

Autore	Ufficio Privacy (Zucchetti Spa)/Responsabile sviluppo
Approvazione	Direzione

Versione Revisione

Versione	Autore	Consultazione DPO	Data emissione	Motivo della revisione
0.0	Ufficio Privacy (Zucchetti Spa)/Responsabile sviluppo	24/05/2018	25/05/2018	Prima emissione
1.0	Ufficio Privacy (Zucchetti Spa)/Responsabile sviluppo	18/06/2019	19/06/2019	Inserito versioning; modificata finalità del trattamento
2.0	Ufficio Privacy (Zucchetti Spa)/Responsabile sviluppo	07/10/2019	07/10/2019	Descrizione nuove funzioni di sicurezza
3.0	Ufficio Privacy (Zucchetti Spa)/Responsabile sviluppo	13/12/2019	13/12/2019	Inserite procedure di assistenza
4.0	Ufficio Privacy (Zucchetti Spa)/Responsabile sviluppo	05/11/2021	10/11/2021	Inserito riferimento alla funzionalità relativa alla validazione del Green Pass
5.0	Ufficio Privacy (Zucchetti Spa)/Responsabile sviluppo	13/01/2022	13/01/2022	Inserimento tempi di cancellazione log
6.0	Ufficio Privacy (Zucchetti Spa)/Responsabile sviluppo	20/01/2022	21/01/2022	Inserimento dettagli relativi XPOINT e FM
7.0	Ufficio Privacy (Zucchetti Spa)/Responsabile sviluppo	29/02/2024	29/02/2024	Aggiornate misure di assistenza e di sicurezza Data Center
8.0	Ufficio Privacy (Zucchetti Spa)/Responsabile sviluppo	10/12/2025	10/12/2025	Inseriti dettagli relativi al riconoscimento facciale

PARERE DPO OK.

I SERVIZI E PRODOTTI ZUCCHETTI IN RELAZIONE ALLE PRESCRIZIONI DEL GDPR: XATLAS (*a partire dalla versione 1.9.20*)

RESPONSABILE DEL TRATTAMENTO					
Denominazione	Zucchetti Axess S.p.a.				
Partita Iva	03537610960				
Indirizzo	Via Solferino,1				
Città	Lodi	Cap	26900	PV	LO
Legale Rappresentante	Domenico Uggeri				
STRUTTURA ORGANIZZATIVA					
Divisione	XATLAS	Responsabile Divisione	Domenico Uggeri		
Area	XATLAS	Responsabile Reparto	Marco Marchetti		
INCARICATI DEL TRATTAMENTO					
Addetti analisi, sviluppo, controllo qualità, help desk.					
DATI DI CONTATTO					
Responsabile del trattamento	Zucchetti Axess Spa	Ufficio.privacy@zucchetti.it	0371.5947000		
Rappresentante del Responsabile	N/A				
Responsabile protezione dati (DPO)	Mario Brocca	dpo@zucchetti.it	0371.5943191		
DESCRIZIONE					
<p>XATLAS è una piattaforma di security management per la gestione del controllo accessi, della sicurezza delle persone fisiche, della raccolta dati di rilevazione presenze, anti-intrusione, antincendio interfacciandosi con centrali antincendio, videosorveglianza interfacciandosi con telecamere tramite ip o con milestone e passa le informazioni ad altre applicazioni per la gestione dei pasti nelle mense aziendali.</p> <p>All'interno di XATLAS è possibile attivare una specifica funzionalità relativa alla validazione del green pass, che viene effettuata attraverso una soluzione sviluppata direttamente da Zucchetti Axess.</p> <p>Non viene salvato alcun dato, se non il QR CODE per il tempo strettamente necessario alla verifica stessa finalizzata ad autorizzare l'accesso al varco.</p> <p>Tramite XAtlas è possibile il riconoscimento delle persone fisiche anche mediante biometria facciale per l'accesso ad aree sensibili.</p>					
FINALITA' DEL TRATTAMENTO					
Gestione del controllo accessi, sia di mezzi sia di persone fisiche; gestione della sicurezza di persone e cose. La finalità del trattamento è quella di erogare i servizi di assistenza e manutenzione al Titolare.					

CATEGORIA INTERESSATI
Dipendenti, collaboratori, visitatori, veicoli delle anagrafiche di Xatlas.
CATEGORIE DI DATI PERSONALI
<p><u>Dati personali</u>: dati anagrafici, accessi a varchi e transiti di persone e automezzi.</p> <p><u>Categorie particolari di dati personali</u>: non vengono trattati dati personali che presentano rischi specifici. Esistono campi liberi in cui il Titolare del trattamento può inserire dati personali contestuali rispetto alla finalità applicativa di cui noi non conosciamo i contenuti.</p> <p>Il SW può lavorare interfacciandosi con sistemi hw di biometria.</p> <p>XAtlas può essere venduto in cloud (da approfondire le modalità di vendita)</p>
CATEGORIA DI DESTINATARI A CUI I DATI POTRANNO ESSERE COMUNICATI
Subappaltatori/subfornitori, qualora la comunicazione sia necessaria per adempiere a quanto contrattualmente previsto per finalità di assistenza e manutenzione applicativa.
TRASFERIMENTO DATI ALL'ESTERO
Non è previsto, da parte del Responsabile, il trasferimento dei dati all'estero.
TEMPI DI RETENTION
I dati sono conservati per tutta la durata del contratto e, seguito della cessazione degli effetti del medesimo, rimane per il Cliente la fruibilità dell'intero software per i successivi 90 giorni. Terminato suddetto termine decorrono 12 mesi di conservazione per le copie di backup.

1. MISURE TECNICHE IMPLEMENTABILI A LIVELLO APPLICATIVO

- *Sistema di autenticazione:*

Xatlas ha diverse metodologie di autenticazione:

- 1) con login e password;
- 2) configurabilità con SITEMINDER (meccanismo di sso);
- 3) può essere integrata la parte client con l'utenza di windows. La pagina di log in può essere autenticata da Xatlas o appoggiarsi ad una pagina che fa ldap.

Qualora la login e password siano configurata da Xatlas ci sono diverse configurabilità sia di complessità che di massimo riutilizzo delle stesse, in particolare:

Regole Password e username: lunghezza minima, ogni quanto sostituirla, è possibile consegnare password temporanee con sostituzione obbligatoria al primo utilizzo, vietato riutilizzo password già utilizzate, controllato il numero di errore consecutivi di errata digitazione delle password con blocco nei tentativi di accesso, utenza non utilizzata da almeno 6 mesi disabilitata, la stessa utenza non utilizzabile contemporaneamente da due stazioni diverse, la password salvata in db con crittografia SHA 256, configurabilità nella complessità quindi deve contenere almeno numero, carattere maiuscolo, minuscolo, carattere speciale. Dopo del tempo di inutilizzo del sistema con log in attiva il sistema interrompe in autonomia la sessione.

- *Funzione di estrazione dati in formato strutturato (**diritto alla portabilità**):*

possono essere esportate le timbrature in formato csv. I dati generati o rimangono sul sistema oppure sono inviati su aree SFTP o WEB service, oppure possono rimanere su db e trasferiti con connessione diretta ad altri db. Ogni operazione schedulata o fatta da operatori sono schedulate da un log eventi. Se gli operatori generano un csv l'informazione è salvata nel log. Qualora un dipendente, cliente, visitatore richieda il diritto di accesso ai dati viene effettuata un'estrazione in formato json con cui vengono forniti i dati presenti sul sistema.

- *Utenze nominative per amministratori di sistema:*

al cliente è consegnata un'utenza amministrativa di default che il cliente deve sostituire e tenere segreta. La scelta sull'individualità degli utenti generati e dei profili di accesso assegnati è lasciata al cliente.

- *Supporto alle verifiche previste dal GDPR:*

con apposite estrazioni dati, dal sistema possono essere stampati sia gli operatori che i profili di accesso al sistema

- *Profili predefiniti per ruoli operatore più comuni con diritti di accesso ridotti (**privacy by default**):*

al cliente viene consegnato l'operatore admin e l'operatore guest che è in sola lettura. Con l'utenza admin il cliente può generare un operatore con diritti admin con cui configurare tutti gli altri utenti. L'utente admin quando utilizzato può essere reso inutilizzabile dal cliente. In Xatlas sono predefiniti dei ruoli che sono l'operatore di laboratorio, tecnico, operatori di sicurezza, operatori hr e operatori di reception, in modo che il cliente possa avere già configurazioni standard e non corra il rischio di fare configurazioni errate.

- *Cancellazione di dati personali (**Diritto all'oblio**):*

i dati possono essere cancellati in due macro categorie: ci sono dati sempre presenti e dati legati al tempo. I dati possono essere cancellati o storicizzati. Il cliente in fase di start up può decidere quali dati storicizzare, dove conservarli e dopo quanto tempo cancellarli; sulle anagrafiche è possibile impostare il fine utilizzo esplicito che è una data che se impostata consente di cancellare un modo configurabile dal cliente una serie di dati. Il cliente sceglie le modalità di cancellazione in modo autonomo. Queste funzioni sono elaborate su dipendenti, esterni, veicoli e sulle relative timbrature.

- *Anonimizzazione:*

tutti i log in e password verso altri sistemi sono salvati in SHA256. I dati anagrafici non sono anonimizzati ma si procede direttamente alla cancellazione a fine vita del dato secondo quanto espresso al paragrafo precedente.

- *Log*

I log registrano log in, log out, e ogni operazione che viene fatta di scrittura o attivazione comandi. I log sono conservati per 24 mesi se a db o su txt quando raggiungono la dimensione di 1 mega. Quando raggiungono questa dimensione i txt sono rinominati fino al massimo di 10 volte. E' compito del cliente salvare in un altro repository se desidera conservarli più a lungo.

- *Offuscamento file di LOG:*

di default sono in chiaro ma è possibile, su richiesta del cliente, configurare un log criptato. La registrazione avviene come sopra descritta.

- Per garantire la continuità del servizio il db può convenuto col cliente come cluster e c'è la possibilità di ridondare i nodi. L'FM garantisce la continuità del servizio per la rilevazione delle timbrature anche qualora la rete e la connettività sia momentaneamente interrotta.

- *Change management:*

sono valutate le RQS e deciso se inserirle nel sistema e svilupparle. La procedura viene valutata dal responsabile dello sviluppo applicativo.

Lato FM e XPOINT (per brevità in seguito FM) e terminali.

In particolare possiamo elencare i seguenti macro items:

- Condizione necessaria è che lo specifico terminale abbia un firmware con implementate le modifiche per il GDPR; l'FM comunque è in grado di gestire scenari misti;
- L'FM riconosce automaticamente se il firmware del singolo terminale supporta o meno la crittografia e quindi, senza particolari configurazioni, si pone automaticamente nella configurazione "sicurezza GDPR";
- Gestione invio template biometria anonimizzati: sia l'invio che la ricezione dei template delle impronte è stato oscurato. L'FM anonimizza prima di trasmettere e fa il lavoro contrario in ricezione. In questo caso non rimangono dati sul filesystem del terminale che fa solo da passacarte verso il DB del sensore;
- Gestione tabella utenti anonimizzata: la gestione sull' FM è simile a quella della biometria ma in questo caso sul terminale rimane traccia se la tabella è anonimizzata o meno;
- Offuscamento file di log: sul FM, così come anche su XAtlas, è possibile offuscare i file di log modificando il file di configurazione *log4j* impostando opportunamente l'appendicer che gestisce la crittografia. Naturalmente dove viene effettuata questa impostazione i log risultano illeggibili e la loro decodifica può essere fatta solo da R&D sul file interessato ricevuto.
- Protocolli di comunicazione sicuri: è possibile configurare i terminali in modo che comunichino solo in formato https. Il cliente decide in fase di start up ed in fase di configurazione. I dati sono scambiati tramite file manager in macchina linux oppure direttamente in FM con appositi db proprietari in modo che vive in modo autonomo anche se scollegato dalla rete. L'FM conserva i dati secondo il numero di timbrature configurato dai clienti.
- scambio file crittografati: lo sceglie il cliente se crittografare in Https

Le funzioni di sicurezza sopra riportate non sono attive di default. Il Titolare del trattamento dovrà eseguire le necessarie configurazioni per attivare le opportune funzioni di contenimento del rischio.

Per quanto riguarda le misure di sicurezza dei servizi cloud si rimanda alle misure di sicurezza dichiarate dall'erogatore dei servizi stessi.

Biometria Facciale

XAtlas può identificare le persone fisiche anche mediante biometria facciale. La biometria facciale è disponibile tramite il terminale XPoint Face, oppure dotando di telecamera USB un FM fisico oppure utilizzando telecamere IP.

L'enrollment di nuovi volti può essere fatta da XPoint Face o direttamente da una stazione XAtlas dotata di telecamera.

Per la biometria facciale, valgono le stesse soluzioni tecniche del riconoscimento biometrico delle impronte digitali tra cui la “gestione invio template biometria anonimizzati” descritta in precedenza. In particolare, si evidenzia che:

- Il template facciale usato per il riconoscimento è ottenuto dall’immagine del volto della persona da registrare, con un algoritmo di terze parti non invertibile che non è noto a Zucchetti AXESS
- Dai dati memorizzati (template facciale) non è possibile risalire alla foto dell’utente
- I template biometrici facciali possono essere memorizzati criptati con algoritmo RC4
- I template biometrici vengono distribuiti ai dispositivi che effettuano il riconoscimento (FM e XPoint FACE) con algoritmi di comunicazione criptata
- XAtlas può memorizzare nel suo database di anagrafiche anche la foto dell’utente per poter eventualmente rigenerare i template in autonomia.

Nello specifico il terminale XPoint Face è un dispositivo XPoint con in aggiunta una telecamera integrata e l’algoritmo per la gestione dei template facciali installato. Aggiunge quindi alle funzioni standard di XPoint anche la possibilità di enrollare volti ed effettuare il riconoscimento dell’utente mediante biometria facciale.

XPoint Face può anche essere configurato per eseguire l’enrollment e memorizzare i template nella sua memoria interna senza inviarli a XAtlas. In questo modo nessun dato biometrico viene trasmesso sulla rete. Il riconoscimento del volto avviene tutto in locale confrontando l’immagine del volto della persona davanti alla telecamera con i template memorizzati nella memoria interna di XPoint.

I dati biometrici facciali possono essere memorizzati nel database locale di XPoint Face in formato criptato con algoritmo RC4. I template biometrici vengono scambiati con il server di XAtlas (qualora sia abilitata questa possibilità) con protocolli di comunicazione criptati.

E’ possibile effettuare riconoscimento facciale anche dotando l’FM di una telecamera USB esterna e abilitando la funzione di riconoscimento volti. Valgono le stesse considerazioni dell’XPoint Face

2. RESPONSABILE DEL TRATTAMENTO: PROCEDURE DI ASSISTENZA

MODALITA' DEL SERVIZIO DI ASSISTENZA

L'assistenza ai prodotti e servizi Zucchetti Axess, in funzione della modalità di erogazione, viene effettuata nei seguenti modi:

- Assistenza On Site
- Assistenza telefonica
- Assistenza tramite email/tickets web
- Assistenza attraverso la ricezione di data base dei clienti
- Assistenza attraverso collegamento da remoto
- Assistenza attraverso collegamento da remoto tramite vpn

CONTRAENTI A CUI VIENE FORNITO IL SERVIZIO DI ASSISTENZA

Il servizio di assistenza è erogato verso:

- Clienti diretti Zucchetti Axess
- Clienti Indiretti

La gestione dell'assistenza prevede, generalmente:

- per i clienti diretti: telefonata o email al service (backoffice/casella di posta dedicata) che invia una mail all'assistenza. La chiamata viene aperta su V-Tiger;
- per i clienti indiretti la richiesta viene inviata direttamente dal cliente a una casella di posta dedicata (support@axesstmc.com) .
-

PROCEDURE

ASSISTENZA ON SITE

Gli addetti Zucchetti Axess accedono presso la struttura del cliente per fare formazione od effettuare attività tecnica di manutenzione/assistenza e installazione.

In questo caso lavorano come se facessero parte della struttura del Cliente/Titolare del trattamento ed adottano tutte le procedure che il Cliente richiede di adottare. I clienti/Titolari del trattamento potranno generare utenze individuali per l'accesso ai loro sistemi, oppure potranno far accedere gli incaricati Zucchetti Axess in affiancamento per formare il loro personale.

ASSISTENZA TELEFONICA

Non presenta problemi da un punto di vista di trattamento di dati personali. Non sono trasmessi dati o archivi e la comunicazione rimane verbale. Generalmente, il primo contatto dopo la richiesta di assistenza da parte del cliente avviene sempre in questa modalità, per definire nel dettaglio la problematica segnalata.

ASSISTENZA TRAMITE EMAIL/TICKETS WEB

Nell'assistenza tramite email inserire sempre nel testo del messaggio il disclaimer:

"Il contenuto di questa email e degli eventuali allegati è strettamente confidenziale, non producibile in giudizio e destinato alla/e persona/e a cui è indirizzato. Il contenuto della risposta alla presente email potrebbe essere conosciuto anche da altri collaboratori facenti parte dello stesso Gruppo omogeneo dello scrivente o di gruppi omogenei differenti ma speculari alla soluzione del problema da Lei segnalato. Se avete ricevuto per errore questa email, Vi preghiamo di segnalarcelo immediatamente e di cancellarla dal Vostro computer. E' fatto divieto di copiare e divulgare il contenuto di questa email. Ogni utilizzo abusivo delle informazioni qui contenute da parte di persone terze o comunque non indicate nella presente email, potrà essere perseguito ai sensi di legge. Si informa che per l'esercizio dei diritti previsti dagli artt. 15 e ss. del Regolamento UE 2016/679 (GDPR), è possibile rivolgersi al seguente indirizzo: ufficio.privacy@zucchetti.it".

Gli incaricati Zucchetti Axess non devono mai farsi mandare le credenziali di accesso del Cliente via email (solo quelle utilizzate e in possesso del Cliente stesso, non quelle generate appositamente per i tecnici che devono collegarsi), né tantomeno salvarle sullo strumento di ticketing e/o nelle mail.

Qualora un Cliente/partner invii le credenziali di accesso al proprio ambiente senza richiesta da parte degli incaricati Zucchetti Axess è necessario rispondere che non siamo autorizzati ad accedere ai sistemi con credenziali di altri utenti in quanto questa modalità viola il Regolamento UE 2016/679 (GDPR). Quindi gli incaricati Zucchetti AX dovranno richiedere credenziali individuali oppure il collegamento da remoto.

Ogni email deve essere firmata con nome e cognome dell'operatore che ha gestito il problema del Cliente e l'informazione dovrà essere salvata nel ticketing e/o nella mail.

Precisazioni:

Il disclaimer può essere inserito anche nei tickets web.

Non devono essere utilizzate email personali, in quanto non controllabili.

ASSISTENZA ATTRAVERSO LA RICEZIONE DI DATA BASE DEI CLIENTI

Qualora per risolvere il problema segnalato dal Cliente/Titolare del trattamento fosse necessario farsi trasmettere la base dati o altri files o query contenenti dati personali è necessario comunicare al cliente questa necessità. Se il cliente non è in grado autonomamente di effettuare la copia e richiede agli incaricati Zucchetti Axess di provvedere autonomamente, è necessario ricevere la sua autorizzazione anche al collegamento con VPN (da salvare nello strumento di ticketing e/o nella mail).

Per svolgere questa attività è necessario mandare al cliente/Titolare del trattamento una email del seguente tenore:

"Stimatissimo Cliente,

al fine di risolvere il problema da Lei segnalato è necessario effettuare delle verifiche sui Suoi archivi.

Le chiediamo di autorizzarci al collegamento attraverso la VPN per prelevare copia e a trattarli per la risoluzione di quanto segnalato".

Gli archivi saranno conservati per il tempo strettamente necessario alla risoluzione della problematica segnalata e dovranno essere cancellati, da parte degli incaricati Zucchetti Axess, al termine dell'intervento.

I dati devono essere salvati in Directory non soggette a backup".

Qualora vi fosse la necessità di mantenere gli archivi vi è la necessità di mandare una email al cliente, come di seguito:

"Stimatissimo cliente,

avendo risolto i problemi sugli archivi da lei inviatici, Le chiediamo l'autorizzazione alla conservazione dei Suoi archivi presso la nostra infrastruttura per ulteriori ____ giorni. Tale conservazione è finalizzata a verificare eventuali problematiche che Lei ci segnalerà durante l'utilizzo degli archivi ripristinati. Al termine del periodo sopramenzionato provvederemo all'eliminazione definitiva degli archivi. Se dopo tale termine ci sarà la necessità dei suoi archivi provvederemo a richiederglieli.

Le chiediamo una conferma espressa in tal senso rispondendo a questo messaggio. Qualora la Sua risposta fosse negativa provvederemo all'immediata cancellazione dei Suoi archivi".

Gli archivi dei clienti non potranno mai essere trasmessi a gruppi di lavoro differenti rispetto a quelli finalizzati alla risoluzione del problema segnalato dal cliente.

L'unica possibilità che abbiamo per conservare gli archivi senza la previa autorizzazione del cliente è l'anonimizzazione degli stessi.

ASSISTENZA ATTRAVERSO COLLEGAMENTO DA REMOTO

Questa modalità di collegamento sugli strumenti dei clienti garantisce la privacy in quanto:

- Il collegamento è sempre richiesto dal cliente
- Le credenziali di accesso sono sempre individuali
- Il cliente ci fa accedere ad un ambiente con profilo di autorizzazione da lui scelto per farci eseguire le attività di assistenza
- Il cliente può sconnetterci quando desidera.

Attraverso il collegamento da remoto è possibile far accedere anche l'assistenza di 2 livello alla stessa sessione da noi aperta. In questo caso il cliente ne ha l'evidenza perché fornita dallo strumento e quindi accetta implicitamente tale modalità.

ASSISTENZA ATTRAVERSO COLLEGAMENTO TRAMITE VPN

Qualora l'attività di assistenza debba essere svolta tramite VPN o accessi privati è necessario che gli addetti Zucchetti Axess entrino nei sistemi dei clienti:

- Previa autorizzazione del cliente
- Che abbiano le credenziali attive per il tempo necessario all'esecuzione delle attività richieste
- Che al termine dell'attività siano disattivate da parte del Cliente/Titolare del trattamento

La creazione dell'utenza deve essere richiesta solo al cliente che deve generarla individuale per ogni incaricato Zucchetti AX.

Le utenze vengono generate dal cliente in fase di inizializzazione del contratto e rimangono attive per tutta la durata.

Al termine delle attività di assistenza i tecnici Zucchetti Axess comunicano al cliente che l'attività di assistenza si è conclusa.

ASSISTENZA PER LA VIDEOSORVEGLIANZA

L'assistenza sui sistemi di videosorveglianza viene effettuata in primis da remoto per verificare la problematica. Se da remoto la telecamera non è raggiungibile, si procede on site.

I tecnici non accedono mai alle registrazioni, se non per richiesta espressa dei clienti.

ASSISTENZA NELLA FASE DI TEST

Qualora sia necessario fare dei test sul DB del Cliente, il personale Zucchetti Axess li eseguirà presso i sistemi del cliente, su una nuova macchina/server messa a disposizione, la quale successivamente, al termine dei test, verrà utilizzata per la produzione

3. RESPONSABILE DEL TRATTAMENTO: MISURE DI SICUREZZA APPLICATE AL DATA CENTER

Zucchetti Axess nell'ambito della fornitura del servizio si avvale del Data Center fornito da AWS.

Certificazioni: Zucchetti Axess ritiene la sicurezza un elemento prioritario e irrinunciabile per l'azienda e per i propri clienti per questo ha organizzato i propri sistemi di gestione in modo da seguire rigidi criteri di sicurezza. L'organizzazione di un sistema di gestione impone la creazione di ruoli, flussi di attività e procedure chiaramente definiti a presidio dei processi aziendali. **Certificazioni: ISO 9001 e ISO 27001**

Compliance: i processi aziendali di Zucchetti Axess rispondono alle normative vigenti, in particolare per quanto riguarda la rispondenza ai requisiti di privacy. In tale ambito l'azienda ha adeguato il proprio sistema di gestione alle richieste del provvedimento del Garante per la Protezione dei Dati Personali riguardo gli amministratori di sistema. Qualora le prescrizioni di legge vengano modificate Zucchetti Axess adeguerà immediatamente le modalità di erogazione del servizio e le caratteristiche tecniche per essere conforme alle eventuali modifiche.

Accesso alle informazioni: il sistema di gestione di Zucchetti Axess prevede l'esplicita classificazione del livello di riservatezza di ogni documento. In particolare, i documenti contenenti informazioni sui sistemi di sicurezza vengono classificati come riservati e non sono diffusi all'esterno dell'azienda.

Accesso ai sistemi: gli accessi ai sistemi sono sempre classificabili in accessi di produzione e accessi di amministrazione. Gli accessi di produzione sono quelli oggetto della fornitura del servizio. Gli accessi di amministrazione sono quelli effettuati da Zucchetti Axess o dal cliente con finalità diverse quali la manutenzione, la verifica di anomalie, l'acquisizione di dati. Gli accessi di amministrazione da parte di Zucchetti Axess sono riservati a personale con la qualifica ("ruolo") di amministratore di sistema. L'azienda pone particolare attenzione all'assegnazione di tale ruolo soltanto a personale di elevate capacità tecniche e avente caratteristiche di comprovata affidabilità e moralità. L'accesso amministrativo ai sistemi da parte di personale del cliente avverrà attraverso l'assegnazione nominale di personale a ruoli ai quali sono assegnati privilegi di accesso.

Auditing: nell'ambito del proprio sistema di gestione Zucchetti Axess pone particolare attenzione all'audit dei sistemi e delle attività amministrative compiute sugli stessi. L'infrastruttura AWS è configurata per riportare i propri log verso un sistema centralizzato di elaborazione, classificazione, repository e alerting (CloudWatch). Sono riscontrabili sia eventi singoli che pattern di malfunzionamento dell'infrastruttura (es. sovraccarichi). I sistemi di gestione e analisi dei log vengono inoltre utilizzati per il monitoraggio delle attività degli amministratori di sistema come prescritto dal provvedimento del Garante per la privacy. L'accesso al sistema di gestione dei log è riservato al personale di Zucchetti Axess.

Riservatezza dei dati: il presente documento è stato prodotto assumendo che i dati raccolti dal cliente e presenti sui sistemi ospitati all'interno del Datacenter siano di tipo personale/sensibile, secondo la classificazione prevista dal Codice in materia di protezione dei dati personali. In ogni caso Zucchetti Axess non tratterà i dati del Cliente se non per l'unica finalità della loro conservazione. Zucchetti Axess non potrà conoscere in nessun modo i dati personali inseriti dal cliente se non previa sua autorizzazione finalizzata all'esecuzione di attività di manutenzione e assistenza dell'ambiente. Zucchetti Axess non si assume alcuna responsabilità riguardo all'uso che di tali dati viene fatto da parte del cliente o da società incaricate dal cliente stesso che gestiscono o utilizzano il servizio ubicato e gestito nel Datacenter AWS. Zucchetti Axess gestirà e conserverà le informazioni in conformità alle norme espresse dalla vigente normativa.

Log Management: i log dei sistemi contengono informazioni necessarie alle attività amministrative, di diagnostica e di sicurezza. Ogni sistema viene configurato per loggare ogni evento significativo. I log generati da ogni sistema vengono trasferiti ad un repository centrale che ha il compito di analisi, classificazione e storage. La conservazione dei log avviene secondo le norme di legge, in particolare il Codice Privacy e le norme sulla conservazione dei dati di traffico telefonico e telematico. I log dei sistemi riportano tutte le attività significative ai fini della sicurezza quali gli accessi amministrativi, le modifiche ai permessi e alle configurazioni di sistema e di sicurezza, le anomalie. Tali log sono conservati con le stesse modalità dei log di sistema. In particolare, sono tracciate ed archiviate tutte le attività di accesso e amministrazione in conformità al provvedimento del Garante per la Protezione dei Dati Personali del 27 novembre 2008 riguardo gli amministratori di sistema-

Controlli di sicurezza: sull'intera infrastruttura sono svolti Penetration Test e Vulnerability Assessment con cadenza annuale

Firewalling: il networking del Datacenter è separato dalle reti pubbliche, dalle altre reti di Interviewweb e dalle altre reti del cliente. I flussi dati tra il networking del Datacenter e l'esterno vengono mediati da sistemi di firewall. Tali sistemi di firewall permettono il transito soltanto ai flussi dati necessari al funzionamento del servizio ed esplicitamente autorizzati. I sistemi utilizzati per l'isolamento del Networking sono: Virtual Private Cloud (Aws VPC), Security Groups (Aws), NAT, LoadBalancers.

Intrusion Prevention: il Datacenter è protetto da sistemi di Intrusion Prevention System (IPS) che permettono di analizzare tutto il traffico in entrata individuando immediatamente i tentativi di attacco in corso. Il traffico di rete, su segmenti significativi della piattaforma, passa attraverso sistemi che ispezionano ogni pacchetto del traffico in transito e si comportano in modo trasparente nei confronti del traffico legittimo.

Filesystem Antivirus: tutti i server dispongono di moduli Antivirus sul filesystem e, su base progettuale, possono essere configurati prodotti antivirus specifici gestiti centralmente in termini di aggiornamento, distribuzione delle policy, avvio di scansioni on demand, notifiche e gestione della area di quarantena.

Security Patch Management: la piattaforma è sottoposta ad un processo periodico di verifica delle patch o delle fix rilasciate dal produttore e ritenute critiche per l'erogazione del servizio o per la sicurezza.

ACCESSO AI SERVER

L'accesso ai server in avviene mediante scambio chiave (RSA-256 Pubblica/Privata).

Ogni Amministratore di sistema è in possesso della propria chiave di accesso SSH ed utenza nominale.

Tale utenza non ha privilegi di amministratore.

Qualora sia necessario acquisire diritti superiori, esiste la possibilità di scalare su un utente amministratore.

Ogni tentativo di accesso al sistema operativo (accettato o fallito) viene loggato così come eventuali escalation utente e comandi inviati.

BACKUP

Tutti i database sono soggetti a doppio backup notturno.

1. Backup automatico quotidiano erogato dal servizio RDS-AWS
2. Backup automatico quotidiano su file system del server che ospita il software

CERTIFICAZIONI DEL DATACENTER AWS

ISO 9001 – ISO 27001 - ISO 20000 - ISO 23301 - ISO 27017 - ISO 27018 - ISO 277001