Is7.2.M REV01 Protocollo di affidamento servizi cloud

Revisione	Data	Motivo della revisione	Visto preparazione	Visto approvazione
00	20/11/2018	Prima emissione	---	---
01	06/12/19	Modifica dei paragrafi 1.18, 1.29 e 1.36 e piccoli aggiustamenti in tutto il documento	Massimo Libretti	Luciano Doro

1. PREMESSA

L'affidamento dei dati in cloud ai sensi della ISO 27017:2015 prevede la verifica di determinati requisiti sia per il Cliente che per Boxxapps.

Boxxapps in completa trasparenza per la gestione dei servizi offerti vi fornisce in seguito un riepilogo dei vostri adempimenti anche riferiti a quelli che Boxxapps adotta come fornitore in ottemperanza alla ISO 27017: 2015.

Qualora riscontriate delle difformità rispetto a quanto sotto riportato e gli eventuali servizi offerti, vi invitiamo a segnalarcelo tramite i nostri consueti canali di comunicazione.

2. PROTOCOLLO DI AFFIDAMENTO SERVIZI CLOUD

1.1. I dati memorizzati nell'ambiente di cloud computing possono essere soggetti all'accesso e alla gestione da parte di Boxxapps; a tutela del Cliente, Boxxapps adotta l'applicazione di metodi e processi certificati da terzi in ambito ISO 27001, ISO 27018 e ISO 27017;

1.2. Per fruire del servizio del servizio cloud, ricordiamo che devono essere ben definiti gli utenti. A tal fine, Boxxapps adotta 2 diversi profili:

- Utenti del Cliente con profilo amministratori del servizio cloud che hanno accesso privilegiato;
- Utenti con un profilo User, che possono eseguire operazioni limitate.

1.3. Boxxapps ha un'adeguata allocazione dei ruoli e delle responsabilità in materia di sicurezza delle informazioni e conferma che è nelle condizioni di adempiere ai propri ruoli e responsabilità in materia di sicurezza dei dati. A tal fine, sono condotte periodiche rivalutazioni dell'analisi dei rischi, vulnerability assestmet e penetration test. Il Cliente che ritiene di modificare e/o integrare le prassi di controllo di Boxxapps è tenuto a definire tali aspetti preventivamente, in uno specifico accordo tra le parti.

1.4. Boxxapps ha identificato nel Garante della Privacy, Agid e nella Polizia Postale le Autorità rilevanti per la protezione dei dati. Qualora il Cliente ritiene di modificare e/o integrare tali organismi, è tenuto a definire tali aspetti preventivamente, in uno specifico accordo tra le parti.

1.5. Si ricorda che il Cliente è tenuto ad aggiungere ai propri programmi di formazione i seguenti elementi di sensibilizzazione, istruzione per:

- I responsabili,
- Gli amministratori,

- Gli integratori di servizi cloud
- Gli utenti del servizio cloud, inclusi i dipendenti e gli appaltatori interessati.

La consapevolezza della sicurezza delle informazioni, i programmi di istruzione e formazione sui servizi cloud dovrebbero essere forniti alla direzione e ai responsabili della supervisione, compresi quelli delle unità operative.

Questi sforzi supportano un efficace coordinamento delle attività di sicurezza delle informazioni in ambiti quali:

- Standard e procedure per l'utilizzo dei servizi cloud;
- Rischi per la sicurezza delle informazioni relativi ai servizi cloud e come tali rischi sono gestiti;
- Rischi per l'ambiente di rete e di sistema con l'uso di servizi cloud;
- considerazioni legali e normative applicabili.

1.6. L'inventario delle proprie risorse che effettua periodicamente Boxxapps tiene conto delle informazioni e delle risorse associate e archiviate nell'ambiente di cloud computing. I registri dell'inventario indicano dove vengono mantenute le risorse.

1.7. Boxxapps colloca i dati dei Clienti sempre e solo su server all'interno dell'Unione Europea;

1.8. Ogni informazione dislocata nel cloud di Boxxapps è identificata ed etichettata. Una apposita procedura interna ne garantisce l'applicazione. Boxxapps rimane a completa disposizione del Cliente sia per fornirgli il registro del trattamento per i servizi in essere come responsabile sia per dargli indicazioni circa la procedura di classificazione delle informazioni che attua.

1.9. La politica di controllo dell'accesso in cloud al servizio cha adotta Boxxapps prevede la compartimentazione per ciascun servizio cloud.

1.10. Si ricorda che il Cliente deve sempre utilizzare tecniche di autenticazione sufficienti per autenticare i suoi utenti con profilo amministratore (ma anche user); a tale scopo, opportune policy adottate di Boxxapps impediscono di usare credenziali deboli o inadatte allo scopo.

1.11. Si invita il Cliente a verificare che la procedura di gestione di Boxxapps per l'allocazione delle informazioni di autenticazione segreta, come le password, soddisfi i propri requisiti.

1.12. Si invita il Cliente a verificare e garantire che l'accesso alle informazioni nel servizio cloud possa essere limitato in conformità con la sua politica di controllo degli accessi e che tali restrizioni siano realizzate. Ciò include:

- La limitazione dell'accesso ai servizi cloud;
- Alle funzioni del servizio cloud;
- Ai dati dei clienti gestiti dal servizio cloud.

1.13. Laddove l'utilizzo di programmi di utilità è consentito, il Cliente deve identificare i programmi di utilità da utilizzare nel proprio ambiente e assicurarsi che non interferiscano con i controlli del servizio cloud.

1.14. Per l'utilizzo dei servizi cloud, il Cliente, se giustificato dalla propria analisi del rischio, deve implementare controlli crittografici. I controlli devono essere sufficienti a mitigare i rischi identificati, indipendentemente dal fatto che tali controlli siano forniti da Boxxapps.

Boxxapps adotta una specifica procedura scritta per il controllo e la manutenzione dell'efficacia delle chiavi crittografiche per ciascuna fase del ciclo di vita, ossia: la generazione, la modifica o l'aggiornamento, la memorizzazione, il ritiro, il recupero, il mantenimento e la distruzione.

Normalmente Boxxapps applica i controlli crittografici su tutte le transazioni da/per il Cliente, con standard di protezione in linea con il mercato, con valutazione periodica dello stato del certificato utilizzato.

Quando Boxxapps offre la crittografia, il Cliente deve esaminare tutte le informazioni fornite da Boxxapps per confermare se le funzionalità di crittografia:

- soddisfano i suoi requisiti di politica;
- sono compatibili con qualsiasi altra protezione crittografica già utilizzata;
- sono applicate ai dati a riposo e in transito e all'interno del servizio.

Si ricorda che il Cliente non dovrebbe consentire a Boxxapps di archiviare e gestire le chiavi di crittografia per operazioni crittografiche quando il Cliente impiega la propria gestione delle chiavi o un servizio di gestione delle chiavi separato e distinto.

1.15. Boxxapps ha specifiche politiche e procedure scritte per lo smaltimento sicuro o il riutilizzo delle risorse. Se richiesto, Boxxapps fornirà tali documenti.

1.16. Il processo di gestione del servizio in cloud offerto al Cliente deve tenere conto del profilo di accesso al servizio fornito da Boxxapps. A tale fine, Boxxapps informa il Cliente sulle modalità di accesso standard, durante l'attivazione del servizio.

1.17. Il Cliente deve assicurarsi che la capacità di erogazione del servizio concordata con Boxxapps venga soddisfatta. Il Cliente deve monitorare l'utilizzo dei servizi e prevedere le proprie esigenze di capacità richiesta, al fine di garantire le prestazioni dei servizi cloud che gli necessitano nel tempo. Boxxapps si rendere disponibile a mettere a disposizione adeguati strumenti (Control Room) per facilitare al Cliente questa attività.

1.18. Laddove Boxxapps fornisca funzionalità di backup come parte del servizio cloud, il Cliente deve:

- richiedere le specifiche sulle modalità di esecuzione del backup da Boxxapps (RPO, retentions, ecc.);
- verificare che le specifiche di backup indicate da Boxxapps siano compatibili con le proprie necessità di conservazione;

Boxxapps adotta sistemi di disaster recovery in ottica UNI EN ISO 22301, sia per la parte dei dati e/o informazioni, sia per la parte di software, che per i sistemi, con verifica dei dati backuppati e con periodici test di ripristino. I backup sono crittografati, con accesso limitato e regolamentato da procedure interne, e l'accesso è limitato a personale di Boxxapps specifico.

Quando non è Boxxapps a fornire il servizio di backup (ovvero quando non esiste uno specifico contratto a tal proposito), il Cliente deve essere responsabile dell'implementazione, mantenimento e verifica delle necessarie funzionalità di backup.

1.19. Boxxapps implementa un set di log standard che consentono di monitorare una serie di eventi. Ciò non toglie che il Cliente è tenuto a verificare se tale set di log è sufficiente e in linea con le proprie politiche; diversamente, deve definite con Boxxapps i requisiti per la registrazione degli eventi e verificare che il servizio cloud soddisfi tali requisiti.

1.20. Se le operazioni di amministrazione informatica sono delegate al Cliente, è necessario registrare l'operazione e le prestazioni di tali operazioni. Quando questo servizio è erogato da Boxxapps, il Cliente deve determinare se le funzionalità di registrazione fornite dal Boxxapps sono appropriate.

1.21. Boxxapps adotta una policy di sincronizzazione di tutti gli orologi aziendali, e ne verifica periodicamente l'applicazione, in modo da garantire che ogni ambiente sia sincronizzato. Su richiesta, Boxxapps può fornire informazioni al Cliente sulla policy di sincronizzazione dell'orologio utilizzata per i servizi cloud.

1.22. Il Cliente deve richiedere informazioni a Boxxapps sulla gestione delle vulnerabilità tecniche che possono influenzare i servizi forniti. In ogni caso, in tale ambito Boxxapps adotta una propria politica di vulnerability assessment e di penetration test; su esplicita richiesta del Cliente, Boxxapps è in grado di fornire documentazione a riguardo, nei limiti dell'interesse del Cliente.

1.23. Ricordiamo che il Cliente deve identificare le vulnerabilità tecniche di cui sarà responsabile e dovrà definire chiaramente un processo per gestirle.

1.24. Boxxapps adotta una politica di separazione delle reti per ottenere l'isolamento nell'ambiente condiviso per il servizio cloud. Su esplicita richiesta del Cliente, Boxxapps è in grado di fornire documentazione a riguardo, , nei limiti dell'interesse del Cliente.

1.25. Il Cliente deve determinare i requisiti di sicurezza delle informazioni e quindi valutare se i servizi offerti da Boxxapps soddisfino tali requisiti. Per questa valutazione, il Cliente può sempre richiedere a Boxxapps informazioni sulle funzionalità di sicurezza delle informazioni adottate.

1.26. Boxxapps effettua le operazioni di sviluppo in ambiente sicuro e dedicato, con dati di prova non reali o adeguatamente anonimizzati. Le operazioni di sviluppo sono governate da specifiche procedure scritte. Su esplicita richiesta del Cliente, Boxxapps è in grado di fornire documentazione a riguardo, nei limiti dell'interesse del Cliente.

1.27. Il Cliente deve includere Boxxapps nella sua politica di sicurezza delle informazioni, nelle relazioni con i fornitori. Ciò contribuirà a mitigare i rischi associati all'accesso e alla gestione dei dati gestiti nei servizi offerti da Boxxapps.

1.28. Il Cliente deve confermare i ruoli e le responsabilità in materia di sicurezza delle informazioni relative al servizio cloud, descritti nel contratto di servizio. Questi possono includere, a seconda dei servizi offerti, i seguenti processi:

- protezione da malware;
- backup;
- controlli crittografici;
- gestione della vulnerabilità;

- gestione degli incidenti;
- controllo della conformità tecnica;
- test di sicurezza;
- auditing;
- raccolta, manutenzione e protezione delle prove, compresi i registri e le liste di controllo;
- protezione delle informazioni al termine del contratto di servizio;
- autenticazione e controllo degli accessi;
- identità e gestione degli accessi.

1.29. Boxxapps ha una specifica procedura scritta per la gestione degli incidenti di sicurezza delle informazioni. Il Cliente deve verificare se l'assegnazione delle responsabilità per la gestione degli incidenti di sicurezza delle informazioni sono adeguate e deve assicurarsi che soddisfino i propri requisiti.

In caso di incidente che coinvolga la perdita di una o più caratteristiche tra Riservatezza, Integrità, Disponibilità, Autenticità riguardanti informazioni personali (Data Protection), è compito della Parte che identifica l'incidente dare immediata informazione all'altra Parte. Ove necessario, entro un tempo massimo di 48 ore, deve essere deciso di comune accordo quale delle due Parti debba aprire il Data Breach, ed inviare entro un massimo di 72 ore la comunicazione al Garante della Privacy, così come previsto dal Regolamento UE 2016/679 – GDPR.

1.30. Il Cliente deve richiedere informazioni a Boxxapps riguardo ai meccanismi per:

- segnalare a Boxxapps un evento di sicurezza delle informazioni che ha rilevato;
- ricevere segnalazioni riguardanti un evento di sicurezza delle informazioni rilevato da Boxxapps;
- tenere traccia dello stato di un evento di sicurezza delle informazioni segnalato.

1.31. Il Cliente deve considerare che Leggi e Regolamenti pertinenti possono essere quelli delle giurisdizioni che regolano Boxxapps, oltre a quelli che regolano lui stesso. Il Cliente deve richiedere evidenza della conformità di Boxxapps con le normative e gli standard pertinenti richiesti per le sue attività. Tali prove possono essere le certificazioni prodotte dagli auditor di terze parti in a ambito ISO o modelli di gestione quali il 231.

1.32. Si ricorda che l'installazione di software con licenza commerciale in un servizio cloud può causare una violazione dei termini della licenza per il software. Il Cliente deve avere una procedura per identificare i requisiti di licenza specifici per il cloud prima di consentire a Boxxapps l'installazione di qualsiasi software con licenza. Un'attenzione particolare deve essere rivolta ai casi in cui il servizio cloud è elastico e scalabile e il software può essere eseguito su più sistemi o core del processore rispetto a quanto concordato.

1.33. Si ricorda che il Cliente deve richiedere informazioni a Boxxapps sulla protezione dei record raccolti e archiviati da Boxxapps rilevanti per l'utilizzo dei servizi. Boxxapps si impegna a fornire tali informazioni, nei limiti dell'interesse del Cliente.

1.34. Si ricorda che il Cliente deve richiedere prove documentate che l'implementazione dei controlli di sicurezza delle informazioni e linee guida per il servizio cloud sia in linea con quanto definito in sede contrattuale. Tali prove devono includere certificazioni rispetto agli standard pertinenti. A tal proposito, Boxxapps è in possesso di varie certificazioni del proprio sistema; per maggiori dettagli, si veda il sito www.boxxapps.com

1.35. Si ricorda che il Cliente deve definire o estendere le sue politiche e procedure esistenti in conformità con il suo uso dei servizi cloud e rendere gli utenti del servizio consapevoli dei loro ruoli e responsabilità nell'uso del servizio cloud.

1.36. Si ricorda che il Cliente può richiedere a Boxxapps una descrizione documentata del processo di cessazione del servizio che copra il reso e la rimozione delle risorse del Cliente seguita dalla cancellazione di tutte le copie di tali risorse dai sistemi di Boxxapps. La riconsegna dei dati avverrà in modo sicuro, attraverso canali protetti. Avvenuta la restituzione, i dati “in linea” del CLIENTE saranno immediatamente eliminati, attraverso metodi di cancellazione sicura. Quando è attivo un servizio di backup (si veda punto 1.18), il Cliente deve essere consapevole della complicazione delle operazioni necessarie all'eliminazione definitiva dei dati del Cliente dai backup di Boxxapps, e pertanto accetta che questi rimangano nei backup di Boxxapps al più e non oltre 12 mesi. Qualora il Cliente richieda comunque di procedere all'eliminazione definitiva immediata dei dati dai backup, invierà una richiesta formale, adeguatamente motivata e giustificata.

1.37. Quando si configurano macchine virtuali, Boxxapps adotta un proprio template standard, gestito con logiche di hardening (ad esempio solo porte e protocolli dei servizi necessari), adottando misure tecniche appropriate (ad esempio, anti-malware, logging, etc.). Il Cliente, deve verificare e garantire che tali aspetti siano appropriati per ogni macchina virtuale utilizzata.

1.38. Si ricorda che il Cliente deve documentare le procedure per operazioni critiche in cui un errore può causare danni irreversibili alle risorse nell'ambiente di cloud computing. Esempi di operazioni critiche sono:

- installazione, modifica e cancellazione di dispositivi virtualizzati come server, reti e storage;
- procedure di terminazione per l'utilizzo del servizio cloud;
- backup e ripristino.

Il documento deve specificare che un supervisore dovrebbe monitorare queste operazioni.

Marcon, lì 06/12/2019

BOXXAPPS S.r.l.
Doro Luciano