Sicurezza Cloud – C.I.S.O. a.bocerani@basedigitalegroup.com
- DPO – privacy.bdp@basedigitalegroup.com

7.2 Sede geografica di trattamento dei dati

I servizi cloud di BDP sono erogati da una infrastruttura contrattualizzata in Iaas con il fornitore REEVO S.p.A. e dalle infrastrutture in housing presso Retelit Digital Services S.p.A. a Milano Caldera e Via Perrier a Roma. I datacenter di riferimento sono certificati secondo gli standard di riferimento per i servizi cloud e sono regolarmente auditati/verificati dall'area Compliance di BDP.

Per quanto riguarda specifiche necessità di storage richieste dai clienti, BDP si avvale di AWS con alti standard di sicurezza e residenti in server farm site in UE.
Per informazioni di dettaglio:

- Responsabile Sicurezza Cloud - C.I.S.O. a.bocerani@basedigitalegroup.com

7.3 Gestione degli asset e classificazione dele informazioni

L'accesso agli asset del cliente avviene in relazione alle disposizioni contrattuali ed in conformità con le disposizioni legislative.

A tutela dei diritti degli interessati i cui dati sono oggetto del trattamento, BDP si impegna ad informare costantemente i propri clienti su politiche, pratiche e tecnologie di sicurezza e protezione dei dati applicate. Questi impegni includono:

- Accesso e proprietà: il cliente conserva il controllo dei propri contenuti e la proprietà dei dati rimane al cliente.
- Divulgazione dei contenuti dei clienti: BDP non divulga i contenuti del cliente se non richiesto dalla legislazione vigente o da ordinanze vincolanti emesse da un'autorità statale;
- Controlli di Sicurezza: BDP adotta politiche, standard e linee guida su privacy e protezione dei dati per raggiungere il più alto livello di sicurezza e protezione della confidenzialità.

7.4 Gestione accessi utente

L'accesso ai Servizi cloud da parte dell'utente avviene attraverso un processo di installazione di software specifico, registrazione e/o eventualmente di download volontaria dell'app associata al servizio.
I dati trattati sono quelli relativi ai dati identificativi degli utenti ed a seconda del servizio potrebbe essere prevista la gestione di dati personali comuni o particolari degli interessati, siano essi in transito o anche con funzione di repository.
La cancellazione delle utenze di accesso e dei dati avviene nel rispetto del GDPR e comunque secondo le modalità concordate nella definizione dell'ordine/contratto comprensivo della nomina a responsabili/sub-responsabili del trattamento.

8. VIRTUALIZZAZIONE

I controlli di separazione logica sono in parte fisici (ovvero server separati), in parte la separazione viene forzata attraverso l'utilizzo di apparati virtuali e la segmentazione e l'integrità dei dati viene garantita attraverso controlli logici. BDP opera per garantire, nell'ambiente virtuale, un livello di sicurezza della separazione dei sistemi almeno analogo a quello degli ambienti fisici.
Per consentire un'efficace protezione dei sistemi virtuali:

- in fase di valutazione del fornitore sono valutate le politiche di sicurezza adottate prestando particolare attenzione all'adozione di standard e best

practice riconosciuti. Le politiche, a titolo esemplificativo, contemplano i seguenti aspetti:

- disabilitazione (o rimozione) di tutte le interfacce, porte, servizi e dispositivi non strettamente necessari;
- configurazione con principi di sicurezza delle informazioni di tutte le interfacce di rete virtuali e le aree di archiviazione;
- limiti sull'utilizzo delle risorse della VM;
- hardening (adozione di politiche di sicurezza) di tutti i sistemi operativi e delle applicazioni in esecuzione all'interno della macchina virtuale;
- validazione dell'integrità delle operazioni di gestione delle chiavi crittografiche;

- Il CSP adotta controlli per garantire che vengano acquisiti solo gli snapshot previsti e autorizzati e che il livello di classificazione, posizione di archiviazione e crittografia che gli viene assegnato sia in linea con la sensibilità dei dati trattati
- assicura inoltre che i seguenti controlli siano applicati:
  - accesso agli access log amministrativi dell'hypervisor VMWare;
  - registrazione di tutti i log dell'hypervisor
- BDP identifica l'elenco completo dei suoi fornitori coinvolti nella gestione del cloud per l'erogazione del servizio contrattualizzato. Laddove vi siano anche dati personali (PII), BDP assicura l'adempimento di quanto previsto dalla normativa vigente sul trattamento dei dati personali. Il cliente in qualsiasi momento può acquisire informazioni sull'elenco completo dei fornitori coinvolti facendo riferimento ai contatti identificati al punto sub 7.1) del presente documento.

9. SEPARAZIONE DEGLI AMBIENTI

La separazione dei diversi sistemi logici che coesistono su una infrastruttura Cloud è una delle principali misure per garantire la riservatezza e l'integrità dei dati memorizzati oltre che la sicurezza di tutta l'infrastruttura di erogazione dei servizi.
Nel caso di servizi cloud acquisiti sul mercato, BDP garantisce la separazione logica delle reti utilizzate da tutti i suoi clienti e, inoltre, anche la separazione tra la rete di gestione dell'infrastruttura e le reti destinate all'erogazione dei servizi.
I fornitori esterni di cloud services forniscono a BDP, se richiesto, tutto il supporto necessario a verificare che tale segregazione sia garantita anche quando venissero richiesti elementi di segregazione addizionali nel rispetto delle proprie politiche.

10. GESTIONE DELLE IDENTITA' DIGITALI

La gestione delle identità digitali rispetta la normativa sulla protezione dei dati personali e i più alti standard di sicurezza.
Tale gestione può essere integrata con la soluzione centralizzata Single Sign-On (SSO); in questo caso quando un utente tenta di accedere alla nostra piattaforma software configurata con il SSO, il sistema verifica la sua identità contro il sistema di gestione dell'identità digitale Active Directory.
È anche possibile l'integrazione della gestione dell'identità digitale con meccanismi di autenticazione a più fattori (MFA) aumentando il livello di sicurezza dell'accesso.
Su richiesta del cliente vengono fornite informazioni più dettagliate a seconda della linea di prodotto alla quale occorre accedere.

11. GESTIONE DEI LOG

Quando BDP utilizza servizi di Cloud di terze parti, rispetta quanto previsto nella procedura di riferimento per i sistemi in gestione e concorda con il fornitore, laddove possibile, le caratteristiche dei log necessari.
Quando BDP opera in qualità di CSP, offre ai suoi clienti la possibilità di definire e concordare i requisiti di monitoraggio degli accessi e delle attività svolte, in particolare per quanto riguarda le operazioni che richiedono privilegi di amministratore. In questo caso le operazioni sono tracciate con l'utilizzo di una piattaforma di SIEM (Security Information and event management) come indicato nel documento *IO OPER 13 Gestione SIEM-FIM*.

12. BACKUP

BDP nella gestione dei dati in cloud assicura l'esecuzione di backup per quanto riguarda le informazioni di configurazione di ogni specifica istanza. Nel caso in cui il Cliente sia interessato a commissionare a BDP anche il backup dei dati trattati nel corso della durata contrattuale e non solo delle configurazioni della piattaforma, questo tipo di servizio viene gestito tramite apposito contratto integrativo. Il Cliente può acquisire informazioni di dettaglio sulle logiche di backup facendo riferimento ai contatti identificati al punto sub 7.1 del presente documento.
La gestione generale di backup in BDP è approfondita nella *IO OPER 05 Backup Patching Antivirus Decommissioning*.

13. SICUREZZA DELLE APPLICAZIONI

BDP ha a disposizione un team per gestire gli incidenti di sicurezza e una struttura di Compliance a supporto di tutte le aree aziendali per adottare quanto definito nelle procedure e istruzioni sullo "sviluppo sicuro" del software *PSQ RIC 01 Controllo della progettazione e sviluppo* e nella gestione dei data breach *IO OPER 12 Gestione violazione dati personali data breach*.

14. DISASTER RECOVERY

Nel caso di servizi cloud acquisiti sul mercato, i fornitori qualificati per i servizi cloud adottano dei processi di gestione delle modifiche e di risposta agli incidenti conformi alle politiche di sicurezza definite da BDP e coerenti con gli SLA contrattualizzati dei servizi erogati.

I fornitori qualificati per i servizi cloud, nello specifico ad oggi Retelit Digital Services, REEVO e AWS, inoltre, definiscono e gestiscono piani di Disaster Recovery che garantiscono il ripristino dei servizi nelle tempistiche e con il livello di servizio contrattualizzato. Il piano è richiesto che sia testato almeno una volta all'anno e, su richiesta di BDP, i fornitori devono dare evidenza del rapporto di test, di eventuali criticità emerse e delle relative azioni correttive.

15. INDAGINI INFORMATICHE

Ai clienti dei servizi cloud viene garantito il massimo supporto, nel rispetto della normativa vigente, nel caso questi avviassero delle indagini sui servizi contrattualizzati con BDP.
Nel caso di servizi cloud acquisiti sul mercato, per consentire un'efficace attività di investigazione, deve essere concordata, con il fornitore qualificato per i servizi cloud, la modalità per la richiesta di dati necessari ad indagini interne ovvero a seguito di richiesta alle autorità legali competenti.

16. REQUISITI CONTRATTUALI

L'adozione dei servizi cloud può comportare maggiori rischi rispetto all'integrità, riservatezza e disponibilità dei dati. Per questa ragione, i contratti che BDP stipula con i suoi fornitori che hanno come oggetto la fornitura di servizi cloud, devono almeno prevedere:

- che il cliente conserverà il diritto "esclusivo" alla proprietà dei dati per tutta la durata dell'accordo. La proprietà include le eventuali copie dei dati contenuti nei backup;
- l'espresso divieto per il fornitore di utilizzare i dati per finalità di marketing e/o pubblicità o qualsiasi altro scopo secondario non esplicitamente autorizzato;
- l'indicazione del paese(i) in cui i dati vengono conservati;
- che la normativa sulla protezione dei dati personali applicabile sia conforme alla normativa europea;
- il Service Level Agreement (SLA) del servizio;
- l'obbligo da parte del fornitore come CSP di informare senza ingiustificato ritardo in merito a qualsiasi violazione dei dati;
- l'obbligo per il CSP di eliminare completamente qualsiasi traccia di dati/informazioni, al termine dell'Accordo, da tutti i suoi sistemi, a meno di obblighi di legge che estendano i termini di conservazione;
- le modalità con cui il CSP potrà restituire i dati a BDP in qualità di Responsabile/Sub-responsabile del trattamento al termine dell'accordo.

I requisiti di cui sopra andranno rispettati anche nella contrattualizzazione di servizi quando BDP opera in qualità di CSP verso i suoi clienti, facendo anche riferimento al documento *Istruzioni per il trattamento dei dati personali* e alle *Condizioni di fornitura per i servizi SaaS e prestazioni di servizi*.

17. TRATTAMENTO DEI DATI PERSONALI

A tutela dei diritti degli interessati i cui dati sono oggetto del trattamento, il cliente del servizio Cloud, in qualità di Titolare o Responsabile del trattamento, provvede a nominare il CSP, quale Responsabile o Sub- Responsabile del trattamento, con un atto formale specifico o incluso nel contratto/ordine stipulato.

BDP si impegna a monitorare costantemente lo scenario in continua evoluzione di regolamenti e leggi riguardanti la protezione dei dati personali al fine di identificare i cambiamenti e determinare gli strumenti di cui i clienti potrebbero avere necessità per le esigenze di conformità, in funzione delle loro applicazioni e del settore nel quale operano.

BDP si impegna a tenere informati costantemente i propri clienti su politiche, pratiche e tecnologie di sicurezza applicate.
Questi impegni includono:

- Accesso e proprietà: il cliente conserva il pieno controllo dei propri contenuti. La proprietà dei dati rimane al cliente;
- Divulgazione dei contenuti dei clienti: BDP non divulgherà i contenuti del cliente se non richiesto dalla legislazione vigente o da ordinanze vincolanti emesse da un'autorità competente;
- Controlli di Sicurezza: BDP adotta politiche, standard e linee guida su privacy e protezione dei dati per raggiungere il più alto livello di sicurezza.

18. MODALITA' DI AGGIORNAMENTO

Eventuali modifiche ai contenuti del presente documento possono essere comunicate ai clienti attraverso il sito internet o tramite mail e/o pec
La versione aggiornata del presente documento è comunque sempre disponibile su richiesta del cliente oppure in fase di pre-vendita da parte di chi sia interessato ad acquistare i servizi in cloud di BDP.