Asmenet S.c.a.r.l.

Piano della Sicurezza del Sistema di Conservazione

Registro delle Versioni

Azione	Data	Nominativo	Funzione
Redazione	02/05/2023	Cristina Falciano	Responsabile del servizio di conservazione
Verifica	10/05/2023	Cristina Falciano	Responsabile del servizio di conservazione
Approvazione		Cristina Falciano	Responsabile del servizio di conservazione

Sommario

1. SCOPO E AMBITO DEL DOCUMENTO

Ill presente documento costituisce il Piano della Sicurezza (PdS) di ASMENET S.C.A.R.L e ne descrive l'implementazione del Sistema di Gestione della Sicurezza Informatica (SGSI). esclusivamente per quanto attiene le attività di conservazione documentale ex DPCM 3 dicembre 2013 e, quindi, inerenti quanto definito nell'ambito del Codice dell'Amministrazione Digitale (D.Lgs. 7 marzo 2005, n. 82 e successive modificazioni). Pertanto, ogni indicazione contenuta nel PdS è da intendersi riferita, ove altrimenti non indicato, esclusivamente alle predette attività di conservazione documentale.

Il PdS fa riferimento ad una serie di documenti e procedure che devono essere utilizzati all'interno della organizzazione stessa. Nel seguito, si fa riferimento agli aspetti della norma ISO/IEC 27001, la cui certificazione è obbligatoria per l'accreditamento alla conservazione documentale e alle norme ISO/IEC 27001 e lo ETSI TS 101 533-01.Si considerano inoltre, a puro titolo di esempio, aspetti contemplati nella norma ISO 9001:2008, oltre che ad altre eventuali norme e/o dispositivi legislativi.

1.1. Dati identificativi del Conservatore

Denominazione	ASMENET S.C.A.R.L.
Indirizzo	Via G. Porzio, 4-IS G1 80143 Napoli (NA)
Direttore	Arch. Tarallo Gennaro
E-mail di riferimento	supporto@asmenet.it
N° telefono	081 7877540
Sito web istituzionale	https://www.asmenet.it/
E-mail istituzionale	supporto.asmenet@asmepec.it

Contesto di riferimento

Il 1° gennaio 2022 sono entrate in vigore le Linee guida sulla formazione, gestione e conservazione dei documenti informatici (da ora Linee Guida) emanate da Agenzia per l'Italia Digitale (da ora AgID) ai sensi dell'art. 71 del D. lgs 7 marzo 2005 n. 82 recante il Codice dell'Amministrazione Digitale (da ora CAD). Asmenet si configura conservatore degli oggetti digitali iscritto al marketplace di AgID in ragione della natura giuridica dei titolari dell'oggetto di conservazione e secondo quanto previsto dal regolamento sui criteri per la fornitura del servizio di conservazione dei documenti informatici. Il servizio di conservazione degli oggetti digitali è formalizzato mediante accordo di affidamento tra ogni titolare dell'oggetto di conservazione e il conservatore in cui si definiscono le specifiche relative alla conservazione.

1.2. Modifiche al documento

Il presente documento e i suoi riferimenti sono puntualmente aggiornati. L'attività di aggiornamento può essere realizzata in merito a modifiche applicative, funzionali e procedurali che hanno impatti architetturali, infrastrutturali e organizzativi sulla gestione del servizio. Il numero

delle versioni, le date e le modifiche apportate sono indicate nel "Registro delle versioni**Errore. L'origine riferimento non è stata trovata.**" a cui si rimanda.

2. NORMATIVA E STANDARD DI RIFERIMENTO

2.1. Normativa di riferimento

ASMENET S.C.A.R.L verifica periodicamente la presenza di aggiornamenti alla normativa. Le norme monitorate e applicabili sono:

- **Regolamento (UE) 910/2014 eIDAS**
  "in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno";
- **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 e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)", applicabile in tutti gli Stati membri a partire dal 25 maggio 2018;
- **Codice civile** (Libro Quinto del Lavoro, Titolo II del lavoro nell'impresa, Capo III delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili, art. 2215 bis) - Documentazione informatica;
- **Decreto legislativo 22 gennaio 2004, n. 42, e successive modificazioni**
  "Codice dei beni culturali e del paesaggio";
- **D. Lgs. 7 marzo 2005, n. 82, e s.m.i;**
  "Codice dell'Amministrazione digitale (CAD)";
- **DPCM 22 Febbraio 2013**
  "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali";
- **Decreto Ministero Economia e Finanze 17.06.2014**
  "Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82/2005";
- **Linee Guida AgID**
  "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici (G.U. n.259 del 19 ottobre 2020)";
- **Regolamento AgID sui criteri per la fornitura dei servizi di conservazione dei documenti informatici.**

2.2. Standard di riferimento

Così come richiesto dalle Linee Guida – AgID, e secondo quanto previsto dall'Allegato 4, di seguito si riportano gli standard adottati per la conservazione dei documenti informatici.

- **ISO 14721:2012 OAIS** (Open Archival Information System), Sistema informativo aperto per l'archiviazione;

- **ISO/IEC 27001:2013**, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- **ETSI TS 101 533-1 V1.3.1 (2012-04)** Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- **ETSI TR 101 533-2 V1.3.1 (2012-04)** Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- **UNI 11386:2020 Standard SInCRO** - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- **ISO 15836:2019** Information and documentation - The Dublin Core metadata element set, Sistema di metadati del Dublin Core.

Organizzazione del sistema di conservazione

Asmenet eroga servizi di conservazione digitale utilizzando soluzioni tecnologiche che soddisfano i requisiti di alta affidabilità, richiesti dalla normativa. Il modello organizzativo adottato dal conservatore è idoneo a gestire il servizio di conservazione in base a quanto stabilito dalle vigenti Linee Guida all'art. 4.3. Il sistema di conservazione opera secondo modelli organizzativi esplicitamente definiti che garantiscono la sua distinzione logica dal sistema di gestione documentale, se esistente. Il modello organizzativo del conservatore è stato realizzato secondo lo standard ISO 14721:2012 basato su una struttura organizzata di persone e sistemi, che accetti la responsabilità di conservare l'informazione e di renderla fruibile all'utente.
Di seguito sono indicati i ruoli dei soggetti incaricati nell'ambito del servizio di conservazione dei documenti informatici.

- ***Responsabile del servizio di conservazione**:* Cristina Falciano

La nomina è stata formalizzata in data 03/08/2020 e decorre dal giorno 03/08/2020. La nomina è stata firmata per accettazione dal responsabile designato.
Cronologia dei responsabili del servizio di conservazione.

Nome e Cognome	Funzione	Data nomina	Data Revoca
Cristina Falciano	Responsabile del servizio di conservazione	03/08/2020	//

- ***Responsabile della funzione archivistica di conservazione:*** Cristina Falciano

La nomina è stata formalizzata in data 03/08/2020 e decorre dal giorno 03/08/2020. La nomina è stata firmata per accettazione dal responsabile designato.
Cronologia dei responsabili della funzione archivistica di conservazione.

Nome e Cognome	Funzione	Data nomina	Data Revoca
Cristina Falciano	Responsabile della funzione archivistica di conservazione	03/08/2020	//

- ***Responsabile della sicurezza dei sistemi per la conservazione**:* Massimo Mazzella

La nomina è stata formalizzata in data 01/09/2021 e decorre dal giorno 01/09/2021. La nomina è stata firmata per accettazione dal responsabile designato.
Cronologia dei responsabili della sicurezza dei sistemi per la conservazione.

Nome e Cognome	Funzione	Data nomina	Data Revoca
Massimo Mazzella	Responsabile della sicurezza dei sistemi per la conservazione	01/09/2021	//

- ***Responsabile dei sistemi informativi per la conservazione:*** Massimo Mazzella

La nomina è stata formalizzata in data 01/09/2021 e decorre dal giorno 01/09/2021. La nomina è stata firmata per accettazione dal responsabile designato.
Cronologia dei responsabili dei sistemi informativi per la conservazione.

Nome e Cognome	Funzione	Data nomina	Data Revoca
Massimo Mazzella	Responsabile dei sistemi informativi per la conservazione	01/09/2021	//

- ***Responsabile dello sviluppo e della manutenzione del sistema di conservazione**:* Massimo Mazzella

La nomina è stata formalizzata in data 01/09/2021 e decorre dal giorno 01/09/2021. La nomina è stata firmata per accettazione dal responsabile designato.
Cronologia dei responsabili dello sviluppo e della manutenzione del sistema di conservazione.

Nome e Cognome	Funzione	Data nomina	Data Revoca
Massimo Mazzella	Responsabili dello sviluppo e della manutenzione del sistema di conservazione	01/09/2021	//

- **Responsabile del trattamento dei dati personali:** Ciro Pasquale Mancino

La nomina è stata formalizzata in data 05/04/2018 e decorre dal giorno 05/04/2018.

Nome e Cognome	Funzione	Data nomina	Data Revoca
Ciro Pasquale Mancino	Responsabile del trattamento dei dati personali	05/04/2018	//

Responsabile e incaricati al trattamento dei dati

Il conservatore Asmenet S.c.a.r.l., ogni qualvolta eroga servizi di conservazione, assume il ruolo di Responsabile del trattamento dei dati ai sensi dell'art. 28 del GDPR (così come stabilito inoltre dall'art. 3.9 delle Linee Guida AgID) e tutti i collaboratori autorizzati dal Responsabile del trattamento assumono il ruolo di incaricati del trattamento e vengono opportunamente istruiti in tal senso. I predetti ruoli sono nominati in conformità al Regolamento (UE) 2016/679 e alla normativa italiana (D.Lgs 196/2003 s.m.i.).

Perimetro del sistema di conservazione

L'impianto fisico del sistema di conservazione di Asmenet S.c.a.r.l. è situato in Europa, all'interno della struttura Google Cloud Platform, disponibile in diverse regioni, a partire da settembre 2018. Google Cloud Platform è disponibile in Europa. I dati saranno pertanto allocati in Europa, nel rispetto del GDPR 679/2016.

I sistemi infrastrutturali sono progettati per eliminare i singoli punti di guasto e ridurre al minimo l'impatto dei rischi ambientali previsti. I circuiti doppi, gli interruttori, le reti o altri dispositivi necessari contribuiscono a fornire questa ridondanza. I Servizi sono progettati in modo da consentire a Google di eseguire alcuni tipi di manutenzione preventiva e correttiva senza interruzioni. Tutte le apparecchiature e le strutture ambientali sono dotate di procedure di manutenzione preventiva documentate che descrivono in dettaglio il processo e la frequenza delle prestazioni in conformità alle specifiche del produttore o alle specifiche interne. La manutenzione preventiva e correttiva delle apparecchiature del data center è pianificata attraverso un processo di modifica standard secondo procedure documentate.

I sistemi di alimentazione elettrica dei data center sono progettati per essere ridondanti e soggetti a manutenzione senza impatto per le operazioni continue, 24 ore al giorno, 7 giorni alla settimana.

I server utilizzano un'implementazione basata su Linux personalizzata per l'ambiente applicativo.

I data center sono collegati tramite collegamenti privati ad alta velocità per fornire un trasferimento dati sicuro e veloce tra i centri dati.

Google utilizza più strati di dispositivi di rete e di rilevamento delle intrusioni per proteggere la sua superficie di attacco esterno. Google analizza i potenziali vettori di attacco e incorpora tecnologie appropriate nei sistemi a tutela da attacchi esterni.

Il rilevamento delle intrusioni ha lo scopo di fornire informazioni sulle attività di attacco in corso e di fornire informazioni adeguate per rispondere agli incidenti. Il rilevamento delle intrusioni di Google comporta:

- rigorosi controlli sulle dimensioni e sulla composizione della superficie d'attacco di Google attraverso misure preventive;
- utilizzo di controlli di rilevamento intelligenti nei punti di ingresso dati; e
- utilizzo di tecnologie che pongono automaticamente rimedio ad alcune situazioni di pericolo.

Google monitora una serie di canali di comunicazione per gli incidenti di sicurezza e il personale di sicurezza di Google reagisce prontamente agli incidenti noti.

Google mette a disposizione la crittografia HTTPS (chiamata anche connessione SSL o TLS). I server di Google supportano lo scambio di chiavi crittografiche effimere a curva ellittica Diffie-Hellman firmato con RSA ed ECDSA. Questi metodi di perfetta segretezza in avanti (PFS) aiutano a proteggere il traffico e a minimizzare l'impatto di una chiave compromessa, o di una svolta crittografica.

Politiche di sicurezza

Per ASMENET la sicurezza delle informazioni ha come obiettivo primario la protezione dei dati e delle informazioni, della struttura tecnologica, fisica, logica ed organizzativa, responsabile della loro gestione.

Questo significa ottenere e mantenere un sistema di gestione sicura delle informazioni, nell'ambito del campo di applicazione definito per l'ISMS, attraverso il rispetto delle seguenti proprietà:

1. **Riservatezza**: assicurare che l'informazione sia accessibile solamente ai soggetti e/o ai processi debitamente autorizzati;
2. **Integrità**: salvaguardare la consistenza dell'informazione da modifiche non autorizzate;
3. **Disponibilità**: assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architetturali associati quando ne fanno richiesta;
4. **Controllo**: assicurare che la gestione dei dati avvenga sempre attraverso processi e strumenti sicuri e testati;
5. **Autenticità**: garantire una provenienza affidabile dell'informazione.
6. **Privacy**: garantire la protezione ed il controllo dei dati personali.

Nell'ambito della gestione dei servizi offerti da ASMENET, attraverso la propria infrastruttura tecnologica, l'osservanza dei livelli di sicurezza stabiliti attraverso l'implementazione dell'ISMS, assicura:

- la garanzia di aver incaricato un partner affidabile al trattamento del proprio patrimonio informativo;
- un'elevata immagine aziendale;
- la completa osservanza delle Service Level Agreement stabilite, ove previsto, con i clienti;
- la soddisfazione del cliente;
- il rispetto delle normative vigenti e degli standard internazionali di sicurezza.

Per questo motivo ASMENET ha sviluppato un sistema di gestione sicura delle informazioni seguendo i requisiti specificati della Norma ISO 27001 e delle leggi cogenti come mezzo per gestire la sicurezza delle informazioni nell'ambito della propria attività.
ASMENET assicura attraverso la sua politica di sicurezza delle informazioni la protezione degli asset dell'organizzazione accessibili da parte dei fornitori.
La politica della sicurezza di ASMENET rappresenta l'impegno dell'organizzazione nei confronti di clienti e terze parti a garantire la sicurezza delle informazioni, degli strumenti fisici, logici e organizzativi atti al trattamento delle informazioni in tutte le attività.

Gestione degli incidenti

Per "incidenti di sicurezza delle informazioni" s'intende un evento avverso che ha causato o ha il potenziale di causare danni agli assets, alla reputazione e/o al personale dell'organizzazione, attraverso l'intrusione, la compromissione e l'abuso di informazioni e risorse.
Quindi è la realizzazione di una delle minacce analizzate nel Risk Assessment dell'organizzazione.

Le principali categorie di incidente sono:

Livello	Classe incidente	Esempi	Descrizione	Responsabilità
1	ORDINARIO	• Tentata penetrazione delle difese • spedizione email non appropriate senza	L'incidente non provoca disservizi significativi e l'impatto	Responsabile del servizio o suo delegato

Livello	Classe incidente	Esempi	Descrizione	Responsabilità
		comunicazione di informazioni	sull'operatività della Società non è rilevante. L'evento è risolvibile con mezzi di intervento ordinari	Comunicazione da chi ha rilevato incidente entro 48 ore al Resp. del servizio o suo delegato
2	SIGNIFICATIVO	• Spedizioni email non appropriate con comunicazione di informazioni non riservate a non autorizzati a riceverle • Tentata penetrazione delle difese con rischio di blocco	Degrado Interruzione di una percentuale minoritaria (< 25%) del servizio per cui lo stesso continua ad essere erogato anche se in modalità rallentata	Responsabile del servizio o suo Delegato Comunicazione da chi ha rilevato incidente entro 8 ore al Resp. del servizio o suo delegato
3	GRAVE	• uso di un software privo di licenza • accesso e/o uso non autorizzato dei dati di accesso di un altro utente	Degrado o interruzione di una percentuale da media a elevata (26% < x < 55%) del servizio per cui lo stesso continua ad essere erogato ma causando gravi disservizi	Comunicazione da chi ha rilevato incidente entro 4 ore al Resp. Continuità Operativa che a sua discrezione definisce le azioni da intraprendere
4	DISASTROSO	• furto di documenti • computer infettato da virus • attacco haker	Incidente che causa l'interruzione di una percentuale da elevata a completa del servizio (56% < x < 100%)	Avvertire immediatamente il Comitato di crisi che deve intervenire per definire le azioni da attuare

L'organizzazione riconosce che ci sono dei rischi associati all'accesso degli utenti e alla gestione delle informazioni nello svolgimento delle proprie attività, infatti questa politica mira a:

- Ridurre l'impatto delle violazioni di sicurezza, assicurando che gli incidenti siano seguiti correttamente.
- Aiutare a identificare le aree di miglioramento per ridurre il rischio e l'impatto di futuri incidenti.
- Ridurre il numero degli incidenti

Gli incidenti potrebbero avere un impatto significativo sull'efficienza del funzionamento dell'organizzazione e causare perdite finanziarie, multe e l'impossibilità di fornire i servizi necessari agli interessati del trattamento.

Un incidente può e deve essere **rilevato**:

- ✓ Dal personale operativo nello svolgimento delle proprie attività.
- ✓ Dall'avviso automatico dei dispositivi che monitorano le proprie attività di sistema.
- ✓ Dall' utente finale.

Successivamente viene determinato rapidamente e con precisione se l'incidente è un incidente grave.

- ✓ Raccolta dati del problema iniziale - I dati sono raccolti e viene fatta un'appropriata classificazione dell'Impatto.
- ✓ Valutazione dell'Incidente - l'incidente è valutato e la relativa categoria è confermata dal Responsabile della Sicurezza delle informazioni.
- ✓ Incidente Grave o Disastroso - Se l'incidente è classificato come 'Disastroso o Grave, la valutazione deve essere confermata entro 60 minuti dalla rilevazione.

Il processo di comunicazione, poi, ha lo scopo di garantire che tutte le parti siano informate dello stato dell'incidente.

- ✓ I Responsabili di progetto e/o le parti coinvolte devono essere informati dell'incidente e tenuti aggiornati sui relativi progressi per consentire loro di gestire i dati degli interessati.
- ✓ In casi di incidente disastroso o incidente grave la Direzione deve essere informata e tenuta aggiornata.
- ✓ Qualora la violazione possa comportare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare di trattamento notifica al Garante entro 72h dal momento in cui ne è venuto a conoscenza. (Vedi Comunicazione Data Breach al Garante definita nel sistema documentale GDPR).

Il registro Incidenti e quasi Incidenti riassume gli eventi dell'incidente, l'impatto, le azioni intraprese per risolvere l'incidente e le ulteriori misure adottate per ridurre il rischio di accadimento futuro/impatto.

Elenco delle procedure di sicurezza per la conservazione

Di seguito sono elencate tutte le procedure afferenti la sicurezza del sistema di conservazione dei documenti informatici:

Area "Politiche per la sicurezza delle informazioni"		
O/C	**Procedura**	**Descrizione della procedura**
Obiettivo	**Indirizzi della direzione per la sicurezza delle informazioni**	
Controllo	Politiche per la sicurezza delle informazioni	La direzione approva, pubblica e trasmette a tutti i dipendenti nonché alle terze parti interessate un documento di politica per la sicurezza delle informazioni.
Controllo	Riesame della politica per la sicurezza delle informazioni	La politica per la sicurezza delle informazioni è riesaminata in concomitanza di cambiamenti significativi e comunque periodicamente nell'ambito del Riesame della Direzione, per assicurare la sua perdurante idoneità, adeguatezza ed efficacia

Area “Organizzazione della sicurezza delle informazioni”		
O/C	**Procedura**	**Descrizione della Procedura**
Obiettivo	**Organizzazione interna**	
Controllo	Ruoli e responsabilità per la sicurezza delle informazioni	La direzione richiede che i dipendenti, i collaboratori e gli utenti di terze parti applichino le norme di sicurezza nel rispetto delle politiche e delle procedure vigenti nell'organizzazione.
Controllo	Separazione dei compiti	I compiti e le aree di responsabilità sono separati, attraverso l’uso della profilazione degli accessi, per ridurre le occasioni di modifica non autorizzata o incidentale o l'uso improprio dei beni dell'organizzazione.
Controllo	Contatti con le autorità	I contatti con le autorità competenti sono mantenuti nel rispetto degli obblighi di legge.
Controllo	Contatti con gruppi specialistici	L'organizzazione mantiene rapporti con consulenti e gruppi specialistici nell'ambito della gestione della sicurezza delle informazioni
Controllo	Sicurezza delle informazioni nella gestione dei progetti	L'organizzazione ha adottato una politica sulla sicurezza delle informazioni nella gestione dei progetti volta alla definizione di specifici obblighi contrattuali
Obiettivo	**Dispositivi portatili e telelavoro**	
Controllo	Politica per i dispositivi portatili	L'organizzazione ha adottato una politica una politica e delle misure di sicurezza a suo supporto per la gestione dei rischi introdotti dall’uso di dispositivi portatili
Controllo	Telelavoro	L'organizzazione ha adottato una politica e delle misure di sicurezza r proteggere le informazioni gestite nelle eventuali attività di telelavoro
Area “Sicurezza delle risorse umane”		
O/C	**Procedura**	**Descrizione della Procedura**
Obiettivo	**Prima dell’impiego**	
Controllo	Screening	L'organizzazione procede alla selezione del personale in accordo alla misure in essere per la P.A.
Controllo	Termini e condizioni di impiego	L'organizzazione assegna responsabilità relativamente alla sicurezza delle informazioni tramite specifiche lettere di incarico
Obiettivo	**Durante l’impiego**	
Controllo	Responsabilità della direzione	La direzione richiede a tutto il personale e ai collaboratori di applicare le politiche, le procedure e tutte le misure necessarie alla sicurezza delle informazioni
Controllo	Consapevolezza, istruzione, formazione e addestramento sulla sicurezza delle informazioni	L'organizzazione assicura che tutto il personale ed i collaboratori siano adeguatamente sensibilizzati sulle politiche e procedure in essere, e pianifica le necessarie attività di

		istruzione, formazione e addestramento coerentemente alla attività lavorativa svolta dagli stessi.
Controllo	Processo disciplinare	Esiste un processo disciplinare formale per gli impiegati che hanno commesso una violazione di sicurezza
Obiettivo	**Cessazione e variazione del rapporto di lavoro**	
Controllo	Cessazione o variazione delle responsabilità durante il rapporto di lavoro	Le responsabilità per interrompere o variare un impiego sono chiaramente definite e assegnate. Ad ogni interruzione di rapporto di lavoro o di cambio mansione l'AdS aggiorna le autorizzazioni agli accessi ed ai profili autorizzati.

Area "Gestione degli asset"

O/C	Procedura	Descrizione della Procedura
Obiettivo	**Responsabilità per gli asset**	
Controllo	Inventario degli asset	L'organizzazione ha definito un Asset Inventory, sottoposto a regolare aggiornamento
Controllo	Responsabilità degli asset	L'Asset Inventory identifica il responsabile di ciascun asset
Controllo	Utilizzo accettabile degli asset	La direzione ha approvato la politica d'utilizzo accettabile degli asset
Controllo	Restituzione degli asset	Tutti i dipendenti, i collaboratori e gli utenti di terze parti restituiscono ogni bene dell'organizzazione in loro possesso al termine del loro contratto o accordo d'impiego. Apparati dimessi o trasferiti a terzi sono posti a trattamento di eliminazione sicura di tutte le informazioni precedentemente contenute.
Obiettivo	**Classificazione delle informazioni**	
Controllo	Classificazione delle informazioni	L'organizzazione ha adottato una politica di classificazione delle informazioni in base agli obblighi normativi
Controllo	Etichettatura delle informazioni	La politica di classificazione delle informazioni adottata definisce la modalità di etichettatura delle informazioni
Controllo	Trattamento degli asset	Gli asset sono trattati secondo procedure sviluppate in base allo schema di classificazione
Obiettivo	**Trattamento dei supporti**	
Controllo	Gestione dei supporti rimovibili	L'organizzazione ha adottato procedure che definiscono le modalità d'uso consentito e/o vietato dei supporti rimovibili
Controllo	Dismissione dei supporti	L' analisi dei rischi è stata impiegata per definire la modalità di gestione della dismissione dei supporti all'interno delle politiche per la gestione degli asset
Controllo	Trasporto dei supporti fisici	L' analisi dei rischi è stata impiegata per definire la modalità di trasporto dei supporti all'interno delle politiche per la gestione degli asset

Area “Controllo degli accessi”		
O/C	**Procedura**	**Descrizione della Procedura**
Obiettivo	**Requisiti di business per il controllo degli accessi**	
Controllo	Politica di controllo degli accessi	L'organizzazione ha adottato procedure che definiscono le modalità di controllo degli accessi sulla base della classificazione delle informazioni, la loro etichettatura e la gestione dei rischi
Controllo	Accesso alle reti e ai servizi di rete	Le modalità di approvazione delle assegnazioni e/o revoche degli accessi, da parte degli utenti, alle reti e i servizi in rete sono sottoposti al vaglio della direzione
Obiettivo	**Gestione degli accessi degli utenti**	
Controllo	Registrazione e de-registrazione degli utenti	La politica della sicurezza dei dati definisce le modalità di gestione del processo di registrazione e de-registrazione per abilitare l'assegnazione dei diritti di accesso
Controllo	Provisioning degli accessi degli utenti	La politica della sicurezza dei dati definisce le modalità di gestione del processo di assegnazione e revoca dei diritti di accesso agli utenti
Controllo	Gestione dei diritti di accesso privilegiato	La modalità di approvazione delle assegnazioni e/o revoche degli accessi privilegiati, alla reti ed ai servizi in rete sono sottoposti al vaglio della direzione.
Controllo	Gestione delle informazioni segrete di autenticazione degli utenti	La modalità di assegnazione di informazioni segrete di autenticazione, per l'accesso alle reti ed ai servizi in rete sono condotte in conformità con le politiche approvate dalla Direzione.
Controllo	Riesame dei diritti di accesso degli utenti	La direzione conduce ad intervalli regolari sessioni di riesame dei diritti di accesso degli utenti
Controllo	Rimozione o adattamento dei diritti di accesso	All'atto della cessazione del rapporto di lavoro, del contratto o accordo, oppure in occasione di ogni variazione organizzativa, i diritti di accesso vengono adattati o rimossi al fine di mantenere l'adeguato livello di sicurezza.
Obiettivo	**Responsabilità dell'utente**	
Controllo	Utilizzo delle informazioni segrete di autenticazione	L'organizzazione assegna responsabilità relativamente alla sicurezza delle informazioni tramite apposite procedure
Obiettivo	**Controllo degli accessi ai sistemi e alle applicazioni**	
Controllo	Limitazione dell’accesso alle informazioni	L'organizzazione adotta misure di gestione per l'assegnazione e il controllo degli accessi
Controllo	Procedure di log-on sicure	L'organizzazione adotta sistemi di log-on sicuri secondo gli standard
Controllo	Sistema di gestione delle password	L'organizzazione adotta gestione delle password secondo gli standard normativi

Controllo	Uso di programmi di utilità privilegiati	L'organizzazione adotta misure di sicurezza mirate a limitare l'accesso a strumenti d'utilità che potrebbero aggirare I controlli applicativi
Controllo	Controllo degli accessi al codice sorgente dei programmi	L'organizzazione adotta la segmentazione delle infrastrutture a protezione degli accessi alle risorse

Area "Crittografia"

O/C	Procedura	Descrizione della Procedura
Obiettivo	**Controlli crittografici**	
Controllo	Politica sull'uso dei controlli crittografici	L'organizzazione adotta misure di sicurezza in conformità con la normativa vigente con eventuali miglioramenti introdotti dalla rivalutazione dei rischi
Controllo	Gestione delle chiavi	L'organizzazione adotta la gestione delle chiavi di accesso

Area "Sicurezza fisica e ambientale"

Per ogni obiettivo esistono più controlli e per ogni controllo più linee guida. A partire dalle linee guida, ove applicabili, inserire un commento ed eventuali evidenze (documenti, procedure, istruzioni operative, registrazioni, prassi documentate, test, ecc.).
Per ogni controllo inserire un commento di sintesi. Nel caso in cui un controllo o una linea guida non risultassero applicabili inserire le motivazioni.

O/C	Procedura	Descrizione della Procedura
Obiettivo	**Aree sicure**	
Controllo	Perimetro di sicurezza fisica	L'organizzazione adotta misure di sicurezza fisica proporzionali alla valutazione dei rischi, rivalutandone periodicamente l'efficacia
Controllo	Controlli di accesso fisico	L'organizzazione ha adottato fornitori che nativamente adottano procedure e sistemi di controllo degli accessi fisici per quanto riguarda gli asset considerati ad alto rischio. Il solo personale autorizzato ha la possibilità di accedere agli impianti
Controllo	Rendere sicuri uffici, locali e strutture	L'organizzazione ha adottato sistemi di controllo degli accessi fisici per quanto riguarda I locali
Controllo	Protezione contro minacce esterne ed ambientali	L'organizzazione adotta
Controllo	Lavoro in aree sicure	L'organizzazione adotta misure di compartimentazione delle risorse e degli addetti ai lavori in rispetto delle normative e in base alla valutazione del rischio
Controllo	Aree di carico e scarico	La sede operativa dell'organizzazione dispone di aree specifiche protette e gestite a garanzia di eventuali esposizioni ad accessi non autorizzati. Le infrastrutture
Obiettivo	**Apparecchiature**	
Controllo	Disposizione delle apparecchiature e loro protezione	L'organizzazione adotta il posizionamento delle apparecchiature in base al loro livello esposizione al rischio

Controllo	Infrastrutture di supporto	L'organizzazione adotta misure di protezione in conformità con la normativa vigente
Controllo	Sicurezza dei cablaggi	L'organizzazione adotta l'uso di impianti rispondenti agli standard tecnologici al fine di prevenire il verificarsi di eventi di
Controllo	Manutenzione delle apparecchiature	L'organizzazione si avvale di fornitori specializzati per le attività di manutenzione delle proprie apparecchiature
Controllo	Trasferimento degli asset	Lo spostamento degli asset è sottoposto all'approvazione della Direzione
Controllo	Sicurezza delle apparecchiature e degli asset all'esterno delle sedi	L'organizzazione affida l'housing delle proprie infrastrutture critiche a fornitori di servizi rispondenti alle esigenze in termini di standard di sicurezza
Controllo	Dismissione sicura o riutilizzo delle apparecchiature	Le apparecchiature oggetto di dismissione o di riallocazione sono gestite secondo il processo di gestione dei cambiamenti
Controllo	Apparecchiature incustodite degli utenti	L'organizzazione adotta misure di prevenzione atte ad evitare l'accesso ad apparecchiature lasciate incustodite con relativa formazione del personale
Controllo	Politica di schermo e scrivania puliti	L'organizzazione adotta misure di prevenzione atte ad evitare l'accesso ad informazioni lasciate incustodite nel perimetro delle postazioni di lavoro con relativa formazione del personale

Area "Sicurezza delle attività operative"

O/C	**Procedura**	**Descrizione della Procedura**
Obiettivo	**Procedure operative e responsabilità**	
Controllo	Procedure operative documentate	devono essere documentate e rese disponibili delle procedure operative a tutti gli utenti che ne necessitano
Controllo	Gestione dei cambiamenti	La direzione approva, pubblica e trasmette a tutti i dipendenti nonché alle terze parti interessate la politica per la gestione dei cambiamenti
Controllo	Gestione della capacità	La direzione adotta sistemi di monitoraggio e politiche per la stima dei fabbisogni
Controllo	Separazione degli ambienti di sviluppo, test e produzione	La direzione approva, pubblica e trasmette a tutti i dipendenti nonché alle terze parti interessate la politica per la gestione dei cambiamenti
Obiettivo	**Protezione dal malware**	
Controllo	Controlli contro il malware	In base alle normative vigenti l'organizzazione adotta strumenti di protezione contro possibili fonti malware
Obiettivo	**Backup**	
Controllo	Backup delle informazioni	La direzione approva, pubblica e trasmette a tutti i dipendenti nonché alle terze parti interessate la politica per la gestione dei backup

Obiettivo	**Raccolta di log e monitoraggio**	
Controllo	Raccolta di log degli eventi	La direzione adotta sistemi di raccolta di log protetti da manomissioni in rispondenza alle direttive normative e attua politica di protezione di tali dati da eventuali manomissioni
Controllo	Protezione delle informazioni di log	La direzione adotta sistemi di raccolta di log protetti da manomissioni in rispondenza alle direttive normative e attua politica di protezione di tali dati da eventuali manomissioni
Controllo	Log di amministratori e operatori	La direzione adotta sistemi di raccolta di log protetti da manomissioni in rispondenza alle direttive normative e attua politica di protezione di tali dati da eventuali manomissioni
Controllo	Sincronizzazione degli orologi	La direzione adotta, in base ai termini di legge l'uso di servizi di sincronizzazione a valore legale
Obiettivo	**Controllo del software di produzione**	
Controllo	Installazione del software sui sistemi di produzione	La direzione adotta una politica di gestione dei cambiamenti al fine di garantire la corretta attuazione sugli ambienti di produzione
Obiettivo	**Gestione delle vulnerabilità tecniche**	
Controllo	Gestione delle vulnerabilità tecniche	Le attività di VA sono pianificate e comunque condotte in caso di cambiamenti significativi ai sistemi informativi. I risultati di tali test sono tempestivamente comunicati al fine di gestire le vulnerabilità emerse.
Controllo	Limitazioni all'installazione del software	Gli amministratori di sistema sono chiamati a rispettare politiche di gestione dei cambiamenti atte a governare l'installazione di software
Obiettivo	**Considerazioni sull'audit dei sistemi informativi**	
Controllo	Controlli per l'audit dei sistemi informativi	Le attività di audit sui dei sistemi di produzione vengono pianificate coinvolgendo i responsabili dei processi e AdS in modo da minimizzare i rischi di interferenza con i processi.

Area "Sicurezza delle comunicazioni"

O/C	**Procedura**	**Descrizione della Procedura**
Obiettivo	**Gestione della sicurezza della rete**	
Controllo	Controlli di rete	L'organizzazione adotta sistemi di controllo della rete al fine di limitare il rischio di esposizione a problemi di sicurezza dei sistemi
Controllo	Sicurezza dei servizi di rete	L'organizzazione adotta strumenti atti a proteggere gli elementi connessi in rete
Controllo	Segregazione nelle reti	L'organizzazione adotta la segmentazione delle infrastrutture a protezione degli accessi alle risorse
Obiettivo	**Trasferimento delle informazioni**	

Controllo	Politiche e procedure per il trasferimento delle informazioni	La direzione adotta una politica di gestione della sicurezza delle informazioni con relativa trasmissione al personale addetto e gli eventuali attori esterni
Controllo	Accordi per il trasferimento delle informazioni	La direzione adotta una politica di gestione della sicurezza delle informazioni con relativa trasmissione al personale addetto e gli eventuali attori esterni
Controllo	Accordi per il trasferimento delle informazioni	La direzione adotta una politica di gestione della sicurezza delle informazioni con relativa comunicazione al personale addetto e gli eventuali attori esterni
Controllo	Accordi di riservatezza o di non divulgazione	L'organizzazione stabilisce accordi di riservatezza con gli attori esterni chiamati a gestire informazioni non necessariamente pubbliche
Area "Acquisizione, sviluppo e manutenzione dei sistemi"		
O/C	**Procedura**	**Descrizione della Procedura**
Obiettivo	**Requisiti di sicurezza dei sistemi informativi**	
Controllo	Analisi e specifica dei requisiti per la sicurezza delle informazioni	Nell'ambito della politica di gestione dei cambiamenti l'organizzazione include aspetti specifici mirati a definire e valutare le azioni mirate a minimizzare le problematiche di sicurezza delle informazioni
Controllo	Sicurezza dei servizi applicativi su reti pubbliche	Nell'ambito della politica di gestione dei cambiamenti l'organizzazione include aspetti specifici mirati a definire e valutare le azioni mirate a minimizzare le problematiche di sicurezza delle informazioni
Controllo	Protezione delle transazioni dei servizi applicativi	Nell'ambito della politica di gestione dei cambiamenti l'organizzazione include aspetti specifici mirati a definire e valutare le azioni mirate a minimizzare le problematiche di sicurezza delle informazioni
Obiettivo	**Sicurezza nei processi di sviluppo e supporto**	
Controllo	Politica per lo sviluppo sicuro	Nell'ambito della politica di gestione dei cambiamenti l'organizzazione include aspetti specifici mirati a definire e valutare le azioni mirate a minimizzare le problematiche di sicurezza delle informazioni
Controllo	Procedure per il controllo dei cambiamenti di sistema	Nell'ambito della politica di gestione dei cambiamenti l'organizzazione include aspetti specifici mirati a definire e valutare le azioni mirate a minimizzare le problematiche di sicurezza delle informazioni
Controllo	Riesame tecnico delle applicazioni in seguito a cambiamenti nelle piattaforme operative	Nell'ambito della politica di gestione dei cambiamenti l'organizzazione include aspetti specifici mirati a definire e valutare le azioni mirate a minimizzare le problematiche di sicurezza delle informazioni
Controllo	Limitazioni ai cambiamenti dei pacchetti software	Nell'ambito della politica di gestione dei cambiamenti l'organizzazione include aspetti specifici mirati a definire e

		valutare le azioni mirate a minimizzare le problematiche di sicurezza delle informazioni
Controllo	Principi per l'ingegnerizzazione sicura dei sistemi	Nell'ambito della politica di gestione dei cambiamenti l'organizzazione include aspetti specifici mirati a definire e valutare le azioni mirate a minimizzare le problematiche di sicurezza delle informazioni
Controllo	Ambiente di sviluppo sicuro	L'uso degli ambienti di sviluppo vengono regolamentati in modo da garantire la rispondenza alle politiche di sviluppo sicuro
Controllo	Sviluppo affidato all'esterno	L'organizzazione nell'affidare a fornitori esterni le attività di sviluppo del software impone, attraverso le proprie politiche, la definizione sotto forma di accordi contrattuali dei requisiti e delle politiche che il fornitore è tenuto a rispettare
Controllo	Test di sicurezza dei sistemi	All'interno della gestione del processo di gestione dei cambiamenti, definito attraverso apposita politica, viene definita l'obbligatorietà della definizione e l'esecuzione di test
Controllo	Test di accettazione dei sistemi	All'interno della gestione del processo di gestione dei cambiamenti, definito attraverso apposita politica, viene definita l'obbligatorietà della definizione e l'esecuzione di test
Obiettivo	**Dati di test**	
Controllo	Protezione dei dati di test	L'organizzazione vieta l'uso di dati reali per l'esecuzione di test in ambienti non qualificati con livelli di sicurezza adeguati

Area "Relazioni con i fornitori"

O/C	**Procedura**	**Descrizione della Procedura**
Obiettivo	**Sicurezza delle informazioni nelle relazioni con i fornitori**	
Controllo	Politica per la sicurezza delle informazioni nei rapporti con i fornitori	E' definita una politica di gestione dei rapporti con i fornitori che specifica i requisiti di sicurezza che gli stessi sono tenuti a rispettare. Tali requisiti sono anche definiti attraverso specifiche clausole negli accordi contrattuali.
Controllo	Indirizzare la sicurezza all'interno degli accordi con i fornitori	E' definita una politica di gestione dei rapporti con i fornitori che specifica i requisiti di sicurezza che gli stessi sono tenuti a rispettare. Tali requisiti sono anche definiti attraverso specifiche clausole negli accordi contrattuali.
Controllo	Filiera di fornitura per l'ICT (Information and Comunication Technology)	Gli accordi contrattuali inerenti la gestione dei rischi relativi alla sicurezza delle informazioni contemplano il trasferimento degli obblighi alla filiera di fornitura.
Obiettivo	**Gestione dell'erogazione dei servizi dei fornitori**	
Controllo	Monitoraggio e riesame dei servizi dei fornitori	La direzione riesamina periodicamente i livelli di erogazione dei servizi da parte dei fornitori. La direzione definisce inoltre le modalità di monitoraggio dell'operato e le sessioni di audit da condurre.

Controllo	Gestione dei cambiamenti ai servizi dei fornitori	L'organizzazione adotta procedure per la gestione del cambiamento, che contemplano la gestione dei cambiamenti ai servizi dei fornitori. Tali procedure tengono conto della criticità del business, dei sistemi e dei processi coinvolti.
Area "Gestione degli incidenti relativi alla sicurezza delle informazioni"		
O/C	**Procedura**	**Descrizione della Procedura**
Obiettivo	**Gestione degli incidenti relativi alla sicurezza delle informazioni e dei miglioramenti**	
Controllo	Responsabilità e procedure	L'organizzazione adotta procedure per la gestione di incidenti legati alla sicurezza
Controllo	Segnalazione degli eventi relativi alla sicurezza delle informazioni	L'organizzazione adotta misure di comunicazione in ottemperanza con le vigenti norme
Controllo	Segnalazione dei punti di debolezza relativi alla sicurezza delle informazioni	L'organizzazione adotta procedure per la gestione di incidenti legati alla sicurezza
Controllo	Valutazione e decisione sugli eventi relativi alla sicurezza delle informazioni	L'organizzazione adotta procedure per la gestione di incidenti legati alla sicurezza
Controllo	Risposta agli incidenti relativi alla sicurezza delle informazioni	L'organizzazione adotta procedure per la gestione di incidenti legati alla sicurezza
Controllo	Apprendimento dagli incidenti relativi alla sicurezza delle informazioni	A seguito di incidenti relativi alla sicurezza delle informazioni, è condotta un'analisi sulle cause degli stessi per definire le azioni volte non solo alla loro risoluzione, ma anche alla loro correzione e prevenzione di eventi simili.
Controllo	Raccolta di evidenze	La gestione degli incidenti è opportunamente documentata raccogliendo le informazioni utili quali evidenze degli incidenti e del processo di gestione degli stessi
Area "Aspetti relativi alla sicurezza delle informazioni nella gestione della continuità operativa"		
O/C	**Procedura**	**Descrizione della Procedura**
Obiettivo	**Continuità della sicurezza delle informazioni**	
Controllo	Pianificazione della continuità della sicurezza delle informazioni	L'organizzazione adotta una politica per la business continuity e la gestione del disaster recovery
Controllo	Attuazione della continuità della sicurezza delle informazioni	L'organizzazione adotta una politica per la business continuity e la gestione del disaster recovery
Controllo	Verifica, riesame e valutazione della continuità della sicurezza delle informazioni	L'organizzazione adotta una politica per la business continuity e la gestione del disaster recovery in cui viene previsto il riesame periodico e l'adeguamento legato al processo di gestione dei cambiamenti
Obiettivo	**Ridondanze**	

Controllo	Disponibilità delle strutture per l'elaborazione delle informazioni	L'organizzazione adotta in sede di rivalutazione delle esigenze e delle stime capacitive
Area "Conformità"		
O/C	**Procedura**	**Descrizione della Procedura**
Obiettivo	**Conformità ai requisiti cogenti e contrattuali**	
Controllo	Identificazione della legislazione applicabile e dei requisiti contrattuali	L'organizzazione individua, documenta e mantiene aggiornati tutti i requisiti cogenti e contrattuali pertinenti.
Controllo	Diritti di proprietà intellettuale	L'organizzazione attua procedure volte a garantire la conformità ai requisiti cogenti e contrattuali per l'uso del materiale sul quale insistono diritti di proprietà intellettuale e per l'uso di prodotti software proprietari.
Controllo	Protezione delle registrazioni	Le registrazioni sono protette da perdita, distruzione, falsificazione, accesso non autorizzato e rilascio non autorizzato in conformità ai requisiti cogenti, contrattuali e di business.
Controllo	Privacy e protezione dei dati personali	L'organizzazione si è dotata di un sistema della protezione dei dati conforme al Reg. UE 2016/679, definendo ed assegnando anche il ruolo di DPO.
Controllo	Regolamentazione sui controlli crittografici	I controlli crittografici sono utilizzati nel rispetto degli accordi, della legislazione e dei regolamenti pertinenti.
Obiettivo	**Riesami della sicurezza delle informazioni**	
Controllo	Riesame indipendente della sicurezza delle informazioni	La gestione della sicurezza delle informazioni e la sua attuazione sono riesaminati in modo indipendente ad intervalli pianificati. In ogni caso, il riesame è condotto qualora si attuino cambiamenti significativi.
Controllo	Conformità alle politiche e alle norme per la sicurezza	La direzione sottopone regolarmente a riesame la conformità dei processi di elaborazione delle informazioni rispetto alle politiche, alle norme e ai requisiti per la sicurezza..
Controllo	Verifica tecnica della conformità	I sistemi informativi sono periodicamente riesaminati per riscontrare la loro conformità con le politiche e con le norme per la sicurezza.
Area "CLOUD SERVICE (27017)"		
O/C	**Procedura**	**Descrizione della Procedura**
Obiettivo	**Responsabilità negli assets**	
Controllo	Inventario degli asset	Per gli asset fisici gestiti da ASMENET, sono inventariati e sono assegnate le responsabilità per la loro gestione. Gli asset immateriali (es. dati dei clienti; SW, ….) sono gestiti in accordo alle politiche

		Per gli asset di proprietà del fornitore del servizio Cloud, il controllo è demandato al fornitore del servizio Cloud.
Controllo	Proprietà degli asset	Gli asset sono di proprietà del fornitore del servizio Cloud
Controllo	Uso accettabile degli asset	La direzione ha approvato la politica di sicurezza di gestione del Servizio Cloud
Controllo	Restituzione degli asset	Gli asset del Cloud sono di proprietà del fornitore del servizio Cloud e gestiti dallo stesso Per gli asseti di proprietà, vedi A.8.1.4 (27001)
Controllo	Gestione chiusura contratto assets	E' fornita una descrizione documentata del processo di cessazione del servizio da parte del fornitore di servizi cloud.
Obiettivo	**Controllo degli accessi sui dati disponibili su ambienti virtuali condivisi**	
Controllo	Segregazione ambienti virtuali	La configurazione predefinita del servizio Cloud, prevede la segregazione logica delle VM, il che impedisce qualsiasi tipo di comunicazione, se non espressamente autorizzato.
Controllo	Potenziamento macchine virtuali	Su indicazione del fornitore del Software specifico, si predispongono le risorse minime da assegnare alla VM e le relative politiche di Firewalling.
Obiettivo	**Procedure operative e responsabilità**	
Controllo	Procedure operative documentate	devono essere documentate e rese disponibili delle procedure operative a tutti gli utenti che ne necessitano
Controllo	Gestione dei cambiamenti	La direzione approva, pubblica e trasmette a tutti i dipendenti nonché alle terze parti interessate la politica per la gestione dei cambiamenti
Controllo	Gestione della capacità	La direzione adotta sistemi di monitoraggio e politiche per la stima dei fabbisogni
Controllo	Separazione degli ambienti di sviluppo, di test e operativi Controllo	La direzione approva, pubblica e trasmette a tutti i dipendenti nonché alle terze parti interessate la politica per la gestione dei cambiamenti
Controllo	Sicurezza operativa dell'amministratore	Le operazioni critiche in cui un guasto può causare danni irrecuperabili sono documentate in specifiche politiche e procdure.
Obiettivo	**Logging e monitoraggio**	
Controllo	Registrazione degli eventi	La direzione adotta sistemi di raccolta di log protetti da manomissioni in rispondenza alle direttive normative e attua politica di protezione di tali dati da eventuali manomissioni

Controllo	Protezione delle informazioni di log	La direzione adotta sistemi di raccolta di log protetti da manomissioni in rispondenza alle direttive normative e attua politica di protezione di tali dati da eventuali manomissioni
Controllo	Log dell'amministratore e dell'operatore	La direzione adotta sistemi di raccolta di log protetti da manomissioni in rispondenza alle direttive normative e attua politica di protezione di tali dati da eventuali manomissioni
Controllo	Sincronizzazione del Clock	La direzione adotta, in base ai termini di legge l'uso di servizi di sincronizzazione a valore legale
Controllo	Monitoraggio dei servizi cloud	Il fornitore di servizi cloud mette a disposizione una console che permette di monitorare il funzionamento dei servizi cloud.
Obiettivo	**Network security management**	
Controllo	Controlli di rete	L'organizzazione adotta sistemi di controllo della rete al fine di limitare il rischio di esposizione a problemi di sicurezza dei sistemi
Controllo	Sicurezza dei servizi di rete	L'organizzazione adotta strumenti atti a proteggere gli elementi connessi in rete
Controllo	Segregazione nelle reti	L'organizzazione adotta la segmentazione delle infrastrutture a protezione degli accessi alle risorse
Controllo	Allineamento della gestione della sicurezza per reti virtuali e fisiche	L'accesso attaverso il browser da parte degli utenti è definito attraverso URL specifici. La rete di management e quella delle VM sono disciplinate da un accesso autenticato e granulare a seconda del profilo assegnato. ASMENET non gestisce macchine fisiche.
Area "PPI Protection (27018)"		
O/C	**Procedura**	**Descrizione della Procedura**
Obiettivo	**Generali**	
Obiettivo	**Consenso e scelta**	
Controllo	Obbligo di cooperare per i diritti PII	Sono forniti al cliente del servizio cloud i mezzi per consentirgli l'esercizio dei diritti dei titolari delle PII di accedere, correggere e/o cancellare le PII che li riguardano.
Obiettivo	**Legittimità e specificazione dello scopo**	
Controllo	Modalità gestione PII	Sono forniti al cliente i mezzi per consentirgli l'esercizio dei diritti dei titolari delle PII (accedere, correggere e/o cancellare le PII che li riguardano)
Controllo	Elaborazione per uso commerciale	Non è previsto il trattamento delle informazioni a fini di marketing e/o pubblicità.
Obiettivo	**Limitazione della raccolta**	

Obiettivo	**Minimizzazione dati**	
Controllo	Cancellazione sicura file temporanei	La Politica di Sviluppo SW descrive le modalità di gestione dei file temporanei.
Obiettivo	**Limitazione dell'uso, della conservazione e della divulgazione**	
Controllo	Notifica divulgazione PII	Il contratto (determina) prevedere i tempi concordati di mantenimento delle informazioni e le modalità di comunicazione delle stesse
Controllo	Registrazione divulgazione PII	E' prevista la registrazione nel registro del responsabile del trattamento
Obiettivo	**Precisione e qualità**	
Obiettivo	**Apertura, trasparenza e notifica**	
Controllo	Divulgazione da sub-contratto	E' prevista la possibilità di sub responsabili del trattamento
Obiettivo	**Partecipazione individuale e accesso**	
Obiettivo	**Responsabilità**	
Controllo	Divulgazione data breach PII	Il cliente è informato tempestivamente in caso di accesso non autorizzato alle PII o di accesso non autorizzato alle apparecchiature o alle strutture di elaborazione con conseguente perdita, divulgazione o alterazione delle PII.
Controllo	Periodo di conservazione per i criteri e le linee guida per la sicurezza amministrativa	devono essere documentate e rese disponibili delle procedure operative a tutti gli utenti che ne necessitano
Controllo	Restituzione PII, trasferimento e distruzione	E' definita una politica in materia di restituzione, trasferimento e/o smaltimento delle PII ed è resa disponibile al cliente del servizio cloud.
Obiettivo	**Sicurezza delle informazioni**	
Controllo	Accordi di riservatezza o non divulgazione	L'organizzazione stabilisce accordi di riservatezza con gli attori esterni chiamati a gestire informazioni non necessariamente pubbliche
Controllo	Limitazione della creazione di materiale cartaceo	La documentazione cartacea è limitata alla sola documentazione che deve essere prodotta e/o archiviata in tal forma per adempiere ad un obbligo di legge o contrattuale.
Controllo	Controllo e registrazione del ripristino dei dati	La direzione approva, pubblica e trasmette a tutti i dipendenti nonché alle terze parti interessate la politica per la gestione dei backup
Controllo	Protezione dati sui supporti di memorizzazione in uscita	L'organizzazione ha adottato procedure che definiscono le modalità d'uso consentito e/o vietato dei supporti rimovibili
Controllo	Utilizzo di supporti e dispositivi di memorizzazione portatili non crittografati	

Controllo	Crittografia delle PII trasmesse su reti pubbliche di trasmissione dati	La componente di traffico è gestita in autonomia dal fornitore del servizio Cloud; impostata come predefinita. Per il servizio di Conservazione e per quello di Protocollo, la crittografia è applicata con protocolli HTTPS e certificato SSL di tipo Organization Validation (OV), i cui vantaggi principali sono: visualizzazione deil simbolo del lucchetto nel browesr; rimozione degli avvisi di sicurezza dal browser; miglioramento il ranking SEO; associazione del dominio ad ASMENET.
Controllo	Smaltimento sicuro dei materiali cartacei	I documenti cartacei contenti informazioni di rilievo sono smatiti utilizzando un trita documenti
Controllo	Uso univoco degli ID utente	La modalità di assegnazione di informazioni segrete di autenticazione, per l'accesso alle reti ed ai servizi in rete sono condotte in conformità con le politiche approvate dalla Direzione.
Controllo	Registri degli utenti autorizzati	
Controllo	Gestione ID utente	
Controllo	Misure contrattuali	I contratti con i clienti (Enti soci) del servizio cloud specificano le misure tecniche e organizzative atte a garantire le previste misure di sicurezza e che i dati siano trattati per scopi in base alle istruzioni del responsabile del trattamento.
Controllo	Elaborazione PII da aprte di sub responsabili del trattamento	I contratti con i sub responsabili del trattamento che trattano le PII specificano le misure tecniche e organizzative in riferimento al reg. EU 2016/679
Controllo	Accesso ai dati sullo spazio di archiviazione	Le procedure del fornitore del servizio Cloud prevedono la sovrascrittura dei dati eliminati per rendere irrecuperabili
Obiettivo	**Conformità alla privacy**	
Controllo	Posizione geografica PII	L'area geografica definita in cui sono allocate le risorse cloud è "Europe-wes1" coincidente con "St. Ghislain - Belgio"
Controllo	Destinazione prevista PII	Il requisito è insito nella Politica di Sviluppo SW