Linee guida sulla stipula di contratti per i servizi cloud destinati all'accesso remoto sicuro ai sistemi d'allarme e alla trasmissione sicura degli allarmi

Tabella di revisione delle modifiche

Data	Revisione	Paragrafo/Pagina	Modifica
Febbraio 2025	1.0		Prima versione

PREFAZIONE

Questo documento ha lo scopo di fornire indicazioni generali e non sostituisce una consulenza dettagliata in situazioni specifiche. Nonostante sia stata posta la massima attenzione nella redazione e preparazione di questa pubblicazione per garantirne l'accuratezza, Euralarm non può in alcun caso essere ritenuta responsabile per eventuali errori, omissioni o consigli forniti, né per eventuali perdite derivanti dall'affidamento alle informazioni contenute in questo documento.

DISCLAIMER

Questo documento è destinato esclusivamente a fornire indicazioni ai membri di Euralarm e, se nel caso, ai loro associati, sullo stato dell'arte relativo all'argomento trattato. Sebbene sia stato fatto ogni sforzo per garantirne l'accuratezza, i lettori non devono farvi affidamento in termini di completezza o correttezza, né considerarlo una fonte di interpretazione legale. Euralarm non potrà essere ritenuta responsabile per eventuali informazioni errate o incomplete contenute nel presente documento.

Nota: la versione inglese del presente documento è il documento di riferimento Euralarm approvato.

Euralarm • Gubelstrasse 11 • CH-6300 Zugo • Svizzera

E-mail: secretariat@euralarm.org
Sito web: www.euralarm.org

Sommario

1. Introduzione

L'uso delle tecnologie più recenti per la trasmissione degli allarmi su rete IP e per l'accesso remoto ai sistemi di sicurezza e/o antincendio (FSSS – Fire Safety and Security Systems) sta diventando sempre più comune. Questo approccio implica spesso il posizionamento di una parte dell'infrastruttura al di fuori della sede del fornitore di servizi FSSS, ad esempio all'interno di un data center. Il presente documento è pensato per supportare i fornitori di servizi FSSS (come gli installatori) nell'utilizzo di data center per ospitare parte delle apparecchiature.

Vengono analizzati due diversi scenari d'uso, ciascuno con requisiti specifici e un pubblico di riferimento distinto:

- Il primo caso riguarda la trasmissione degli allarmi tramite un Sistema di Trasmissione Allarmi (ATS – Alarm Transmission System), gestito da un Fornitore di Servizi di Trasmissione Allarmi (ATSP – Alarm Transmission Service Provider). In questo ambito, la disponibilità del servizio, i tempi di trasmissione, la segnalazione dei guasti e la protezione contro la sostituzione dell'apparecchiatura sono elementi fondamentali. Lo standard EN 50136-1 per i sistemi ATS consente configurazioni in hosting, a condizione che la componente cloud risieda in una sede sicura, come un data center. Le categorie più elevate di ATS includono requisiti di sicurezza da rispettare in tutto il sistema. Le indicazioni per questo scenario si rivolgono a chi assume il ruolo di ATSP.
- Il secondo caso riguarda l'accesso remoto ai sistemi FSSS attraverso un'infrastruttura di accesso remoto (RAI – Remote Access Infrastructure), gestita da un Fornitore di Servizi di Accesso Remoto (RAISP – Remote Access Infrastructure Service Provider). In questo caso, la sicurezza dell'accesso ai sistemi FSSS e dei dati trasmessi è un aspetto chiave, mentre la disponibilità del servizio è considerata un valore aggiunto ma non essenziale. La specifica tecnica CLC/TS 50136-10 richiede che il Server di Accesso Remoto (RAS – Remote Access Server) sia collocato in una sede sicura e definisce requisiti specifici per la protezione dei dati. Le indicazioni relative a questo scenario sono rivolte ai soggetti che intendono assumere il ruolo di RAISP, in particolare a piccoli e medi fornitori di servizi FSSS che non hanno familiarità con i servizi cloud e desiderano offrire servizi remoti conformi alla standard EN 50710.

Sebbene vi siano molte valide ragioni per adottare soluzioni cloud, i fornitori di servizi FSSS devono essere consapevoli dell'impatto che queste scelte possono avere sul proprio business, inclusi aspetti legati alla disponibilità, agli accordi sui livelli di servizio (SLA), alla sicurezza dei dati, alla conformità normativa e agli obblighi legali e contrattuali. Rimane necessario dimostrare la conformità agli standard esistenti, ad esempio in termini di prestazioni e disponibilità, backup, controllo degli accessi, ecc. Le responsabilità relative alla manutenzione devono essere ben comprese e accettate da tutte le parti coinvolte, inclusa la gestione del ciclo di vita di sistemi operativi, piattaforme (es. database, virtualizzazione, ecc.) e applicazioni. Il fornitore FSSS deve poter confermare che tali attività siano state eseguite in conformità alle aspettative e agli accordi di servizio stabiliti.

La conservazione, la condivisione e la protezione dei dati rivestono un'importanza cruciale e richiedono una valutazione legale che va oltre l'ambito del presente documento. Pertanto, il documento non intende fornire un'interpretazione né indicazioni sui requisiti legali.

Ampie sezioni di queste linee guida sono tratte, con autorizzazione, dal documento della BSIA (British Security Industry Association) intitolato "ARC considerations when utilising data center or cloud services". EURALARM ringrazia la BSIA (British Security Industry Association), suo membro, per il prezioso contributo.

Queste linee guida descrivono concetti fondamentali legati ai servizi cloud, prendono in considerazione le norme pertinenti e forniscono una panoramica dei criteri legali da valutare nella scelta del fornitore di servizi cloud (CSP – Cloud Service Provider). Tuttavia, non si propone di coprire l'intera normativa vigente nei singoli Paesi europei. È pertanto fondamentale considerare questo documento nel contesto delle normative locali, che prevalgono in caso di conflitto.

2. Abbreviazioni

AICPA: American Institute of Certified Public Accountants – Istituto Americano dei Revisori Contabili Certificati
AMS: Alarm Management System – Sistema di Gestione degli Allarmi
ANSI: American National Standards Institute – Istituto Americano di Normazione
ARC: Alarm Receiving Centre – Centrale di Ricezione Allarmi
AS: Alarm System – Sistema di Allarme
ATS: Alarm Transmission System – Sistema di Trasmissione Allarmi
BSIA: British Security Industry Association – Associazione Britannica dell'Industria della Sicurezza
CLC: CENELEC – Comitato Europeo di Normazione Elettrotecnica
CSP: Cloud Service Provider – Fornitore di Servizi Cloud
EN: European Standard (Norm) – Standard Europeo
FaaS: Function as a Service – Funzione come Servizio
FSSS: Fire Safety Systems and/or Security Systems – Sistemi Antincendio e/o di Sicurezza
IaaS: Infrastructure as a Service – Infrastruttura come Servizio
IEC: International Electrotechnical Committee – Commissione Elettrotecnica Internazionale
ISO: International Standardisation Organisation – Organizzazione Internazionale per la Normazione
IT: Information Technology – Tecnologia dell'Informazione
MARC: Monitoring and Alarm Receiving Centre – Centro di Monitoraggio e Ricezione Allarmi
PaaS: Platform as a Service – Piattaforma come Servizio
PSTN: Public Switched Telephone Network – Rete Telefonica Pubblica Commutata
RAC: Remote Access Client – Client di Accesso Remoto
RAE: Remote Access Endpoint – Endpoint di Accesso Remoto
RAI: Remote Access Infrastructure – Infrastruttura di Accesso Remoto
RAS: Remote Access Server – Server di Accesso Remoto
RCT: Receiving Centre Transceiver – Ricetrasmettitore della Centrale di Ricezione
RCT-A: RCT at the ARC – RCT installato presso l'ARC
RCT-H: Hosted RCT – RCT in Hosting
SaaS: Software as a Service – Software come Servizio
SLA: Service Level Agreement – Accordo sul Livello di Servizio
SOC: System and Organization Controls – Controlli sui Sistemi e sull'Organizzazione
SPT: Supervised Premises Transceiver – Ricetrasmettitore Supervisionato in Sede
TIA: Telecommunications Industry Association – Associazione dell'Industria delle Telecomunicazioni
TS: Technical Specification – Specifica Tecnica

3. Oggetto

Il presente documento riguarda l'elemento cloud di un'infrastruttura di accesso remoto (RAI, utilizzata per accedere da remoto alle funzionalità del FSSS) e di un sistema di trasmissione allarmi (ATS, utilizzato per trasmettere gli allarmi dal FSSS al centro di ricezione allarmi).

3.1. Accesso remoto a FSSS

Nel caso di un RAI, questo elemento della nuvola è identificato come RAS nella Figura 1.

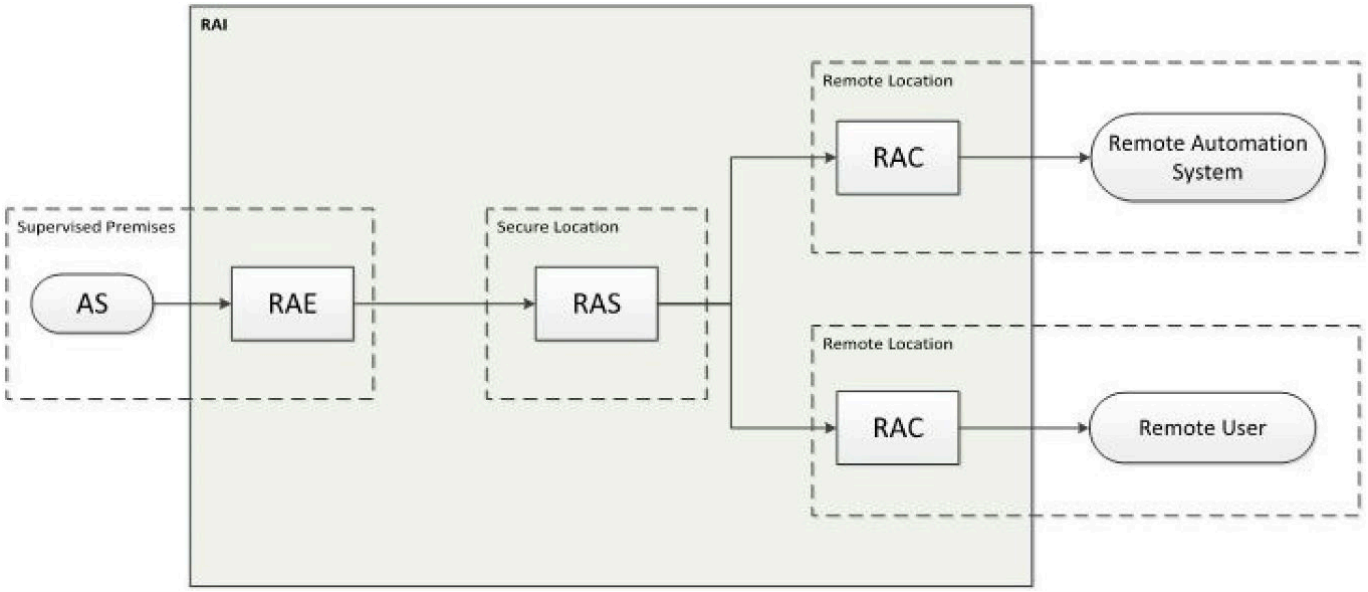

Figura 1. Diagramma logico dell'infrastruttura di accesso remoto (tratto da CLC/TS 50136-10:2022)

3.2. Trasmissione dell'allarme

Nel caso di un sistema di trasmissione allarmi (ATS), la norma europea consente una configurazione non ospitata, illustrata nella Figura 2a. In tale configurazione, viene stabilito un collegamento diretto tra il sistema di allarme (AS) e la centrale di ricezione allarmi (ARC o MARC). Inoltre, lo standard consente una configurazione ospitata illustrata nella Figura 2b. In questa configurazione, i messaggi di allarme provenienti da numerosi sistemi di allarme convergono verso un ricevitore ospitato in un data center e identificato come RCT-H, dove vengono elaborati, riconosciuti e archiviati e l'ARC vi accede tramite un percorso di comunicazione protetto. Le considerazioni per affrontare i cambiamenti dalle comunicazioni PSTN alla trasmissione di allarmi IP sono state fornite in un white paper di Euralarm nel 2019: " Reti di nuova generazione per comunicazioni di allarme " [1]. Il fornitore di servizi FSSS deve garantire che l'ATS sia conforme a EN 50136-1, l'SPT sia conforme a EN 50136-2 e RCT, RCT-H e RCT-A siano conformi a EN 50136-3 (vedere A2.2 nell'Allegato 2 per la spiegazione di tali standard). Ciò garantirà che l'intero ATS invierà i messaggi di allarme in tempo e verrà monitorato per eventuali errori nella trasmissione degli allarmi.

[1] https://www.euralarm.org/resource-report/white-paper-new- generation-networks-for-alarm-communications.html

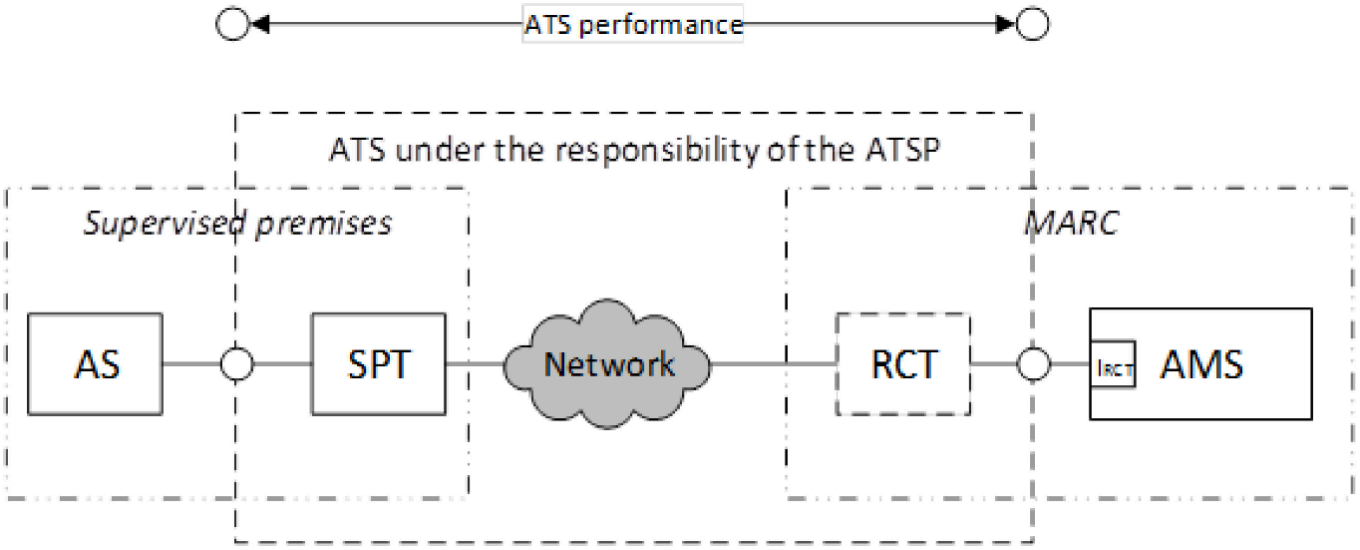

Figura 2a. Esempio di un sistema di trasmissione di allarme **non ospitato** (tratto da EN 50136-1/A1:2018)

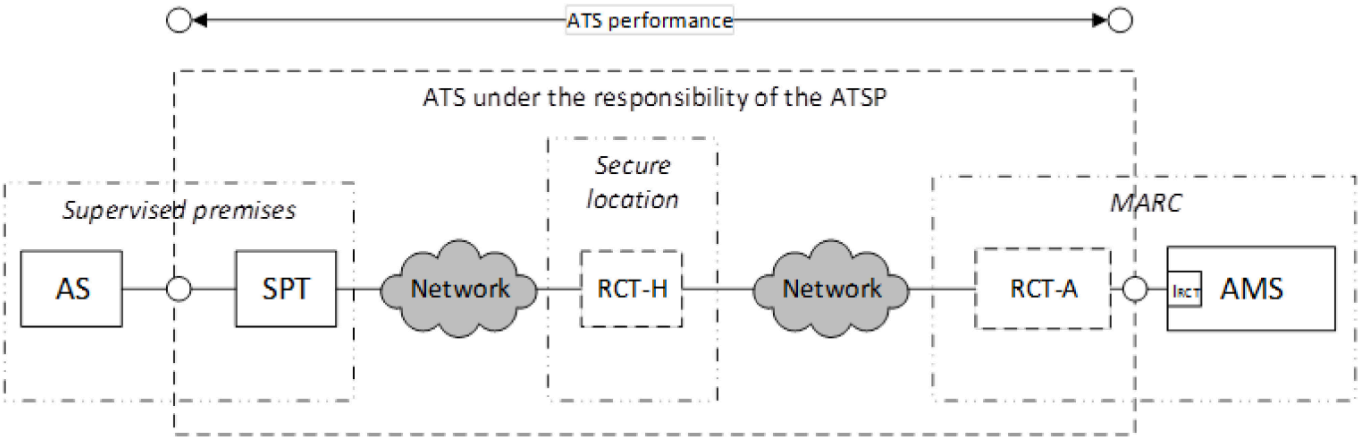

Figura 2b. Esempio di un sistema di trasmissione di allarme **ospitato** (tratto da EN 50136-1/A1:2018)

3.3. Generale

Le presenti linee guida descrivono le considerazioni che un fornitore di servizi FSSS deve fare quando decide di avvalersi dei servizi di un data center o di servizi cloud. Questo documento ha l'obiettivo di supportare la decisione su quanto del servizio FSSS dovrebbe/potrebbe essere ospitato (o parzialmente ospitato) in un ambiente cloud in modo sicuro e protetto.

Un fornitore di servizi FSSS è costantemente impegnato a proteggere le vite umane e le proprietà/beni, e a tal riguardo, i requisiti di sicurezza sono più critici rispetto a quelli di molte altre organizzazioni.

4. Ambienti cloud

4.1. Introduzione

Una dovuta diligenza è fondamentale quando si valuta e seleziona un fornitore di servizi cloud. La dovuta diligenza si riferisce alla ricerca e valutazione approfondita di potenziali fornitori o service provider prima di intraprendere una relazione commerciale con loro. Questo processo aiuta a comprendere meglio le capacità del fornitore, la sua affidabilità, le misure di sicurezza adottate e la sua idoneità complessiva per soddisfare le esigenze specifiche.

Tre ambienti vengono tradizionalmente definiti come: soluzione cloud aziendale privata, data center ospitato (da ora in poi "Data Center") o cloud nativo (da ora in poi "Cloud"). Il fornitore di servizi FSSS può utilizzare uno o più di questi ambienti per ospitare l'attrezzatura tecnica che costituisce l'accesso remoto o la trasmissione degli allarmi, oppure può avvalersi della soluzione offerta dal produttore del FSSS.

Questo documento non implica che le soluzioni cloud aziendali private o gli ambienti cloud siano l'unico modello operativo per tutte le applicazioni, ma riconosce che il fornitore di servizi FSSS potrà operare applicazioni in diversi modelli ambientali. In altre parole, possono utilizzare tutti e tre gli ambienti operativi in misura maggiore o minore, a seconda dei requisiti del servizio.

I fornitori di servizi FSSS dovrebbero anche considerare i requisiti di certificazione di terze parti quando scelgono una propria soluzione o soluzioni offerte da data center o cloud.

L'uso di data center/servizi cloud non esclude le responsabilità del fornitore di servizi FSSS come dettagliato in EN 16763, EN 50710 o EN 50136-1 (vedere A2.2 nell'Allegato 2 per la spiegazione di tali standard). È stata pubblicata una guida Euralarm [2] dedicata all'implementazione di servizi remoti, reperibile sul sito web. Aiuta il fornitore di servizi FSSS a verificare in anticipo la propria conformità ai requisiti di tali standard.

4.2. Soluzione cloud aziendale privata

Le soluzioni aziendali private sono gestite dal fornitore di servizi FSSS. I server sono installati all'interno dello stesso edificio o nelle strutture in cui si trova il fornitore di servizi FSSS, oppure in un altro edificio sotto la responsabilità del fornitore di servizi FSSS. Un fornitore di applicazioni fornirà alla società di servizi il software da eseguire sui server. I server sono acquisiti dal fornitore di servizi FSSS o acquistati come parte del servizio offerto dal fornitore dell'applicazione.

Gli aggiornamenti dei sistemi operativi dei server, dei database e del software applicativo saranno coordinati tra il fornitore di servizi FSSS e il fornitore dell'applicazione. La sicurezza (come la crittografia dei dati a riposo, ecc.) e l'affidabilità (ad esempio la replicazione dei database con diversità geografica) sono soluzioni generalmente implementate dal fornitore dell'applicazione.

4.3. Data Center

Le soluzioni per data center sono server installati in una sede gestita da una società terza che fornisce sicurezza fisica, alimentazione e spazio rack per ospitare i server. Questi server possono essere dedicati ad uno specifico fornitore di servizi FSSS o gestire un ambiente multi-tenant. Questi server sono gestiti dal fornitore di servizi FSSS o dal fornitore dell'applicazione come servizio gestito.

4.4. Cloud

4.4.1. Descrizione

Le soluzioni cloud includono tutte le caratteristiche della soluzione data centre, ma i server e le altre tecnologie correlate (come i database, ecc.) sono forniti e mantenuti dal fornitore del servizio cloud (ad esempio AWS -

[2] https://www.euralarm.org/resource/guidance-on-remote-services---final-xlsx.html

Amazon Web Services, Microsoft Azure, Google Cloud, IBM). Il Cloud Shared Responsibility Model (SRM) è un framework che delinea le responsabilità tra il fornitore del servizio cloud e il fornitore dell'applicazione per garantire la sicurezza dell'ambiente cloud.

Il fornitore del servizio cloud protegge le risorse dell'ambiente dello sviluppatore dell'applicazione. Ad esempio, fornisce la sicurezza fisica e protegge i servizi di virtualizzazione. Il fornitore dell'applicazione protegge le risorse nella propria istanza cloud, ovvero il fornitore dell'applicazione protegge il sistema operativo che installa sui server e gestisce chi ha accesso al proprio ambiente cloud.

Il cloud computing comprende diversi modelli che rispondono a diverse esigenze e casi d'uso. È importante notare che questi modelli non sono mutuamente esclusivi, e i fornitori di servizi cloud offrono spesso una combinazione di essi per soddisfare requisiti e preferenze differenti. Le sezioni seguenti descrivono 4 modelli cloud diversi.

4.4.2. Infrastructure as a Service (IaaS)

Questo modello fornisce risorse di calcolo virtualizzate tramite internet. Offre macchine virtuali, storage e reti che gli utenti possono configurare e gestire. Gli utenti hanno un maggiore controllo sull'infrastruttura, inclusi i sistemi operativi e le applicazioni.

4.4.3. Platform as a Service (PaaS)

PaaS offre una piattaforma per gli sviluppatori per costruire, distribuire e gestire applicazioni senza doversi preoccupare dell'infrastruttura sottostante. Fornisce un ambiente preconfigurato con strumenti, framework e runtime per lo sviluppo delle applicazioni. Gli utenti possono concentrarsi sulla programmazione e sulla logica dell'applicazione, mentre la piattaforma gestisce la scalabilità, il bilanciamento del carico e la distribuzione.

4.4.4. Serverless Computing

Il Serverless computing è un modello in cui gli sviluppatori scrivono e distribuiscono il codice come singole funzioni o unità di codice. Il fornitore del servizio cloud gestisce l'infrastruttura e scala automaticamente le risorse in base alla domanda. Gli sviluppatori non devono preoccuparsi di server o gestione dell'infrastruttura, concentrandosi esclusivamente sulla scrittura del codice.

4.4.5. Software as a Service (SaaS)

SaaS è un'applicazione software completa fornita tramite internet. Gli utenti finali del FSSS o i fornitori di servizi FSSS possono accedere e utilizzare il software senza la necessità di installazione o gestione. I fornitori di soluzioni SaaS eseguono i propri server in modelli IaaS, PaaS o Serverless computing.

4.4.6. Considerazioni sui modelli cloud nativi

È importante considerare con attenzione i requisiti specifici e le limitazioni di un'applicazione mission-critical quando si sceglie tra ambienti. Fattori come le necessità di prestazioni, i requisiti di scalabilità, le opzioni di gestione e le considerazioni sui costi devono essere valutati per determinare la soluzione più adatta agli obiettivi dell'applicazione.

Per ulteriori informazioni fare riferimento all'allegato 1.

4.5. Soluzione del produttore

I produttori di FSSS hanno sviluppato le loro soluzioni e le offrono ai fornitori di servizi FSSS tramite i loro sistemi. Una tale soluzione può essere basata su uno dei 3 ambienti descritti in precedenza. Il fornitore di servizi FSSS non deve preoccuparsi della manutenzione dei server, del software e delle applicazioni. Deve solo garantire un accordo contrattuale che soddisfi le sue esigenze e aspettative.

Di solito, il fornitore di servizi FSSS non ha un contratto con il produttore per l'utilizzo della sua soluzione, ma accetta i termini e le condizioni accedendo all'applicazione nel cloud. Pertanto, si consiglia che il produttore rediga un documento per l'installatore in cui chiarisce l'applicazione cloud:

- Quale fornitore di servizi cloud,
- dove saranno ubicati i dati,
- come sono accessibili, comprese le misure di sicurezza,
- livello di servizio come tempo di ripristino e manutenzione,
- a quale certificazione il produttore può fare riferimento,
- come il fornitore del servizio FSSS dovrebbe connettere correttamente il FSSS,
- ...

4.6. Considerazioni per gli ambienti operativi

Le soluzioni cloud aziendali private e le soluzioni dei data center richiedono investimenti in hardware, software e infrastrutture, nonché competenze per configurarli e mantenerli. Le soluzioni basate sul cloud richiedono comunque che il fornitore dell'applicazione abbia le competenze necessarie per comprendere, monitorare e scalare le funzionalità richieste. Il fornitore di servizi cloud fornisce servizi IT esperti per il deployment e la manutenzione dell'hardware, dei sistemi operativi e del software del database.

Dovrebbero essere adottati provvedimenti per considerare la sicurezza dei dati accessibili tramite connessioni online o basate su cloud.

5. Criteri legali per l'ubicazione dei server

5.1. Introduzione

Le normative sui server di dati nei paesi europei sono disciplinate da una combinazione di leggi nazionali e normative dell'Unione Europea. Ecco una panoramica delle norme chiave in vari paesi europei, nonché del quadro generale dell'UE.

5.2. Regolamento generale sulla protezione dei dati dell'Unione Europea (GDPR)

Il GDPR, in vigore dal maggio 2018, è il principale regolamento che disciplina la protezione dei dati e la privacy nell'Unione Europea. Si applica a tutti gli Stati membri e comprende:

- Principi di trattamento dei dati: legalità, correttezza, trasparenza, limitazione della finalità, minimizzazione dei dati, accuratezza, limitazione della conservazione, integrità e riservatezza;
- Diritti degli interessati: diritto di accesso, rettifica, cancellazione (diritto all'oblio), limitazione del trattamento, portabilità dei dati e opposizione;

- Trasferimenti di dati: restrizioni sul trasferimento di dati personali al di fuori dell'UE/SEE, garantendo livelli adeguati di protezione;
- Notifiche di violazioni dei dati: obbligo di notificare alle autorità e agli individui interessati le violazioni dei dati entro 72 ore.

5.3. Esempi di normative specifiche per paese

Germania

Legge federale sulla protezione dei dati (Bundesdatenschutzgesetz, BDSG): Integra il GDPR con requisiti aggiuntivi, inclusi regolamenti più severi sul trattamento dei dati per scopi occupazionali e obblighi specifici per i responsabili della protezione dei dati.

Francia

Legge sulla protezione dei dati (Loi Informatique et Libertés): Applica le disposizioni del GDPR e aggiunge specifiche nazionali, come le regole sul trattamento dei dati sanitari e poteri aggiuntivi per l'autorità nazionale per la protezione dei dati (CNIL).

Regno Unito

Data Protection Act 2018: implementa il GDPR e include disposizioni specifiche per il trattamento dei dati da parte delle autorità pubbliche e delle forze dell'ordine. Dopo la Brexit, il Regno Unito ha adottato il UK GDPR, che riflette il GDPR dell'UE ma opera in modo indipendente.

Italia

Codice della protezione dei dati personali (Codice in materia di protezione dei dati personali): Allinea con il GDPR, con regole nazionali aggiuntive sul trattamento dei dati per scopi di ricerca scientifica e storica, e per scopi giornalistici.

Spagna

Legge organica sulla protezione dei dati e diritti digitali (LOPDGDD): Completa il GDPR con regole specifiche sui diritti digitali e protezioni aggiuntive per minori e individui vulnerabili.

Paesi Bassi

Legge di attuazione olandese (Uitvoeringswet AVG): Integra il GDPR con disposizioni nazionali, in particolare per il trattamento di registri penali e dati dei dipendenti.

Belgio

Legge di attuazione belga (Gegevensbeschermingsautoriteit GBA): Legge quadro del 30 luglio 2018.

I temi comuni a tutti i paesi sono:

- Localizzazione dei dati: alcuni paesi hanno requisiti specifici per la localizzazione dei dati, in particolare per i dati sensibili come i record sanitari;
- Normative settoriali specifiche: molti paesi impongono regolamentazioni aggiuntive per determinati settori, come finanza, sanità e telecomunicazioni;
- Autorità per la protezione dei dati (DPA): ogni paese ha una DPA nazionale responsabile dell'applicazione delle leggi sulla protezione dei dati e della gestione delle denunce. Esempi includono CNIL in Francia, ICO nel Regno Unito e BfDI in Germania;
- Trasferimenti transfrontalieri di dati: i paesi dell'UE generalmente seguono il quadro del GDPR per i trasferimenti internazionali di dati, che includono meccanismi come le Clausole Contrattuali Standard (SCC), le Regole Aziendali Vincolanti (BCR) e le decisioni di adeguatezza.

Questa lista delle normative specifiche dei vari paesi non è esaustiva. Per normative più dettagliate e gli ultimi aggiornamenti, è consigliabile consultare le rispettive DPA nazionali e i testi legali di ciascun paese.

5.4. Riferimenti utili

- Commissione Europea - Protezione dei dati[3]
- Testo GDPR[4]
- CNIL (Francia)[5]
- ICO (Regno Unito)[6]
- BfDI (Germania)

6. Distribuzione dei ruoli e delle responsabilità

6.1. Impatto delle attività di manutenzione (pianificate/non pianificate)

La disponibilità dell'infrastruttura può variare in base alla criticità dei servizi erogati. I servizi di trasmissione degli allarmi richiedono un'elevata disponibilità, come definito dalla categoria applicabile in EN 50136-1. In generale, la disponibilità è considerata meno critica per i servizi di accesso remoto.

Il fornitore di servizi FSSS (o il produttore nell'ambiente della soluzione del produttore) dovrebbe avere processi definiti per la gestione delle attività di manutenzione e, ove necessario, per la mitigazione dei rischi, ad esempio disponibilità di sistemi secondari o infrastrutture duplicate.

I fornitori di servizi FSSS che considerano una soluzione ospitata dovrebbero assicurarsi che siano in vigore contratti (SLA) con i fornitori di servizi cloud per garantire che il fornitore di servizi FSSS venga notificato in anticipo della durata dei periodi di offline durante la manutenzione programmata. Questi contratti dovrebbero includere anche la gestione e la comunicazione della manutenzione non programmata.

Nel caso in cui i fornitori di servizi FSSS dipendano da terzi per i servizi IT, dovrebbero considerare come gli incidenti possano influire sulla capacità del fornitore di servizi IT di fornire supporto.

6.2. Competenze informatiche

Il fornitore di servizi FSSS è infine responsabile per i propri equipaggiamenti e sistemi e avrà bisogno di un certo livello di competenza IT locale per garantire che le attività di monitoraggio e manutenzione di routine sulla soluzione del fornitore di servizi FSSS siano gestite correttamente.

6.3. Sicurezza

I fornitori di servizi FSSS dovrebbero considerare chi ha accesso ai loro sistemi e ai dati, nonché valutare i requisiti per lo screening del personale. Esistono diverse opzioni per affrontare le sfide legate alla sicurezza, tra cui:

- Gestione dell'identità e dell'accesso (IAM)
- Crittografia
- Monitoraggio della sicurezza e registrazione degli eventi
- Conformità e certificazioni
- Sicurezza della rete

[3]https://commission.europa.eu/law/law-topic/data-protection_en
[4]https://eur-lex.europa.eu/eli/reg/2016/679/oj
[5]https://www.cnil.fr/it
[6]Italiano: https://ico.org.uk

Le soluzioni di data center richiedono personale on-premises e/o accesso remoto per gestire e mantenere l'infrastruttura, compresa la manutenzione dell'hardware, gli aggiornamenti del software e le patch di sicurezza. Al contrario, le soluzioni cloud sono gestite dal provider di servizi cloud, che si occupa di tutta la manutenzione dell'infrastruttura, degli aggiornamenti software e delle patch di sicurezza, liberando il personale IT interno per concentrarsi su funzioni aziendali core.

In ogni ambiente cloud, c'è una responsabilità condivisa tra il Cloud Service Provider (CSP) e l'utente (fornitore di servizi FSSS o produttore). La sicurezza, per aspetti come la classificazione dei dati, i controlli di rete e la sicurezza fisica, necessita di chiari responsabili. La divisione di queste responsabilità è nota come modello di responsabilità condivisa (SRM) per la sicurezza del cloud. Consulta questo diagramma per vedere dove risiedono le responsabilità in diversi ambienti cloud.

.

Soluzione cloud aziendale privata	**Infrastructure as a Service *IaaS***	**Platform as a Service *PaaS***	**Software as a Service *SaaS***
Dati e configurazioni	Dati e configurazioni	Dati e configurazioni	Dati e configurazioni
Codice dell'applicazione	Codice dell'applicazione	Codice dell'applicazione	Codice dell'applicazione
Scalabilità	Scalabilità	Scalabilità	Scalabilità
Tempo di esecuzione	Tempo di esecuzione	Tempo di esecuzione	Tempo di esecuzione
Sistema operativo	Sistema operativo	Sistema operativo	Sistema operativo
Virtualizzazione	Virtualizzazione	Virtualizzazione	Virtualizzazione
Hardware	Hardware	Hardware	Hardware
Gestito dal fornitore del servizio FSSS o dal produttore			
Gestito dal fornitore di servizi cloud			

Ulteriori informazioni e indicazioni su SRM sono disponibili sul sito web del Center for Internet Security (CIS) [7].

7. Contratto di servizi cloud

Nel 2012, la Commissione Europea ha scritto nella sua comunicazione intitolata " Sfruttare il potenziale del cloud computing in Europa" [8]:

> *"Tradizionalmente, i contratti di outsourcing IT venivano negoziati e riguardavano principalmente lo stoccaggio dei dati, le strutture di elaborazione e i servizi, che venivano definiti e descritti in modo dettagliato e anticipato. Al contrario, i contratti per il cloud computing creano essenzialmente un quadro in cui l'utente ha accesso a capacità IT infinitamente scalabili e flessibili, in base alle proprie necessità. Tuttavia, attualmente, la maggiore flessibilità del cloud computing rispetto all'outsourcing tradizionale è spesso bilanciata da una minore certezza per il cliente, a causa di contratti con i fornitori di cloud insufficientemente specifici e sbilanciati.*
>
> *La complessità e l'incertezza del quadro giuridico per i fornitori di servizi cloud porta spesso all'uso di contratti complessi o accordi sui livelli di servizio con numerose clausole di esclusione. L'uso di contratti standard "prendere o lasciare" può risultare vantaggioso in termini di costi per il fornitore, ma spesso è indesiderato per l'utente, inclusi i consumatori finali. Tali contratti possono anche imporre la scelta della legge applicabile o ostacolare il*

[7] https://www.cisecurity.org/insights/blog/shared-responsibility-cloud-security-what-you-need-to-know
[8] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:IT:PDF

recupero dei dati. Anche le grandi aziende hanno poca capacità di negoziazione, e i contratti spesso non prevedono la responsabilità per l'integrità dei dati, la riservatezza o la continuità del servizio."

Per aiutare ad affrontare questa complessità e incertezza, è possibile trovare indicazioni dettagliate sugli elementi contrattuali chiave delle "Linee guida sull'outsourcing ai fornitori di servizi cloud " [9] pubblicate dall'Autorità Europea degli Strumenti Finanziari e dei Mercati (esma) nel 2021 in varie lingue europee. In particolare, ad essere rilevanti sono le seguenti sezioni del documento:

- Linee guida 3 – Elementi contrattuali chiave;
- Linee guida 4 – Sicurezza delle informazioni;
- Linee guida 5 – Strategie di uscita;
- Linee guida 6 – Diritti di accesso e di controllo.

NOTA: indicazioni simili sono disponibili anche sul sito web dall'Autorità Europea delle Assicurazioni e delle Pensioni Aziendali e Professionali (EIOPA) [10].

Inoltre, nell'ambito del Data Act ((UE) 2023/2854), la Commissione Europea sta preparando clausole contrattuali standard per guidare le parti interessate nell'attuazione delle disposizioni relative al cambio di fornitore di servizi cloud e alla condivisione dei dati. Si prevede che questa guida venga pubblicata nel corso del 2025.

Infine, l'allegato 2 delle presenti linee guida Euralarm fornisce riferimenti agli standard e agli schemi di certificazione ai quali può essere richiesta la conformità del contratto con il fornitore di servizi cloud.

Ulteriori informazioni sui contratti di cloud computing sono disponibili sul sito web della CE:

- " Contratti di cloud computing "[11]
- " Studio comparativo sui contratti di cloud computing "[12]

8. Conclusione

Poiché non esiste uno schema di certificazione unico e uniforme per i data center e i servizi cloud, il fornitore di servizi FSSS (FSSS service provider) dovrebbe essere certo che il fornitore di servizi cloud (CSP) garantisca che il data center soddisfi i requisiti di affidabilità e sicurezza necessari per il caso d'uso considerato. Qualsiasi dichiarazione di conformità rilasciata dal CSP o dal produttore per dimostrare l'affidabilità e la sicurezza del servizio cloud dovrebbe almeno comprendere le seguenti considerazioni:

- per quanto riguarda il data center utilizzato:
  - Nome e ubicazione del data center;
  - Livello di garanzia di continuità aziendale, da nessuna continuità a piena continuità in caso di guasto del data center (critico per la trasmissione degli allarmi e conveniente per l'accesso remoto);
  - Misure per minimizzare il rischio di guasto, come la selezione di uno o più siti, struttura dell'edificio, sistemi di alimentazione, sistemi di raffreddamento, sistemi meccanici, architettura, sicurezza fisica, cybersecurity, infrastruttura di cablaggio, sistemi di telecomunicazioni, politica di backup, protezione antincendio e sicurezza (critico per la trasmissione degli allarmi e conveniente per l'accesso remoto.

[9] https://www.esma.europa.eu/document/guidelines-outsourcing-cloud-service-provviders
[10] https://www.eiopa.europa.eu/system/files/2020-04/guidelines_on_outsourcing_to_cloud_service_providers_en.pdf
[11] https://commission.europa.eu/business-economy-euro/doing-business-eu/contract-rules/cloud-computing/cloud-computing-contracts_en
[12] https://op.europa.eu/it/publication-detail/-/publication/40148ba1-1784-4d1a-bb64-334ac3df22c7

- per quanto riguarda il servizio cloud:
    - Ambiente cloud utilizzato;
    - Distribuzione chiara e comprensibile dei ruoli e delle responsabilità, correttamente delineata in un SLA (Service Level Agreement);
    - Piano di Recupero Dati (Disaster Recovery Plan, DRP) in atto (critico per la trasmissione degli allarmi e conveniente per l'accesso remoto);
    - Piano di test dopo un aggiornamento software;
    - Notifica al fornitore FSSS in caso di aggiornamenti di sistema, aggiornamenti software o cambiamento del fornitore.
- per quanto riguarda la sicurezza informatica e la privacy del data center e del servizio cloud:
    - Conformità alla ISO/IEC 27001;
    - Certificato secondo lo schema di certificazione EUCS (quando disponibile, vedi A2.6);
    - Meccanismi di controllo accessi sicuri con autenticazione per accedere ai dati e alle funzioni archiviate;
    - Crittografia dei dati in transito;
    - Mitigazione degli effetti degli attacchi (D)DOS;
    - Processo di gestione delle vulnerabilità;
    - Verifica tramite test di penetrazione.
- per la trasmissione degli allarmi:
    - Conformità dell'ATS allo standard EN 50136-1, con una categoria dichiarata appropriata al rischio protetto (tempo di trasmissione, disponibilità, tempo di segnalazione in caso di guasti nella trasmissione, requisiti di crittografia, sicurezza di sostituzione, modalità di conferma, ecc.);
    - categoria a doppio percorso (DP) in cui sono coperti rischi elevati o per sistemi vitali (pericolosi per la vita);
- per l'accesso remoto a FSSS:
    - Conformità del RAI a CLC/TS 50136-10.

9. Bibliografia

"Considerazioni ARC sull'utilizzo di servizi di data center o cloud", BSIA (British Security Industry Association), numero 1, ottobre 2023.

Allegato 1 - Data Center/IaaS e Serverless

Per un'applicazione mission-critical, sia gli ambienti IaaS (Infrastructure as a Service) che Serverless presentano vantaggi e svantaggi. Ecco alcuni confronti tra i due:

- Complessità di gestione: in un ambiente IaaS, gli utenti hanno il pieno controllo sull'infrastruttura, il che significa che devono occuparsi di attività come la fornitura e la gestione dei server, la configurazione della rete e la garanzia dell'alta disponibilità. Ciò richiede maggiore esperienza, tempo e risorse rispetto a un ambiente Serverless , dove la gestione dell'infrastruttura è astratta. Con il Serverless , i fornitori di applicazioni possono concentrarsi esclusivamente sulla fornitura di servizi software, ma hanno una comprensione ridotta dell'infrastruttura sottostante, il che potrebbe essere una limitazione per alcune applicazioni mission-critical.

- Scalabilità: in un ambiente IaaS, scalare l'infrastruttura per gestire un aumento del traffico o della domanda richiede interventi manuali e configurazione. Al contrario, gli ambienti Serverless scalano automaticamente le risorse in base al numero di richieste o eventi attivati, consentendo una scalabilità più dinamica. Tuttavia, il Serverless può presentare alcune limitazioni sulla scalabilità, come il numero massimo di esecuzioni simultanee o la durata dell'esecuzione, che possono influire su applicazioni ad alte prestazioni.

- Cold Start e Performance: gli ambienti Serverless presentano spesso il concetto di "cold start", in cui la prima esecuzione di una funzione comporta una latenza aggiuntiva dovuta alla necessità di inizializzare l'ambiente di runtime. Questa latenza può influire su applicazioni in tempo reale o a bassa latenza. In un ambiente IaaS, le applicazioni vengono eseguite su server dedicati o macchine virtuali, che offrono generalmente prestazioni costanti senza ritardi legati al cold start. Inoltre, gli ambienti Serverless possono avere limitazioni sulle risorse assegnate a singole funzioni, il che può influenzare le prestazioni di applicazioni che richiedono molte risorse.

- Vendor Lock-In: sebbene sia gli ambienti IaaS che Serverless comportino un certo livello di vendor lock-in, gli ambienti Serverless spesso offrono servizi più strettamente integrati e architetture basate su eventi, il che rende più difficile migrare le applicazioni tra diversi provider di servizi cloud o verso infrastrutture on-premise. In un ambiente IaaS, gli utenti hanno maggiore flessibilità nel trasferire le loro applicazioni tra diversi provider o addirittura portarli in-house.

- Costi e prevedibilità: gli ambienti Serverless seguono un modello di pricing pay-per-use, che può essere conveniente per applicazioni con carichi di lavoro sporadici o variabili. Tuttavia, la struttura dei costi può risultare complessa e imprevedibile, soprattutto con costi aggiuntivi per chiamate API, trasferimento dati e utilizzo delle risorse. In un ambiente IaaS, gli utenti hanno un maggiore controllo sull'allocazione delle risorse e sui costi, il che consente una migliore prevedibilità dei costi, ma con potenziali costi fissi più elevati.

Allegato 2 - Standard e schemi di certificazione

A2.1. Introduzione

Di seguito sono riportati gli standard fondamentali relative alla trasmissione degli allarmi, all'accesso remoto e ai centri dati che potrebbero essere utili per determinare le prestazioni di un sistema o di un servizio in termini di resilienza, robustezza e affidabilità.

A2.2. Standard per la trasmissione degli allarmi, l'accesso remoto ai sistemi di allarme e i servizi remoti

EN 50136-1 Requisiti generali per i sistemi di trasmissione degli allarmi

Questo standard europeo stabilisce i requisiti per le caratteristiche di prestazione, affidabilità e sicurezza dei sistemi di trasmissione degli allarmi. Specifica i requisiti per i sistemi di trasmissione degli allarmi che forniscono la trasmissione degli allarmi tra un sistema di allarme presso un'area sorvegliata e l'attrezzatura di segnalazione in un centro di ricezione degli allarmi.

Questo standard europeo si applica ai sistemi di trasmissione per tutti i tipi di messaggi di allarme, come allarmi antincendio, intrusioni, controllo accessi, allarmi sociali, ecc.

Un fornitore di servizi FSSS che assume il ruolo di ATSP (Fornitore del Servizio di Trasmissione degli Allarmi) deve essere conforme alle disposizioni di questo standard.

CLC/TS 50136-10 Sistemi di allarme - Requisiti per l'accesso remoto

Questo documento specifica i requisiti minimi per una connessione sicura e una sessione di accesso remoto a uno o più sistemi di allarme, come i sistemi di sicurezza antincendio, i sistemi di allarme contro l'intrusione e antirapina, i sistemi di controllo elettronico degli accessi, i sistemi di sicurezza perimetrale esterni, i sistemi di videosorveglianza e i sistemi di allarme sociale.

Questo documento stabilisce i requisiti per le caratteristiche di prestazione, affidabilità, integrità e sicurezza di un'infrastruttura di accesso remoto.

Questo documento definisce i requisiti per un'infrastruttura di accesso remoto tra un client di accesso remoto e un sistema di allarme presso l'area sorvegliata, che può essere integrata come parte dell'ATS o come un'infrastruttura separata.

Un fornitore di servizi FSSS che assume il ruolo di RAISP (Fornitore di Servizi di Infrastruttura per l'Accesso Remoto) deve essere conforme alle disposizioni di questa specifica tecnica.

EN 50710 Requisiti per la fornitura di servizi remoti sicuri per sistemi antincendio e sistemi di sicurezza

Questo documento specifica i requisiti minimi per la fornitura di servizi remoti sicuri tramite un'infrastruttura di accesso remoto (RAI), effettuati sia in loco che da remoto (ad esempio, tramite connessioni IP), per i seguenti sistemi:

a) sistemi di sicurezza antincendio, tra cui, a titolo esemplificativo ma non esaustivo, sistemi di rilevamento e allarme antincendio, sistemi fissi antincendio, sistemi di controllo del fumo e del calore;
b) sistemi di sicurezza, inclusi, a titolo esemplificativo ma non esaustivo, sistemi di allarme contro l'intrusione e antirapina, sistemi di controllo elettronico degli accessi, sistemi di sicurezza perimetrali esterni e sistemi di videosorveglianza;
c) sistemi di allarme sociale;
d) sistemi di diffusione sonora di emergenza;
e) una combinazione di tali sistemi;
f) sistemi di gestione connessi ai sistemi a) – e).

Questo standard è inteso a integrare EN 16763 *Servizi per sistemi antincendio e sistemi di sicurezza.*

A2.3 Standard per i servizi cloud

CEN/TS 18026 Approccio a tre livelli per un insieme di requisiti di sicurezza informatica per i servizi cloud

Questa specifica tecnica (TS) fornisce un set di requisiti di sicurezza informatica per i servizi cloud. Questa TS è applicabile alle organizzazioni che forniscono servizi cloud e alle loro organizzazioni di sottoservizi.

Nota: si prevede che questa nuova TS venga pubblicata durante l'estate del 2024.

A2.4 Standard per i sistemi di gestione della sicurezza delle informazioni

ISO/IEC 27001 Sicurezza delle informazioni, sicurezza informatica e protezione della privacy - Sistemi di gestione della sicurezza delle informazioni - Requisiti

ISO/IEC 27001 è uno standard internazionale ampiamente riconosciuto che delinea le migliori pratiche per l'implementazione e il mantenimento di un Sistema di Gestione della Sicurezza delle Informazioni (ISMS). Questo standard fornisce un quadro per la gestione dei rischi relativi alla sicurezza delle informazioni, includendo persone, processi e tecnologie.

ISO/IEC 27001 copre tutti gli aspetti della sicurezza delle informazioni, inclusi la riservatezza, l'integrità e la disponibilità, e richiede alle organizzazioni di implementare controlli per garantire la riservatezza, l'integrità e la disponibilità delle loro risorse informative.

Lo standard richiede inoltre che le organizzazioni adottino un approccio basato sul rischio nella gestione della sicurezza delle informazioni, che implica l'identificazione e la valutazione dei rischi, l'implementazione di controlli appropriati per mitigare tali rischi e il monitoraggio e la revisione continua dell'efficacia dei controlli.

Implementando ISO/IEC 27001, le organizzazioni possono dimostrare il loro impegno nella sicurezza delle informazioni e fornire garanzie agli stakeholder che le loro risorse informative vengono gestite in modo sicuro ed efficace. Lo standard è applicabile a organizzazioni di tutte le dimensioni e settori e viene ampiamente riconosciuto come un punto di riferimento per la gestione della sicurezza delle informazioni.

A2.5. Standard per i data center

ISO/IEC 22237 (e EN 50600) Tecnologia dell'informazione - Strutture e infrastrutture del data center

ISO 22237 è la serie di standard ISO che governa la progettazione, la struttura, l'operatività, la sicurezza fisica e informativa dei data centre. L'intenzione dello standard è definire le condizioni necessarie per consentire il raggiungimento degli obiettivi di ISO 27001 in un ambiente di data centre.

EN 50600 è la serie di standard EN che disciplina la pianificazione, la progettazione, l'approvvigionamento, l'integrazione, l'installazione, l'operatività e la manutenzione delle strutture e delle infrastrutture all'interno dei data centre. Sebbene la serie EN 50600 fornisca disposizioni simili agli standard ISO 22237, non sono completamente allineati.

EN 50600 è una famiglia di standard in crescita, attualmente composta dalle seguenti parti:

- EN 50600-1, Concetti generali
- EN 50600-2-1, Costruzione di edifici
- EN 50600-2-2, Alimentazione e distribuzione di energia
- EN50600-2-3. Controllo ambientale
- EN 50600-2-4, Infrastruttura di cablaggio per telecomunicazioni
- EN 50600-2-5, Sistemi di sicurezza
- EN 50600-3-1, Informazioni gestionali e operative
- EN 50600-4-1, Panoramica e requisiti generali per gli indicatori di prestazione
- EN 50600-4-2, Efficienza nell'uso dell'energia
- EN 50600-4-3, Fattore di energia rinnovabile

EN 50600 prevede un sistema di classificazione basato sui criteri chiave di disponibilità, sicurezza ed efficienza energetica:

1. Classe di disponibilità: la classificazione AC è definita nelle aree di alimentazione, ventilazione e sistemi di condizionamento dell'aria e cablaggio;
2. Classe di protezione: la classificazione PC è definita per la prevenzione delle intrusioni, la protezione contro il fuoco, la protezione contro il fumo e la protezione contro i pericoli ambientali. Devono essere formate almeno tre classi di protezione;
3. Livello di granularità (GL): la capacità di operare in modo energeticamente efficiente è definita tramite qualità di misurazione e ambito di misurazione per i sistemi di ventilazione e condizionamento dell'aria. Lo standard differenzia tra tre livelli di granularità differenti.

Affinché la progettazione di un data center sia conforme a questo standard:

a. Deve essere completata un'analisi dei rischi aziendali;
b. Una classe AC appropriata deve essere selezionata utilizzando l'analisi del rischio aziendale;
c. Un PC adatto ai percorsi e agli spazi del data center;
d. Un livello adeguato di abilitazione dell'efficienza energetica, GL;
e. Devono essere applicati il processo e i principi di progettazione.

Nota: attualmente, i data center (di solito) non prendono in considerazione né la EN 50600 né la ISO 22237. I data center (come AWS, ...) sono generalmente certificati dall'istituto privato Uptime Institute (certificazione Tier) e/o secondo lo standard ANSI/TIA-942. Questi due schemi di certificazione sono considerati complementari.

Certificazione Uptime Institute Tier

Questo ente di certificazione privato applica i propri Standard Tier per la disponibilità del data center e le prestazioni complessive. Consente vari livelli di prestazioni che considerano sia l'ambiente costruito, sia

l'approccio e le prestazioni del team operativo. Sono definiti 4 livelli:

- Tier I - Capacità di base: sono necessari arresti completi del sito per lavori di manutenzione o riparazione. I guasti alla capacità o alla distribuzione influenzeranno il sito.
- Tier II - Componenti di capacità ridondanti: gli arresti completi del sito per manutenzione sono ancora necessari. I guasti alla capacità possono influenzare il sito. I guasti alla distribuzione influenzeranno il sito.
- Tier III - Manutenibile in parallelo: ogni componente di capacità e ogni percorso di distribuzione di un sito può essere rimosso per manutenzione o sostituzione programmata senza impattare le operazioni. Il sito è comunque esposto a guasti dell'attrezzatura o errori dell'operatore.
- Tier IV - Tollerante ai guasti: un singolo guasto dell'attrezzatura o un'interruzione del percorso di distribuzione non influenzerà le operazioni. Ad un sito tollerante ai guasti possono essere effettuate manutenzioni in modo continuo.

Standard ANSI/TIA-942 per infrastrutture di telecomunicazioni per data center

ANSI/TIA-942 è uno standard pubblicato dalla Telecommunications Industry Association (TIA) che fornisce linee guida per la progettazione e la costruzione di data center, inclusi sistemi di alimentazione, sistemi meccanici, architettura, sicurezza, sistemi di telecomunicazione, protezione antincendio e sicurezza. Lo standard è inteso a garantire che i data center siano affidabili, sicuri e scalabili per soddisfare le esigenze in continua evoluzione del settore IT.

ANSI/TIA-942 fornisce un quadro completo per la progettazione di data center, comprese raccomandazioni per la selezione del sito, la struttura dell'edificio, l'infrastruttura di cablaggio, i sistemi di raffreddamento e alimentazione, la sicurezza e la gestione.

ANSI/TIA-942 è utilizzato da progettisti, operatori e revisori di data center per garantire che i data center siano progettati e costruiti in modo da soddisfare le best practice e gli standard del settore. Lo standard è anche spesso citato da enti normativi e clienti per valutare l'affidabilità e la sicurezza dei data center.

Controlli di sistema e organizzazione (SOC) 2

SOC 2 è un insieme di standard sviluppati dall'American Institute of Certified Public Accountants (AICPA) per valutare e verificare la sicurezza, la disponibilità, l'integrità dell'elaborazione, la riservatezza e la privacy dei sistemi e dei dati di un'organizzazione di servizi.

Nota: mentre ISO/IEC 27001 è generico, SOC 2 è contestualizzato appositamente per i data center.

I report SOC 2 vengono utilizzati dalle organizzazioni di servizi (come i data center) per dimostrare ai propri clienti e alle parti interessate di aver implementato efficaci controlli interni per proteggere i propri dati sensibili.

I report SOC 2 si basano sui Trust Services Criteria (TSC), ovvero un insieme di principi e criteri utilizzati per valutare l'efficacia dei controlli di un'organizzazione di servizi sui propri sistemi e dati.

Esistono due tipi di report SOC 2: tipo I e tipo II. I report di Tipo I valutano la progettazione dei controlli di un'organizzazione di servizi, mentre i report di tipo II valutano l'efficacia di tali controlli in un periodo di tempo specificato.

Gli audit SOC 2 vengono condotti da revisori terzi indipendenti, certificati dall'AICPA.

Gli audit SOC 2 sono opzionali, ma stanno diventando sempre più importanti per le organizzazioni di servizi che desiderano dimostrare il proprio impegno nei confronti della sicurezza e della privacy.

Per prepararsi a un audit SOC 2, le organizzazioni di servizi devono condurre una valutazione dei rischi e implementare una serie completa di controlli per soddisfare i criteri dei servizi fiduciari.

Gli audit SOC 2 in genere comportano una combinazione di interviste, revisioni della documentazione e test di sistema per valutare l'efficacia dei controlli di un'organizzazione di servizi.

I rapporti SOC 2 includono un parere del revisore sull'efficacia dei controlli di un'organizzazione di servizi, nonché una descrizione dei controlli testati e delle eventuali carenze identificate.

I report SOC 2 possono essere condivisi con clienti, parti interessate e organismi di regolamentazione per garantire che un'organizzazione di servizi abbia implementato controlli efficaci per proteggere i dati sensibili.

Il report SOC 2 di tipo II è LA raccomandazione per gli aspetti di sicurezza informatica?

SOC 3 (Sistema di controllo dei dati)

SOC 3 è un tipo di report di attestazione che fornisce una panoramica di alto livello dei controlli di un'organizzazione in relazione a sicurezza, disponibilità, integrità dell'elaborazione, riservatezza e privacy.

A differenza dei report SOC 1 e SOC 2, che sono destinati ad un pubblico specifico e forniscono informazioni più dettagliate sui controlli di un'organizzazione, i report SOC 3 sono concepiti per un pubblico generale e forniscono un riepilogo dei controlli dell'organizzazione che può essere condiviso pubblicamente.

I report SOC 3 si basano sugli stessi controlli e criteri dei report SOC 2, ma non forniscono lo stesso livello di dettaglio. Invece, i report SOC 3 includono una breve descrizione del sistema e dei controlli dell'organizzazione, insieme a una dichiarazione di un revisore indipendente che attesta la conformità dell'organizzazione ai criteri SOC 2.

I report SOC 3 sono spesso utilizzati dalle organizzazioni per dimostrare il loro impegno verso la sicurezza e la conformità a clienti, partner e altri stakeholder. Poiché sono disponibili al pubblico, possono anche essere utilizzati da potenziali clienti o investitori per valutare l'impegno verso la sicurezza di un'organizzazione prima di fare affari con loro.

A2.6. Schemi di certificazione

Il Cyber Security Act (CSA, (UE) 2019/881) fornisce un quadro europeo per la certificazione della sicurezza informatica di prodotti, processi e servizi. L'ENISA, l'Agenzia dell'Unione Europea per la Sicurezza Informatica, ha il diritto di sviluppare schemi di certificazione della sicurezza informatica destinati ad essere utilizzati su base volontaria e validi in tutta l'Unione Europea. Il secondo schema intende coprire i Cloud Services (EUCS). È ancora in fase di preparazione alla data di stesura della presente guida. Si prevede che questo schema utilizzi il CEN/TS 18026 descritto sopra. Una volta disponibile, potrebbe rappresentare uno strumento utile per i CSP per dimostrare la sicurezza della propria soluzione e per il fornitore di servizi FSSS per rafforzare la fiducia nel CSP.

Data di pubblicazione: 14/02/2025

Euralarm
Gubelstrasse 22
CH-6301 Zugo (Svizzera)

Numero di registrazione commerciale svizzero:
CHE-222.522.503

E-mail: secretariat@euralarm.org
Sito web: www.euralarm.org