Servizio email SaaS erogato dal TIX di Regione Toscana

REVISIONI DEL DOCUMENTO					
Revisione	**Data**	**Elenco Modifiche**	**Compilato**	**Approvato**	**Validato**
1.0	2019-06-11	Prima versione	C. Gallotti	A. Tarchi (RT)	A. Tarchi (RT)

INDICE

1 Scopo

Questo documento illustra le caratteristiche del servizio di posta elettronica (Mailbox-as-a-Service) offerto da Regione Toscana.

I servizi rispettano la normativa vigente e in particolare:

- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati;
- Decreto Legislativo 196 del 2003 e successive modificazioni;
- Legge 547 del 1993 (computer crime);
- D.Lgs. 82 del 2005, "Codice dell'Amministrazione Digitale" o CAD, e successive modificazioni.

L'ente affida a Regione Toscana, in relazione ai servizi in oggetto, il trattamento di dati personali per la finalità di ricevere i servizi stessi. L'ente stabilisce quali dati trattare nell'ambito dei servizi offerti e pertanto stabilisce autonomamente le categorie di persone interessate al trattamento. A titolo esemplificativo sono:

- Dati del personale e dei collaboratori;
- Cittadini.

I tipi di dati trattati sono Personali, eventualmente anche appartenenti a particolari categorie (es. sensibili o giudiziari) e anche relativi a operazioni particolari come geolocalizzazione e profilazione.

2 Responsabilità

Regione Toscana eroga il servizio di IaaS e PaaS in qualità di:

- titolare del trattamento dei dati personali per le istanze assegnate a Regione Toscana stessa;
- responsabile del trattamento dei dati personali per le istanza assegnate ad altri enti.

Regione Toscana si avvale di fornitori per la gestione dell'infrastruttura informatica e della piattaforma applicativa ("Gestore del TIX") individuato a sua volta come:

1. Responsabile del trattamento dei dati personali per le istanze assegnate a Regione Toscana stessa;
2. Sub-responsabile del trattamento dei dati personali per le istanze assegnate ad altri enti.

È responsabilità di Regione Toscana (e del Gestore del TIX):

- assistere gli enti nel fornire le caratteristiche dei servizi;
- informare gli enti (se responsabile o sub-responsabile del trattamento) e gli interessati e le autorità (se titolare del trattamento) in caso di incidenti e violazioni sui dati personali e assistere gli enti nelle indagini, permettendo anche l'accesso ai log pertinenti;
- mantenere i sistemi e la rete utilizzati per l'erogazione del servizio ad un livello di disponibilità

e di sicurezza adeguati alle esigenze della PAL;

- mantenere le applicazioni assicurando un elevato livello di sicurezza;
- assicurare le adeguate prestazioni del servizio;
- segregare l'ambiente dell'email dagli altri servizi erogati.

È responsabilità dell'ente, in qualità di titolare del trattamento, seguire le pratiche di sicurezza allo stato dell'arte. Tra di esse, a titolo di esempio, ci sono:

- creare password non facili da indovinare: evitare di utilizzare informazioni personali, di inserire parole semplici o frasi come "password" o serie di tasti come "qwerty" o "qazwsx" o sequenze come "abcd1234";
- non lasciare appunti scritti con le password su computer o scrivania;
- cambiare la password ogni volta che vi è il sospetto che qualcuno possa esserne venuto a conoscenza;
- proteggere gli smartphone attivando le funzioni di blocco tramite password, PIN (numerico), disegni o impronta digitale;
- utilizzare software ufficiali e mantenuti;
- mantenere aggiornati i dispositivi;
- resettare i dispositivi quando da dismettere;
- utilizzare software antivirus e personal firewall non solo per attacchi via email;
- quando usato un computer non esclusivo, ricordare di non salvare password e di effettuare il logout ed utilizzare le funzionalità del browser per cancellare dati, password, cache e cookie.
- richiedere subito la sospensione se si sospetta una violazione.

Regione Toscana (e il Gestore del TIX) non assicurano l'attivazione di un servizio di Disaster recovery per il servizio email se non su richiesta esplicita dell'ente.

2.1 Diritto di audit

L'ente ha facoltà di vigilare, anche tramite verifiche periodiche (previa comunicazione scritta fornita con ragionevole anticipo), sulla puntuale osservanza dei compiti e delle istruzioni qui impartite a Regione Toscana.

A sua volta, Regione Toscana assicura che svolgerà periodicamente, e almeno una volta all'anno, una verifica delle proprie misure di sicurezza adottate per controllare i rischi di accesso non autorizzato, divulgazione, mancanza di integrità e indisponibilità dei dati, sia accidentali sia illegali.

2.2 Diritti degli interessati

In qualità di responsabile del trattamento, Regione Toscana garantisce il supporto, attraverso il Service desk, agli enti per il rispetto dei diritti degli interessati.

Regione Toscana, attraverso i suoi fornitori, garantisce tempi di risposta utili affinché l'ente possa rispondere agli interessati nei tempi previsti dalla normativa vigente.

2.3 Comunicazione dei dati

Le richieste di comunicare dati devono venire direttamente dall'ente, dai referenti specificati in fase di accordo o di suoi aggiornamenti. Ogni richiesta pervenuta da altri canali sarà scartata.

Regione Toscana potrebbe ricevere richieste dalle Forze dell'ordine o dalla magistratura. In questi casi ~~ha~~ attiva una procedura per la loro gestione. Se non richiesto direttamente dalle Forze dell'ordine o dalla magistratura, Regione Toscana informa il prima possibile l'ente della richiesta.

2.4 Uso di sub-fornitori

L'ente autorizza Regione Toscana ad affidare, sotto la propria responsabilità, l'esecuzione di operazioni di trattamento a soggetti terzi (c.d. sub-fornitori), che non siano situati in Paesi Extra-UE.

Fanno eccezione i trasferimenti a sub-fornitori che abbiano adottato le seguenti misure esplicitamente previste dalla normativa applicabili:

- una dichiarazione di adeguatezza del Paese di provenienza, confermata dalla pubblicazione sul sito della Commissione europea;
- BCR (o Binding Corporate Rules o norme vincolanti d'impresa) confermate dalla pubblicazione sul sito della Commissione europea;
- contratto con il sub-fornitore basato sulle clausole tipo di protezione dei dati.

Il ricorso a sub-fornitori è condizionato alla sottoscrizione di un contratto tra Regione Toscana e il sub-fornitore che includa i medesimi (o più stringenti) requisiti del presente contratto.

L'ente si riserva il diritto di chiedere in ogni momento a Regione Toscana l'elenco dei suoi sub-fornitori che possono avere accesso (in virtù del contratto di sub-fornitura) ai dati personali dell'ente.

3 Caratteristiche di base

Il servizio di email è erogato dal Data center TIX. Esso è rivolto a tutti gli Enti aderenti (Regione Toscana, SST, comuni, ecc.) ed è erogato secondo il paradigma SaaS.

Il servizio è contabilizzato "a consumo" su base casella di posta elettronica.

4 Caratteristiche tecniche

Il servizio è erogato con minime interruzioni programmate, anche per eventuali attività di migrazioni trasparenti per l'utenza.

Il servizio si basa sull'ultima versione stabile disponibile di Zimbra Collaboration.

4.1 Classificazione

Gli utenti possono classificare le email creando automaticamente le etichette per la propria mailbox.

4.2 Gestione utenze e autorizzazioni

Il cliente ha a disposizione un portale di amministrazione. Per accedervi è necessario fare uso della CNS (applicazione di multi-factor authentication).

Per l'accesso al servizio email, gli utenti usano user-id e password (in futuro potrebbe essere introdotto l'uso di OTP).

L'accesso via webmail e piattaforma amministrativa (login con CNS) avviene su canali cifrati HTTPS. Per l'utilizzo dei client di posta, sono disponibili i protocolli POPs, SMTPs e IMAPs cifrati.

4.3 Backup

Le caselle di email sono oggetto di backup secondo le seguenti regole:

- frequenza giornaliera~~;~~
- conservazione almeno di 30 giorni.

Le macchine virtuali che erogano il servizio sono sottoposte a backup giornaliero con tecnologia "ifincremental" che garantisce il recupero della vm con una singola operazione di ripristino. La retention è di 15 giorni.

I log sono salvati come da termini di legge.

4.4 Monitoraggio

Gli enti aderenti possono monitorare il servizio attraverso:

- Allarmi se ci sono troppi tentativi di accesso non autorizzato;
- Allarmi superamento quote;
- Andamento SLA su richiesta.

Il gestore del TIX, a sua volta, dispone di numerosi strumenti di monitoraggio. Nel caso siano attivati degli allarmi, il gestore del TIX avverte il cliente. Per esempio nei casi di:

- troppi tentativi di accesso non autorizzato;
- superamento quote;
- Virus, intrusioni rilevate via IDS.

Per quanto riguarda i log, sono raccolti con strumenti di log collecting. In questo modo, essi sono anche protetti dal controllo degli accessi impostato per questi stessi strumenti.

L'uso di strumenti di log collecting ~~e di un SIEM~~ assicurano il riesame costante e automatico degli eventi.

Riesami manuali sono svolti solo in caso di eventi particolari.

4.5 Clock di sistema

L'NTP è erogato da due server presso il TIX, a loro volta sincronizzati con un pool di server riconosciuto come affidabile a livello di comunità Internet. Il controllo di affidabilità è effettuato ad ogni sincronizzazione. I sistemi presso il TIX, per assicurare il livello di sicurezza, non si possono collegare autonomamente ad NTP server esterni.

4.6 Chiusura del servizio

Alla chiusura del servizio, la casella di posta viene prima disabilitata e successivamente cancellata.

Copie dei dati sono mantenute nei backup fino alla conclusione della loro rotazione.

I log sono mantenuti come da termini di legge.

5 I livelli di servizio

Indicatori di qualità operativi sono i seguenti:

a. IQ10 – Disponibilità dei Servizi: il valore soglia, con cadenza trimestrale, è definito in modo distinto per i servizi di produzione e per quelli di staging:
   i. valore soglia di IQ10_SP (servizi di produzione) = 99,90%
   ii. valore soglia di IQ10_SS (servizi di staging) = 99,70%
b. IQ11 – Disponibilità dei Sistemi (con cadenza trimestrale)
c. IQ12 - Tempestività di risoluzione degli incident: le priorità (con cadenza trimestrale) sono così definite:
   i. Servizio di Produzione
      - Priorità 1: guasto bloccante 3 ore in orario di lavoro O3 (quindi equivalenti a solari)
      - Priorità 2: guasto non bloccante 8 ore in orario di lavoro O3 (quindi equivalenti a solari)
   ii. Servizio di Staging
      - Priorità 3: guasto bloccante 6 ore in O2
      - Priorità 4: guasto non bloccante 22 ore in O2
d. IQ13 - Tempestività di esecuzione (con cadenza trimestrale) dei change standard/predefiniti, le classi sono così ri-definite:
   i. classe 1 – tempo massimo di esecuzione 1 h
   ii. classe 2 – tempo massimo di esecuzione 2 h
   iii. classe 3 – tempo massimo di esecuzione 4 h
   iv. classe 4 – tempo massimo di esecuzione 8 h
   v. classe 5 – tempo massimo di esecuzione 16 h
e. IQ14 - Tempestività di esecuzione dei change non standard
f. IQ15 – Ticket oggetto di ripianificazione
g. IQ16 - Attività eseguite correttamente.

6 Help desk

È fornito dal presidio un servizio di Helpdesk, con obiettivi elencati nel paragrafo precedente.

L'Helpdesk risponde a:

- Numero verde 800.155.715;
- email operation@tix.it;
- ticket aperti dai referenti del servizio dal portale www.tix.it;
- ticket aperti dagli utenti finali sul portale support.ente.it (personalizzato per ciascun ente).

L'Helpdesk riceve segnalazioni di eventi, richieste di servizio, richieste di chiarimenti.

Per ogni comunicazione è aperto un ticket gestito con uno strumento apposito e con workflow di trattamento impostato basandosi sulle pratiche ITIL.

7 Gestione degli incidenti

Sono incidenti di sicurezza informatica: uno o più eventi di sicurezza informatica, non voluti o non

attesi, che hanno una probabilità significativa di compromettere le informazioni e minacciare la riservatezza, integrità e disponibilità delle informazioni sui sistemi informatici.

Esempi di incidenti relativi alla sicurezza informatica sono:

- rottura o furto o danneggiamento di componenti infrastrutturali;
- errori umani;
- accessi informatici non autorizzati;
- eventi che portano alla indisponibilità dei sistemi informatici del TIX.

7.1 Segnalazione di incidente

Ogni evento, incidente o vulnerabilità riscontrati devono essere comunicati alle opportune strutture in modo da garantirne un rapido trattamento. I clienti devono comunicare gli incidenti all'help desk.

7.2 Trattamento degli incidenti di sicurezza informatica

Per ogni attività, il NOC del gestore segue le proprie procedure.

Se l'incidente comporta interruzioni di servizio prolungate o può portare alla diffusione o alterazione di dati critici (es. dati personali o dati economici), il Direttore di Esecuzione (o suo Assistente o delegato) del servizio pertinente lo comunicano al RUP, ai responsabili delle applicazioni e agli enti aderenti al servizio.

Ogni incidente è oggetto di approfondite analisi per verificare quali dati sono stati compromessi, in particolare i dati personali.

7.3 Rapporto sugli incidenti di sicurezza

In caso di incidenti di sicurezza, è predisposto un rapporto con indicato:

- descrizione dell'evento;
- data di occorrenza e data di segnalazione;
- le azioni eseguite;
- gli elementi che hanno consentito di considerare l'evento risolto;
- data di chiusura della segnalazione.

7.4 Comunicazioni relative a violazioni di dati personali (data breach)

In caso di incidenti con impatto sui dati personali (in particolare se l'incidente ha permesso a persone non autorizzate ad accedere ai dati personali) il Gestore del TIX li comunica al Direttore di esecuzione.

Il Gestore del TIX e il Direttore di esecuzione valuta se la violazione dei dati personali presenta un rischio per i diritti e le libertà delle persone fisiche.

Se l'incidente presenta un rischio per i diritti e le libertà delle persone fisiche, Direttore di esecuzione, in accordo con il RPU, inoltra segnalazione a:

- il Garante per la protezione dei dati personali entro 72 ore dalla rilevazione dell'incidente (se Regione Toscana è titolare del trattamento);
- gli enti titolari dei dati coinvolti dall'incidente entro 24 ore.

La segnalazione riporta:

a) l'evento;
b) la natura della violazione dei dati personali compresi le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
c) il nome e i dati di contatto di Regione Toscana;
d) le probabili conseguenze della violazione dei dati personali;
e) le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi (quest'ultimo punto può essere incluso in una versione successiva del rapporto).

Se Regione Toscana è titolare del trattamento, la medesima segnalazione è inviata agli interessati (è possibile escludere il numero e le categorie degli interessati e il numero di registrazioni). Tale comunicazione agli interessati non è necessaria se:

- i dati sono incomprensibili ad altri (per esempio sono cifrati);
- Regione Toscana ha attuato azioni per ridurre al minimo gli impatti sugli interessati.

7.5 Raccolta di prove

Nel caso sia ritenuto opportuno, potranno essere raccolte opportune prove per perseguire i responsabili dell'evento. In questo caso, è contattato l'Ufficio Legale di Regione Toscana per seguirne le istruzioni se non diversamente specificato dalle autorità competenti.

Gli enti aderenti possono sempre richiedere di raccogliere prove. In questo caso, prima di avviare le attività, dovrà essere contattato l'Ufficio Legale di Regione Toscana. I tecnici di Regione Toscana e del gestore del TIX dovranno collaborare al fine di non compromettere i servizi attivi (in caso di raccolte date "live") e i dati riservati, sia in caso di raccolte date live sia su supporti inattivi.

7.6 Caso specifico di compromissione di credenziali

In caso di compromissione di credenziali, le azioni vanno stabilite dall'ente. Il gestore del TIX, per quanto nelle sue mansioni, può fornire gli strumenti per condurre indagini e per re-inizializzare le credenziali assegnate.

8 Componenti Fisiche

Le componenti fisiche del servizio sono localizzate in:

- sito primario, situato presso la struttura del TIX, via San Piero a Quaracchi 250, Firenze;
- sito secondario, avente almeno le stesse caratteristiche di sicurezza di quello primario ed utilizzato per erogare il servizio di Disaster Recovery (DR), presso il data centre di Cesano Maderno (MB) di Telecom Italia.