INFORMATION SECURITY POLICY

Stato	Redatto e aggiornato da	Rivisto e approvato da
Approvato	Resp. Compliance	Amministratore Delegato
	19/05/2025	20/05/2025

LISTA DI DISTRIBUZIONE

A tutti gli stakeholder

STORIA DELLE MODIFICHE APPORTATE

VERSIONE	DATA	PARAGRAFO	MODIFICHE
1.0	19/05/2025	-	Prima stesura

SOMMARIO

1. SCOPO

Lo scopo del presente documento è quello di individuare le misure tecniche ed organizzative adottate da Argentea al fine di tutelare i dati personali aziendali e dei propri, nonché evitare interruzioni nello svolgimento delle proprie attività, in conformità alla normativa di riferimento e alle certificazioni di cui Argentea è dotata.

Questo documento delinea le politiche, le procedure e le misure adottate dall'azienda per mantenere la riservatezza, l'integrità e la disponibilità delle informazioni. Il documento copre tutti gli aspetti della sicurezza delle informazioni all'interno dell'organizzazione, compresi i sistemi informativi, le reti e i dati trattati.

2. CAMPO DI APPLICAZIONE

La presente procedura si applica per ogni servizio SaaS fornito da Argentea.

3. NORMATIVA

Argentea si impegna a garantire il rispetto di tutta la normativa applicabile, tra la quale spiccano nell'ambito della sicurezza delle informazioni:

- D.lgs. 196/2003 – Codice in materia di protezione dei dati personali;
- Regolamento UE 679/2016 – Regolamento generale sulla protezione dei dati (GDPR);
- Direttiva UE 2555/2022 – Direttiva NIS 2.

4. CERTIFICAZIONI E POLITICHE

Argentea è certificata secondo i seguenti standard internazionali:

Schema di certificazione	Data di prima certificazione	Campo di applicazione
Sistema di Gestione della Qualità (ISO 9001:2015)	2013	➢ Progettazione, sviluppo, manutenzione, erogazione e assistenza di soluzioni software per la gestione dei processi di pagamento e incasso elettronico (attività di O.I.L. - Ordinativo Informatico Locale e Firma Digitale). ➢ Progettazione, sviluppo, manutenzione, installazione, erogazione e assistenza di sistemi integrati di pagamento multibanca. ➢ Progettazione ed erogazione di servizi di Conservazione a norma di documenti informatici.
Sistema di Gestione per la prevenzione della corruzione (ISO 37001:2016)	2024	➢ Progettazione, sviluppo, manutenzione, erogazione e assistenza di soluzioni software per la gestione dei processi di pagamento e incasso elettronico (attività di O.I.L. - Ordinativo Informatico Locale e Firma Digitale). ➢ Progettazione, sviluppo, manutenzione, installazione, erogazione e assistenza di sistemi integrati di pagamento multibanca. ➢ Progettazione ed erogazione di servizi di Conservazione a norma di documenti informatici.
Sistema di Gestione della Sicurezza	2020	➢ Progettazione, sviluppo, manutenzione,

delle Informazioni (ISO 27001:2022)		erogazione e assistenza di soluzioni software per la gestione dei processi di pagamento e incasso elettronico (attività di O.I.L. - Ordinativo Informatico Locale e Firma Digitale). ➢ Progettazione, sviluppo, manutenzione, installazione, erogazione e assistenza di sistemi integrati di pagamento multibanca. ➢ Progettazione ed erogazione di servizi di Conservazione a norma di documenti informatici.
Estensione alle linee guida 27017 e 27018	2020	➢ Progettazione, sviluppo, manutenzione, erogazione e assistenza di soluzioni software per la gestione dei processi di pagamento e incasso elettronico (attività di O.I.L. - Ordinativo Informatico Locale e Firma Digitale). ➢ Progettazione ed erogazione di servizi di Conservazione a norma di documenti informatici.

Tutti i certificati e le relative politiche sono disponibili sul sito internet della società al seguente indirizzo https://www.argentea.it/certificazioni/ .

Argentea garantisce che tutte le pratiche di gestione della sicurezza delle informazioni siano allineate con questi requisiti, assicurando così la protezione adeguata dei dati dei clienti e delle operazioni aziendali.

si impegna ad attuare le misure tecniche e organizzative adeguate al rischio ex art. 32 GDPR personalizzate per ogni servizio offerto e di predisporre le procedure in materia di gestione dei diritti degli interessati ai sensi degli artt. Da 15 a 22 del GDPR.

Inoltre, al fine di prevenire la commissione di reati informatici, Argentea ha adottato un Modello di Organizzazione, Gestione e controllo e un Codice Etico ai sensi del d.lgs. 231/01.

5. RUOLI E RESPONSABILITÀ

Nell'ambito dei propri processi, Argentea ha individuato i principali ruoli e responsabilità nell'ambito del proprio sistema per la sicurezza delle informazioni e di business continuity:

- **CTO - Chief Technology Officer**
  - Condivide con la direzione gli obiettivi di business e i relativi budget.
  - Valuta, sempre con la direzione, la scelta strategica delle tecnologie da utilizzare per il raggiungimento degli obiettivi di business.
  - Definisce, insieme alla direzione, obiettivi di crescita dello staff (formazione, premi, condivisione informazioni)
  - Stabilisce le politiche di project management
- **Security Manager**
  - Predispone gli accorgimenti e i comportamenti utili a prevenire attacchi informatici.
  - Analizza i sistemi informatici in uso per individuare falle e vulnerabilità.
  - Controlla l'efficacia degli strumenti di difesa e degli antivirus.
  - Verifica il corretto funzionamento di applicazione, infrastrutture, processi e che quanto preposto sia adeguato al business.
  - Tutela la privacy di dati e informazioni sviluppando una strategia che ne massimizzi l'integrità, la disponibilità e la riservatezza.
  - Interviene in caso di attacchi informatici, incidenti, guasti o errori.
  - Delinea piani di ripristino e di risposta alle emergenze.

- Adegua l’intero business agli standard legali relativi alla sicurezza, gestendo la compliance normativa e definendo delle policy

➢ **DPO – Data Protection Officer** nominato in conformità con quanto previsto dalla vigente normativa in materia di Privacy e Protezione dei dati personali:
- Conformità normativa: assicura che l'azienda rispetti le normative sulla protezione dei dati personali, in particolare il GDPR.
- Valutazioni d'impatto sulla protezione dei dati (DPIA): conduce DPIA per identificare e mitigare i rischi legati al trattamento dei dati personali.
- Gestione dei diritti degli interessati: facilita l'esercizio dei diritti degli interessati, come l'accesso, la rettifica e la cancellazione dei dati.
- Formazione e sensibilizzazione: educa il personale sulle pratiche di protezione dei dati e promuove una cultura della privacy.
- Rapporti con le autorità di controllo: agisce da punto di contatto con le autorità di protezione dei dati e gestire le comunicazioni in caso di violazioni

➢ **IRT – Incident Response Team**
- Definisce e approva il Piano di Disaster Recovery e i suoi aggiornamenti;
- Promuove e coordina le attività di formazione e sensibilizzazione sui temi della gestione incidenti, della continuità operativa e della sicurezza sul lavoro, del personale dell’organizzazione.
- Valuta le situazioni di emergenza e dichiara lo stato di disastro;
- Supporto al piano di eradication, contenimento e mitigazione dell’incidente;
- Avvia le attività di ripristino delle funzionalità informatiche e controlla il loro svolgimento;
- Gestisce i rapporti con l’esterno e le comunicazioni ai dipendenti;
- Attiva e monitora il processo di rientro dall’emergenza;
- Gestisce tutte le situazioni non contemplate;
- Gestisce i rapporti interni e risolve i conflitti di competenza;
- Dichiara la conclusione dello stato di disastro.

➢ **System Administrator**
- Progetta e adatta il sistema a seconda delle esigenze aziendali
- Installa e aggiorna il software e configura i dispositivi hardware necessari
- Realizza la messa a punto dei sistemi nella loro fase di avvio e stabilisce le regole di funzionamento e di accesso, sulla base delle indicazioni aziendali ricevute
- Verifica il regolare funzionamento del sistema e delle componenti che ne fanno parte (server, web, e-mail, database, servizi FTP, ecc.), al fine di soddisfare la continuità del servizio, i salvataggi, la sicurezza e le esigenze di performance Diagnostica e risolve problemi ed errori, cercando di limitare il più possibile i difetti e i danni e di ripristinare velocemente la funzionalità della rete
- Si conforma alle procedure dell’organizzazione per assicurare l’integrità del sistema.
- Identifica le esigenze del sistema informativo (aggiornamenti, modifiche, ampliamenti, ecc.) e fa da interfaccia con gli specialisti e i fornitori
- Configurazione dei sistemi: garantisce che i sistemi informatici siano configurati in modo sicuro e aggiornato.
- Gestione degli accessi: controlla e monitora gli accessi ai sistemi e alle informazioni sensibili.
- Monitoraggio delle reti: sorveglia le reti aziendali per individuare e rispondere a eventuali minacce.
- Backup e ripristino: gestisce ili backup dei dati e garantisce la disponibilità delle informazioni attraverso piani di ripristino.

➢ **Responsabile del Sistema di Gestione**
- È responsabile della corretta implementazione e mantenimento del sistema di gestione
- Si occupa di garantire che vengano correttamente gestite le non conformità, azioni correttive e preventive.
- Si occupa dello svolgimento degli audit interni e di terza parte e partecipa in maniera attiva ad eventuali visite da parte degli Enti Istituzionali.
- Informa e sensibilizza gli stakeholder individuati nell'analisi del contesto.
- È responsabile della corretta gestione e risoluzione delle segnalazioni

➢ **Responsabili dei processi aziendali**

- Integrazione della sicurezza nei processi: si assicura che le misure di sicurezza siano incorporate nei processi aziendali.
- Protezione dei dati dei clienti e dipendenti: gestisce e protegge i dati personali trattati.

➢ **Dipendenti**
- Conformità alle policy: rispettano le politiche e le procedure di sicurezza e protezione dei dati stabilite dall'azienda.
- Segnalazione degli incidenti: riferiscono tempestivamente eventuali incidenti o sospette violazioni di sicurezza.
- Formazione continua: partecipano ai programmi di formazione e consapevolezza per aggiornarsi sulle best practice di sicurezza e privacy.

6. ANALISI DEI RISCHI

L'analisi dei rischi è un elemento fondamentale nella gestione della sicurezza delle informazioni. Si tratta di un processo sistematico volto a identificare, valutare e gestire i rischi che potrebbero compromettere la sicurezza delle informazioni aziendali. È, inoltre, un processo complesso e continuo che richiede un'attenta pianificazione, implementazione e monitoraggio. L'obiettivo è proteggere gli asset informativi dell'azienda riducendo al minimo l'esposizione alle minacce e garantendo la resilienza operativa.

Argentea, partendo dalla propria analisi del contesto, ha individuato i rischi per i propri sistemi di gestione, tenendo conto di:

- il perimetro dell'attività presa in esame;
- vincoli normativi, tecnologici o economici;
- fattori interni ed esterni;
- le esigenze e le aspettative delle parti interessate;
- la presenza di possibili casi che si sono già verificati con la conseguente applicazione delle soluzioni che si sono già eventualmente adottate;
- delle potenziali minacce che potrebbero compromettere la sicurezza degli asset;
- le vulnerabilità dei propri asset, ossia i punti deboli che potrebbero essere sfruttati dalle minacce.

In base ai risultati ottenuti dall'analisi dei rischi e al concetto di miglioramento del sistema, possono essere intraprese le seguenti azioni:

- evitare il rischio (decidendo ad es. di non iniziare un'attività);
- assumersi il rischio in modo da perseguire un'opportunità (ad es. perseguo l'obiettivo sapendo che potrebbe comportare un aggravamento del rischio);
- rimuovere la fonte di rischio;
- trasferire il rischio a terzi, ad esempio mediante assicurazioni o outsourcing (ad es. stipulare una polizza assicurativa contro i cyber-attacchi);
- modificare la probabilità o le conseguenze;
- accettare il rischio sulla base di una decisione informata.

In tale contesto, si specifica che Argentea si è dotata di una assicurazione a copertura di eventuali danni da violazione o perdita di dati.

Con l'applicazione di una di queste azioni di trattamento del rischio vengono stabiliti il grado di probabilità e degli impatti residui che daranno origine al valore di rischio residuo, ovvero, quel valore di rischio che rimane nonostante le azioni poste in essere (c.d. azioni di mitigazione).

Il rischio residuo ottenuto dovrà quindi essere oggetto di periodici o continui monitoraggi e verrà gestito dai singoli Risk Owner.

Argentea ha implementato un sistema di processi e procedure volto a monitorare continuamente i propri rischi e l'implementazione delle misure di mitigazione e di sicurezza individuate.

7. MISURE PER IL PERSONALE DIPENDENTE

Le principali misure adottate nei confronti del personale dipendente sono:

1. Processo di screening per tutto il personale: le informazioni su tutti i candidati presi in considerazione vengono raccolte e gestite tenendo conto della specifica legislazione applicabile.
2. obbligo di non divulgazione e riservatezza nei confronti di tutto il personale dipendente, prevedendo la possibilità di ricorso a sanzioni disciplinari in caso di violazione.
3. autorizzazione per mezzo dell'atto di nomina ed istruzione tramite le istruzioni tutto il personale dipendente, ai sensi dell'art. 29 GDPR.

7.1 FORMAZIONE E CONSAPEVOLEZZA

Argentea riconosce l'importanza della formazione e della consapevolezza quali elementi fondamentali di un Sistema di Gestione della Sicurezza delle informazioni e della Privacy.

Argentea eroga a tutti i propri dipendenti corsi generici e specifici in materia di Sicurezza delle informazioni, Cyber-sicurezza e della privacy tramite lezioni frontali o corsi on-line tramite la propria piattaforma di e-learning. Tali corsi hanno lo scopo di sensibilizzare sui rischi e sulle migliori pratiche di sicurezza.+

Inoltre, Argentea promuove una cultura della sicurezza attraverso campagne di sensibilizzazione (ad es. campagne di phishing simulate) e iniziative educative.

Tali iniziative mirano a:

- ➢ prevenire incidenti di sicurezza: educare i dipendenti su come evitare comportamenti che potrebbero compromettere la sicurezza delle informazioni.
- ➢ rispondere agli incidenti: assicurare che i dipendenti sappiano come riconoscere e segnalare incidenti di sicurezza.
- ➢ conformità normativa: garantire che il personale sia a conoscenza delle leggi e dei regolamenti pertinenti, come il GDPR.
- ➢ cultura della sicurezza: promuovere una cultura aziendale in cui la sicurezza delle informazioni sia una priorità condivisa da tutti.

Argentea, al fine di creare un programma di formazione e consapevolezza efficace, provvede a pianificare annualmente la formazione, attraverso la raccolta e la valutazione delle esigenze formative basata sul ruolo e sulle responsabilità di ciascun dipendente, nonché la definizione di obiettivi formativi chiari, come la comprensione delle politiche di sicurezza, la conoscenza delle procedure di risposta agli incidenti e la capacità di riconoscere le minacce.

L'erogazione della formazione avviene per i nuovi dipendenti durante il processo di onboarding. In seguito, viene garantito un processo di formazione continua per aggiornare il personale sulle nuove minacce e sulle modifiche alle politiche di sicurezza, e formazione specializzata per i dipendenti con ruoli specifici in ambito di sicurezza delle informazioni, come gli amministratori di sistema e i responsabili della sicurezza.

8. CLASSIFICAZIONE DELLE INFORMAZIONI

Argentea ha definito le linee-guida per la gestione delle informazioni aziendali, al fine di garantire la corretta classificazione, conservazione e diffusione delle stesse.

Le informazioni sono un importante asset aziendale e la loro gestione è un aspetto di cruciale importanza per il Gruppo Argentea . Per tale motivo, Argentea ha individuato e applicato le misure minime indicate nei seguenti paragrafi al fine di tutelare la riservatezza, l'integrità e la disponibilità di tutte le informazioni, nonché per assicurare la conformità alle normative vigenti (GDPR, d.lgs. 196/2001, art. 2220 cod. civ., ecc.). Ulteriori misure potranno essere definite in relazione alla gestione di specifiche tipologie di informazioni per cui siano richieste livelli di protezione migliori.

8.1 PRINCIPI GENERALI

I principi generali in materia di gestione delle informazioni sono:

- **Identificazione e classificazione**: tutte le informazioni devono essere identificate, categorizzate e classificate in base alla loro importanza, sensibilità e criticità per l'organizzazione.
- **Periodi di conservazione**: i dati devono essere conservati solo per il periodo strettamente necessario e in conformità con le normative applicabili.
- **Minimizzazione**: raccogliere, conservare e utilizzare solo le informazioni necessarie per il raggiungimento degli scopi definiti.
- **Trasparenza e Responsabilità**: assicurare la trasparenza riguardo alle pratiche di gestione delle informazioni e individuare i responsabili per ciascuna informazione.
- **Sicurezza delle informazioni**: implementare misure tecniche ed organizzative adeguate a proteggere la riservatezza, integrità e disponibilità delle informazioni, nonché per evitare trattamenti non autorizzati o illeciti.

Ai sensi dell'art. 5 del Regolamento EU 2016/679, i dati personali oggetto di trattamento devono essere:

- trattati in modo lecito, corretto e trasparente;
- raccolti e registrati per scopi determinati, espliciti, legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi (cd. "limitazione delle finalità");
- esatti e, se necessario, aggiornati (cd. "esattezza");
- adeguati, pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono stati raccolti o successivamente trattati (cd. "minimizzazione dei dati");
- conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario per gli scopi per i quali essi sono stati raccolti o successivamente trattati (cd. "limitazione della conservazione")
- trattati in modo da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (cd. "integrità e riservatezza").

8.2 CRITERI DI CLASSIFICAZIONE

I documenti prodotti da Argentea vengono classificati in base alle informazioni che essi contengono.

La classificazione tiene conto delle necessità dell'attività di condividere o limitare l'accesso alle informazioni, così come di rispettare i requisiti giuridici. Le risorse sono mappate in base alla classificazione delle informazioni che vi sono conservate, derivante dalla valutazione degli impatti che subirebbe l'Azienda (in termini economici, reputazionali o legali) qualora vi fosse una perdita di confidenzialità, o comunque una loro diffusione incontrollata.

In funzione della tipologia di informazioni elaborate sono stati definiti i seguenti criteri di classificazione:

- **Pubblico**: informazioni che possono essere diffuse all'esterno senza cagionare danni finanziari e/o reputazionali e/o legali all'azienda (ad esempio le presentazioni aziendali ad uso marketing). L'esposizione pubblica delle informazioni aziendali deve essere opportunamente autorizzata.
- **Ad Uso Interno**: informazioni di normale operatività o documenti di carattere generale, accessibili a tutti in azienda e senza particolari protezioni se non una diffusione basata sul criterio di "need to know". Tale criterio vale anche per la diffusione all'esterno a clienti e fornitori. Per loro natura, qualora vi sia una incontrollata diffusione di tali informazioni, l'azienda potrebbe subire una perdita di valore dell'asset.
- **Riservate**: informazioni il cui perimetro di diffusione è ristretto ai soggetti esplicitamente autorizzati e la cui fuoriuscita può cagionare danni economici e di business diretti, avere impatti reputazionali con perdita di fiducia e credibilità sui clienti, ed eventualmente legali (es. GDPR). I dati così classificati, vengono custoditi solo in ambienti con adeguati livelli di protezione da accessi non autorizzati.

L'associazione della classificazione del documento all'informazione in esso contenuta si basa quindi su una scala basata sugli impatti come segue:

Classificazione	Criticità dell'informazione	Valutazione impatto

Pubblico	Nulla	Non significativo
Ad uso interno	Bassa	Minore
	Media	Moderato
Riservate	Alta o Strategica	Critico

Tutte le informazioni aziendali non esplicitamente classificate devono intendersi almeno **Ad Uso Interno**.

Tutte le informazioni, che contengono dati personali e di cui Argentea è Titolare o Responsabile del trattamento, si considerano perlomeno classificate come Riservate e devono essere trattate conformemente al Regolamento EU 679/16 (c.d. GDPR).

8.3 CRITERI DI CLASSIFICAZIONE

Tutti i documenti gestiti da Argentea sono conservati nelle modalità e nei tempi previsti dalle misure di sicurezza minime indicate in seguito e nel rispetto delle normative di riferimento, nonché delle policy interne.

I Responsabili di ciascuna funzione aziendale designati dovranno controllare periodicamente se esistono dati archiviati la cui "Retention Time" sia scaduta e quindi debbano essere cancellati, ciò al fine di gestire in maniera ordinata l'archivio e permettere di conservare solo i dati considerati necessari.

A tal fine le persone incaricate dovranno procedere:

- all'aggiornamento costante dei documenti prodotti e/o ricevuti, con opportuna classificazione;
- alla programmazione di periodiche verifiche, in rapporto ai tempi di conservazione;
- all'eliminazione / cancellazione periodica degli atti non più necessari.

Argentea attua il principio di minimizzazione dei dati, poiché tratta i dati personali in modo adeguato, pertinente e limitato rispetto a quelle che sono le finalità. Argentea per poter soddisfare il principio di minimizzazione dei dati personali ex art. 5, par. 1, lett. c GDPR, applica le seguenti misure tecniche, se previste dal contratto sottoscritto:

- Filtraggio e rimozione;
- Riduzione del potenziale identificativo attraverso trasformazione;
- Riduzione della natura identificativa del dato;
- Riduzione dell'accumulazione dei dati;
- Limitazione dell'accesso ai dati.

8.3.1 CANCELLAZIONE DEI DATI

Per cancellazione dei dati si intende la distruzione fisica o tecnica sufficiente per rendere le informazioni contenute in un documento non più recuperabili con gli ordinari mezzi disponibili in commercio.

Le informazioni devono essere opportunamente cancellate o distrutte nei seguenti casi:

- Sia terminato il periodo di retention indicato nel registro del trattamento;
- Risultino scaduti i termini legittimi di conservazione siano essi determinati da norme di legge generali e/o di settore o dalle finalità per le quali i dati sono stati raccolti;
- Non siano più utili al raggiungimento delle finalità lavorative.

Per i documenti cartacei, è necessario provvedere alla loro distruzione fisica, tramite per esempio triturazione, in modo che non siano facilmente ricostruibili.

Nel caso in cui i dispositivi elettronici non vengano smaltiti o non vengano affidati a fornitori specializzati, le informazioni ivi contenute devono essere eliminate secondo modalità di cancellazione sicura dei dati, in modo da garantirne l'eliminazione irreversibile.

8.4 TRASFERIMENTO DELLE INFORMAZIONI

8.4.1 TRASMISSIONE SICURA SU RETI PUBBLICHE

Argentea mantiene aggiornati i propri template e gli standard di configurazione delle connessioni instaurate con i clienti, in particolare la configurazione delle VPN IPSec. I parametri di IKE, ESP e AH seguono i più elevati standard del settore, seguono gli standard del settore, in particolare quelli della Commercial National Security Algorithm Suite (CNSA).

8.4.2 CONDIVISIONE DEI DATI

Qualora risultasse necessario condividere con gli operatori del cliente un dato personale (nome, cognome, CF, indirizzo, etc..), in particolar modo se dati sensibili (dati sanitari, dati giudiziari, etc..), è necessario, assicurare sempre la protezione dell'informazione condivisa. Casi di questo tipo sono, ad esempio, la condivisione di files/tracciati/record con flussi dati.

Per la condivisione sicura si possono applicare le seguenti soluzioni:

- Crittografare i dati utilizzando algoritmi robusti, ad esempio AES-256, supportati da tutti i più diffusi tool di compressione (WinZip, 7-Zip, WinRAR…). In questo caso, la password deve essere comunicata al destinatario attraverso un canale diverso rispetto alla mail (es. telefono).
- Quando necessario, condividere i dati tramite gli strumenti aziendali (Google Drive, SharePoint), proteggendo i collegamenti con password. In questo caso, la password deve essere comunicata al destinatario attraverso un canale diverso rispetto al collegamento;

Eventuali documenti ricevuti che contengano informazioni o dati personali eccedenti rispetto alle finalità lavorative devono essere cancellati.

8.5 CRITTOGRAFIA

La crittografia rappresenta un elemento fondamentale per la protezione della riservatezza e dell'integrità delle informazioni all'interno di un'azienda. La sua implementazione è prevista per le informazioni maggiormente sensibili (riservate) e in particolare per i dati personali sensibili.

Argentea ha adottato sistemi di crittografia basati sui più alti standard di sicurezza per la crittografia dei dati a riposo e per la crittografia dei dati in transito. La scelta dell'algoritmo specifico dipende dalla sensibilità dell'informazione, le necessità aziendali e quelle dei clienti.

8.5.1 CRITTOGRAFIA AT REST

L'obiettivo della cifratura a riposo è quella di proteggere i dati memorizzati nei database, dispositivi di archiviazione, dispositivi mobili, server e backup. Le tecnologie che possono essere utilizzate sono:

- **Advanced Encryption Standard (AES)**: richiesta con una chiave di 256 bit per una protezione adeguata;
- **Full Disk Encryption (FDE)**: cifratura completa dei dischi rigidi utilizzata per proteggere tutte le informazioni contenute su un dispositivo;
- **Cifratura a livello di file/cartella**: utilizzo di strumenti come BitLocker, VeraCrypt o simili per cifrare specifici file o cartelle sensibili;
- **Cifratura dispositivi mobili**: per prevenire la perdita di dati in caso di smarrimento o furto, Argentea ha attivato su tutti i dispositivi mobili e portatili la crittografia tramite Bitlocker.
- **Cifratura del Database**: implementazione di cifratura a livello di database utilizzando tecniche come Transparent Data Encryption (TDE) per proteggere i dati sensibili memorizzati nei database, assicurando che le informazioni restino cifrate anche se il database viene compromesso;

8.5.2 CRITTOGRAFIA IN TRANSIT

L'obiettivo della cifratura in transito è quello di proteggere i dati durante la trasmissione attraverso reti pubbliche o private, prevenendo intercettazioni e manomissioni. Le tecnologie che possono essere utilizzate sono:

- **Transport Layer Security** (TLS): protocollo utilizzato per cifrare le comunicazioni su Internet (ad es. HTTPS per i siti web sicuri);
- **Virtual Private Network** (VPN) : crea un tunnel cifrato per il traffico di rete, proteggendo le comunicazioni tra dispositivi e reti; La configurazione di VPN (Virtual Private Network) è necessaria anche per proteggere le comunicazioni remote tra i dipendenti e l'azienda, soprattutto quando i dipendenti lavorano in smartworking.
- **Secure Shell** (SSH): protocollo per accessi remoti sicuri e trasferimenti di file crittografati;
- **Cifratura delle Connessioni ai Database**: implementazione di protocolli sicuri, come TLS o SSL, per cifrare i dati trasmessi tra applicazioni web e database, garantendo che le informazioni sensibili rimangano protette durante il trasferimento tra server e database;
- **Cifratura dei WebSocket**: per applicazioni che utilizzano WebSocket per comunicazioni in tempo reale, la cifratura può essere implementata tramite WebSocket Secure (WSS), che utilizza TLS per proteggere i dati scambiati;
- **Cifratura delle API**: le API, specialmente quelle esposte su Internet, devono essere cifrate utilizzando TLS per proteggere i dati scambiati tra client e server API. Oltre a TLS, è possibile applicare tecniche di cifratura aggiuntive sui payload delle API per una maggiore sicurezza;
- **Internet Protocol Security** (IPSec): protocollo che autentica e cifra ogni pacchetto IP in una sessione di comunicazione, utilizzato per proteggere le comunicazioni con fornitori e clienti.
- **STARTTLS**: estensione dei protocolli di comunicazione come SMTP (per email) o IMAP/POP3 che permette di elevare una connessione non cifrata a una cifrata utilizzando TLS, garantendo la sicurezza dei dati in transito durante lo scambio di email o la sincronizzazione della posta;

9. CONTROLLO DEGLI ACCESSI LOGICI

Il controllo degli accessi è un elemento essenziale della sicurezza, che determina chi può accedere a determinati dati, applicativi e risorse e in quali circostanze. I criteri di controllo degli accessi si basano su tecniche come l'autenticazione e l'autorizzazione, che consentono alle organizzazioni di verificare in modo esplicito che gli utenti siano chi dicono di essere e che venga loro concesso il livello di accesso appropriato in base al contesto, valutato in base a fattori come il dispositivo, la posizione, il ruolo e molto altro.

Il controllo degli accessi protegge le informazioni riservate, come i dati dei clienti e la proprietà intellettuale, contro il furto per mano di utenti malintenzionati o di altri utenti non autorizzati. Riduce anche il rischio di esfiltrazione causato delle azioni dei dipendenti e tiene a bada le minacce Web. Invece di gestire le autorizzazioni manualmente, le organizzazioni più orientate alla sicurezza tendono a utilizzare soluzioni di gestione degli accessi e delle identità per implementare i criteri di controllo degli accessi.

Argentea utilizza un sistema di controllo degli accessi logici, atti ad assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento. Sono definite la lunghezza delle password, la tipologia dei caratteri richiesti, la durata della validità, il numero di tentativi prima del blocco dell'account, ecc.), al fine di limitare i rischi di accesso di persone non autorizzate ai dati personali in forma digitale.

Per fare ciò, Argentea:

- definisce profili di autorizzazione nei sistemi separando le attività e le aree di responsabilità per limitare l'accesso degli utenti ai soli dati strettamente necessari per portare a termine i rispettivi compiti;
- rimuove le autorizzazioni di accesso non appena un utente cessi di essere abilitato ad accedere a una risorsa locale o IT, ovvero allo scadere del contratto;
- realizza una revisione delle abilitazioni per identificare ed eliminare gli account per i dipendenti che cambiano mansione o lavoro e, pertanto, non fanno più parte di Argentea.

9.1 PRINCIPI IN MATERIA DI CONTROLLO DEGLI ACCESSI

L'accesso ai sistemi informativi deve essere controllato tramite procedure di autenticazione e autorizzazione basate sui seguenti principi:

- **Principio del Minimo Privilegio**: Gli accessi devono essere concessi in base al principio del minimo privilegio, ovvero gli utenti devono avere solo l'accesso necessario per svolgere le proprie attività lavorative.
- **Principio del "Need to Know"**: le informazioni devono circolare e essere utilizzate solo da chi, per le proprie ed esclusive necessità lavorative, necessità di averle e gestirle. Queste persone, qualora debbano trasmettere o condividere con altre informazioni aziendali, devono prestare attenzione a chi forniscono tali informazioni, a che titolo e in che forma.
- **Autenticazione Multi-Fattore** (MFA): L'autenticazione multi-fattore deve essere utilizzata per rafforzare la sicurezza durante il processo di accesso, richiedendo più di un metodo di verifica dell'identità dell'utente.
- **Controllo degli Accessi Fisici**: L'accesso fisico alle strutture dell'organizzazione deve essere controllato utilizzando sistemi di sicurezza appropriati, come badge, chiavi elettroniche o dispositivi biometrici.
- **Monitoraggio degli Accessi**: Tutti gli accessi alle risorse dell'organizzazione devono essere registrati e monitorati per individuare e prevenire eventuali abusi o violazioni della sicurezza.
- **Politiche di Accesso Remoto**: Devono essere implementate politiche e procedure per gestire in modo sicuro l'accesso remoto alle risorse dell'organizzazione, inclusi dispositivi mobili e lavoratori remoti.
- **Periodo di Validità degli Accessi**: Gli accessi devono essere revocati o aggiornati in modo tempestivo quando non sono più necessari o autorizzati, ad esempio in caso di cambio di ruolo o cessazione del rapporto lavorativo.

Argentea ha centralizzato la gestione delle utenze, per cui tutti i software e servizi in uso demandano i processi di autenticazione:

- dove sono anche impostati i seguenti criteri per le password di tutte le utenze (Global policy):
- storicizzazione delle password in modo da evitare di reiterare l'utilizzo delle stesse;
- scadenza della password periodica;
- regole per la complessità delle password, come utilizzo di un determinato numero di caratteri, numeri, lettere maiuscole o minuscole e caratteri alfanumerici;
- l'assenza di relazione tra la password e l'utente.

9.2 ASSEGNAZIONE, MODIFICA E REVOCA DELLE UTENZE DI DOMINIO

La gestione delle utenze all'interno del dominio avviene attraverso un software che automatizza il provisioning. Tale software si occupa di mantenere sincronizzato l'alberatura rispetto alle modifiche effettuate sui gestionali interni.

L'Ufficio Personale assegna l'utenza che è allineata agli stati contrattuali e alla posizione lavorativa. Essa si attiva al primo giorno di lavoro e si chiude con la fine del contratto di lavoro. In base alla posizione lavorativa, all'utente vengono assegnati determinati diritti di accesso al filesystem aziendale e ai vari applicativi o servizi dell'organizzazione.

Qualora sorga la necessità di modificare i diritti di un accesso di un collaboratore, è necessario inserire un apposito ticket nel gestionale interno. La richiesta viene, quindi, valutata dagli uffici competenti, i quali possono eventualmente avvalorare la richiesta, chiedendo l'autorizzazione a procedere al superiore gerarchico del richiedente.

Ciascuna modifica dei diritti di accesso viene fatta ad personam e tracciata sull'applicativo dedicato.

Le utenze di amministratore di dominio sono create manualmente su richiesta e dietro specifica autorizzazione da parte delle funzioni competenti. Le utenze da amministratore vengono create con credenziali di dominio privilegiate, per le quali prevista un'autenticazione a due fattore (2FA) obbligatoria.

I diritti di accesso sono sottoposti ad una revisione regolare tramite il monitoraggio e l'analisi dei log e degli alert di sicurezza.

9.3 AMMINISTRATORI DI SISTEMA

Secondo quanto previsto dal provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008, "l'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari del trattamento o dei responsabili, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti". Infatti, Argente ,individua i soggetti autorizzati a trattare i dati personali, definendo le corrette autorizzazioni di accesso ai dispositivi e alle aree ove i dati sono trattati/conservati. Nel caso in cui un soggetto autorizzato non abbia più alcun motivo di effettuare l'accesso, Argentea procederà immediatamente a rimuovere le relative autorizzazioni.

Argentea garantisce che l'accesso di ciascun amministratore sia registrato e conservato secondo le relative policy aziendali, con caratteristiche di completezza, integrità ed inalterabilità e comprende anche i riferimenti temporali, la descrizione dell'evento e del sistema coinvolto.

9.4 ACCESSO DEI CLIENTI AI SERVIZI SAAS ARGENTEA

I clienti possono accedere esclusivamente alle risorse in cloud che sono state loro espressamente messe a disposizione, nel rispetto dei principi di riservatezza e sicurezza. Ogni cliente opera su un'istanza logica dedicata, isolata dalle altre, all'interno di un'infrastruttura progettata con criteri di segmentazione delle reti. Questo approccio garantisce che ciascun cliente possa visualizzare e interagire solo con i propri dati, impedendo qualsiasi accesso non autorizzato a risorse appartenenti ad altri. La configurazione delle reti e delle autorizzazioni è gestita in modo centralizzato e controllato, insieme al fornitore cloud, assicurando la piena separazione tra gli ambienti e il rispetto dei livelli di accesso concordati contrattualmente

9.5 UTENZE DEI CLIENTI

I clienti non hanno accesso diretto all'infrastruttura sottostante, che rimane sotto il controllo esclusivo del fornitore, ma interagiscono con i servizi tramite utenze specificamente generate per l'accesso agli applicativi in modalità SaaS, secondo quanto stabilito a livello contrattuale.

Per ciascun servizio SaaS è previsto un sistema di gestione delle identità e degli accessi che include funzionalità di registrazione e de-registrazione degli utenti in maniera autonoma o supportati dal servizio di assistenza.

Questo garantisce che l'abilitazione e la revoca degli accessi avvengano in modo tracciabile, sicuro e conforme agli accordi e alle politiche di sicurezza dell'informazione applicabili, garantendo anche sistemi di log-in sicuro

10. CONTROLLO DEGLI ACCESSI FISICI

Argentea assicura la presenza di tutte le misure di sicurezza fisiche che hanno il preciso scopo di rafforzare la sicurezza dei locali dell'organizzazione, come di seguito riportato (a titolo esemplificativo e non esaustivo):

- l'accesso ai locali di Argentea è controllato;
- sono stati installati sistemi di allarme antintrusione che vengono controllati periodicamente;
- sono stati installati rilevatori di fumo e strumenti antincendio che vengono controllati periodicamente;
- è garantita la sicurezza delle chiavi e dei codici di allarme che permettono l'accesso ai locali;
- sono state separate le aree degli edifici di Argentea in base ai rischi;
- è presente un elenco aggiornato delle persone o dei dipendenti specificamente autorizzati ad accedere a ciascuna area;
- sono state stabilite delle regole e dei metodi specifici per controllare l'accesso dei visitatori;
- vengono protette fisicamente le apparecchiature IT tramite metodi specifici (sistema di prevenzione incendi dedicato, attrezzatura di sollevamento contro possibili alluvioni, alimentazione elettrica e/o ridondanza del condizionamento d'aria, ecc…).

Argentea demanda contrattualmente ai propri Cloud Service Provider (CSP) la gestione e l'attuazione dei controlli sugli accessi fisici alle infrastrutture che ospitano i servizi cloud erogati. Tali infrastrutture sono situate in data center conformi al livello TIER IV, ubicati esclusivamente sul suolo italiano.

I CSP si impegnano a garantire che gli accessi fisici siano limitati al personale autorizzato, sorvegliati mediante misure di sicurezza adeguate (es. videosorveglianza, badge biometrici, controllo perimetrale), e documentati secondo le migliori pratiche di sicurezza. Argentea si riserva il diritto di richiedere evidenze documentali e/o audit sulle misure adottate.

11. SVILUPPO SICURO DEL SOFTWARE

Allo scopo di costruire una metodologia di sviluppo software sicuro, Argentea ha valutato i seguenti riferimenti disponibili in letteratura:

- Requisiti del Regolamento n° 679/2016 in materia di protezione dei dati personali (nel seguito GDPR);
- Requisiti della norma ISO 27001 in materia di sicurezza delle informazioni;
- Requisiti dello standard OWASP (Open Web Application Security Project);
- Indicazioni contenute nel documento dell'Agenzia per l'Italia digitale "Linee guida per la modellazione delle minacce ed individuazione delle azioni di mitigazione conformi ai principi del secure/privacy by design".
- Linee Guida AGID per lo sviluppo del software sicuro;

Argentea ha adottato un processo che integra pratiche di sicurezza in ogni fase del ciclo di vita dello sviluppo del software, mirando a identificare e mitigare le vulnerabilità sin dalle prime fasi e garantendo che il prodotto finale sia il più sicuro possibile.

Il GDPR non formalizza precise specifiche per lo sviluppo di software conformi al Regolamento, ma pone come capisaldi i principi di protezione dei dati fin dalla progettazione (Privacy by Design) e di protezione per impostazione predefinita (Privacy by Default), che Argentea ha implementato nei propri processi di sviluppo.

Per garantire la sicurezza delle informazioni e la protezione dei dati non solamente personali, Argentea ha raccolto un vasto insieme di misure di sicurezza.

Per ogni nuovo progetto software e per ogni major release di software esistenti, Argentea effettua una accurata analisi dei rischi attraverso una precisa metodologia, che prevede:

- Identificazione delle minacce per la sicurezza che lo possono riguardare;
- Calcolo del livello di rischio per ogni minaccia;
- Identificazione e implementazione delle misure di sicurezza che mitigano i rischi calcolati.

Per testare automaticamente la qualità e il rispetto dei requisiti di sicurezza lungo tutto il processo di sviluppo, Argentea ha standardizzato un sistema preciso e strutturato di software testing e di analisi statica del codice.

12. GESTIONE DELL'INFRASTRUTTURA

Argentea si avvale di infrastrutture messe a disposizione dal proprio Cloud Service Provider (CSP), articolate in due campus localizzati in Italia:

- **Campus 1** ospita un data center di **livello TIER IV**, denominato **DC Primario**, destinato agli ambienti di produzione. È affiancato da un edificio separato dedicato alle operazioni di backup, indicato come **DC Backup**.
  Il DC Primario garantisce elevati livelli di disponibilità, affidabilità e sicurezza, assicurando la continuità delle attività operative e di business.
  Il DC Backup funge da sito di backup off-site, custodendo copie dei dati critici per garantire la protezione e il ripristino delle informazioni in caso di eventi imprevisti.

- **Campus 2** ospita un'ulteriore data center **TIER IV**, destinato alla **Business Continuity e Disaster Recovery**. In tale sede vengono effettuate repliche sincrone degli ambienti di produzione presenti nel DC Primario, permettendo la riattivazione dei sistemi e la continuità dell'erogazione dei servizi in caso di malfunzionamenti o indisponibilità del sito primario.

L'architettura complessiva garantisce la ridondanza dei servizi critici, assicurando resilienza, alta disponibilità e minimizzazione del rischio di interruzione delle attività aziendali.

Su ogni macchina virtuale vengono installati agent di sicurezza che garantiscono la gestione e il monitoraggio dei sistemi, nonché lo svolgimento di attività di Vulnerability Assessment.

Tutte le VM, così come i componenti dell'infrastruttura (server, dispositivi di rete e ambienti virtualizzati), sono hardenizzati e configurati secondo le best practice di sicurezza, disabilitando funzionalità non necessarie, servizi inutilizzati e accessi predefiniti. Vengono inoltre adottati criteri rigorosi di aggiornamento e patch management per minimizzare la superficie di attacco e prevenire l'esposizione a vulnerabilità note.

12.1 NETWORKING

Argentea garantisce un'infrastruttura di rete sicura e segmentata, progettata per prevenire accessi non autorizzati e ridurre i rischi di compromissione. A tal fine, viene adottato un modello di networking che prevede la segregazione logica delle reti, in modo da separare gli ambienti di sviluppo, test e produzione, nonché i dati e i servizi dei diversi clienti.

L'infrastruttura è protetta da firewall configurati con regole restrittive che consentono il traffico necessario al funzionamento dei servizi. Questi dispositivi vengono costantemente monitorati e aggiornati per garantire una protezione efficace contro accessi non autorizzati e minacce esterne, assicurando che solo le connessioni legittime possano raggiungere le risorse aziendali e dei clienti.

Le politiche di controllo degli accessi di rete sono continuamente monitorate, aggiornate e testate per garantire la conformità agli standard di sicurezza e per offrire un ambiente affidabile e protetto in cui i clienti possano operare in totale sicurezza.

12.2 BACKUP

La frequenza e il tempo di conservazione dei backup variano in base alla tipologia di dati trattati e agli accordi contrattuali stipulati con ciascun cliente.

La politica di rotazione dei backup prevede un backup giornaliero per 31 gg, uno mensile per 12 mesi, uno annuale per X anni, dipendentemente dal servizio.

Il controllo della corretta esecuzione dei backup è giornaliero ad opera degli addetti ed è agevolato dall'utilizzo di mail riepilogative e dalla console del backup stessa.

L'infrastruttura di backup sulla quale il servizio agisce è composta da:

- Infrastruttura di backup di data center su una rete separata da quella dei clienti
- Agenti di backup installati sui server oggetto del salvataggio (ove necessario per consentire granularità e consistenza dei backup e dei restore)

Argentea provvede regolarmente allo svolgimento di test periodici di ripristino per verificare che le tecnologie utilizzate per i backup funzionino correttamente e i dati rimangano integri.

12.3 DISASTER RECOVERY

I servizi SaaS sono erogati su un'infrastruttura ad alta affidabilità, basata su un cluster virtualizzato distribuito tra due data center distinti: uno primario e uno dedicato al Disaster Recovery. I dati sono archiviati su storage in replica sincrona tra i due siti, garantendo la disponibilità e l'integrità delle informazioni. Vengono eseguite snapshot lato SAN ogni 4 ore, con una retention di 7 giorni. L'intera architettura è progettata secondo le best practice del settore e include componenti ridondati, assicurando livelli di RPO e RTO prossimi allo zero.

12.4 CESSAZIONE DEL SERVIZIO CLOUD

Il primo passo nel processo di cessazione avviene quando il cliente presenta una richiesta formale di cessazione del servizio, che deve avvenire in conformità ai termini definiti nel contratto, oppure alla scadenza o risoluzione del contratto.

Il cliente viene informato sui dettagli delle operazioni e delle scadenze precise per il completamento delle attività critiche, come il backup e la cancellazione dei dati.

Prima di procedere alla cancellazione dei dati, i dati devono essere trasferiti al cliente attraverso canali sicuri. Il cliente riceve tutte le istruzioni necessarie per completare la copia dei dati entro una data specifica, che deve essere concordata con quest'ultimo. Tale fase è cruciale per assicurare che i dati non vadano persi e che il cliente mantenga il controllo su di essi.

Qualora il cliente non sia in grado di effettuare una copia in autonomia o sia previsto dal contratto, la copia dei dati viene eseguita dall'organizzazione e, successivamente, messa a disposizione del cliente.

A seguito della corretta esecuzione della copia, l'organizzazione procede alla cancellazione dei dati in maniera sicura secondo quanto indicato nel paragrafo 8.3.1. La revoca degli accessi è l'ultimo passaggio fondamentale nella cessazione del servizio. Tutti gli account e le credenziali di accesso agli applicativi devono essere disabilitati, come anche le chiavi di crittografia eventualmente detenute dal cliente. Una volta disabilitati gli accessi, il processo di cessazione del servizio può dirsi concluso.

13. MONITORAGGIO DEI SISTEMI

Il monitoraggio dei sistemi informatici è una componente cruciale per la gestione efficiente e sicura delle infrastrutture IT. Questo processo consiste nella continua osservazione e analisi dei vari componenti di un sistema informatico, inclusi server, reti, applicazioni e database, al fine di garantire prestazioni ottimali, sicurezza e disponibilità. Il monitoraggio permette di identificare tempestivamente anomalie, guasti e potenziali minacce, consentendo interventi rapidi per minimizzare l'impatto sulle operazioni aziendali.

L'utilità del monitoraggio dei sistemi informatici risiede nella sua capacità di fornire una visione completa e in tempo reale dello stato di salute dell'infrastruttura IT. Questo consente ai responsabili IT di prendere decisioni informate e proattive, migliorando la gestione delle risorse e riducendo il rischio di interruzioni non pianificate. Attraverso il monitoraggio continuo, è possibile rilevare problemi di prestazioni, configurazioni errate e vulnerabilità di sicurezza prima che diventino critici, migliorando così la resilienza complessiva del sistema.

Argentea installa su tutte le proprio virtual machine, agent di monitoraggio, agent EDR e agent VMDR.

13.1 VULNERABILITY MANAGEMENT

Argentea adotta un processo continuo per l'identificazione e la gestione delle vulnerabilità nei propri sistemi, suddiviso nelle seguenti fasi principali:

1. **Host Discovery**
   Viene effettuata la rilevazione degli host attivi all'interno delle reti target, con il loro censimento in un sistema di inventario centralizzato. Gli asset vengono classificati tramite etichette (tag) che ne indicano la criticità e la funzione.

2. **Vulnerability Assessment**
   Sugli host identificati vengono eseguite scansioni automatiche per rilevare vulnerabilità note, secondo lo standard CVE (Common Vulnerabilities and Exposures). Le scansioni individuano software obsoleti, configurazioni errate o patch mancanti, fornendo report dettagliati utili alla valutazione del rischio.

3. **Vulnerability Management**
   Le vulnerabilità rilevate vengono gestite attraverso piani di mitigazione che includono: applicazione di patch, aggiornamenti software, modifica delle configurazioni o misure compensative (es. isolamento degli asset critici). Il processo è ciclico e supportato da politiche interne che assicurano interventi tempestivi e tracciabili.

Attraverso questo approccio, Argentea garantisce una gestione proattiva delle minacce e una riduzione continua del livello di rischio IT.

13.2 GESTIONE DEI LOG

La gestione dei log (log management) è un elemento essenziale per garantire la sicurezza, la conformità normativa e l'efficienza operativa. Un sistema efficace consente di raccogliere, centralizzare, analizzare e archiviare i log generati da server, firewall, applicazioni e dispositivi di rete, fornendo informazioni critiche per la gestione IT e la risposta agli incidenti.

Argentea adotta una raccolta continua e centralizzata dei log attraverso sistemi di monitoraggio (SIEM/SOC), utilizzando protocolli sicuri per garantirne la trasmissione protetta. L'analisi automatizzata consente di individuare anomalie e potenziali minacce, mentre il team di sicurezza effettua controlli in tempo reale per rilevare e gestire eventuali incidenti.

I log vengono archiviati in modo sicuro, garantendone l'integrità e la disponibilità, e sono conservati per un periodo minimo di sei mesi, nel rispetto delle normative vigenti e delle policy aziendali. In caso di eventi critici, i log rappresentano una fonte indispensabile per le attività investigative.

14. PRIVACY POLICY

Nel trattamento dei dati personali, Argentea garantisce il rispetto dei seguenti principi generali:

- **Diritto alla protezione dei dati personali**: ogni individuo ha il diritto che il trattamento dei suoi dati personali avvenga secondo modalità che assicurino un elevato livello di tutela, nel rispetto dei suoi diritti e libertà fondamentali, nonché della sua dignità, con particolare riferimento alla riservatezza e all'identità personale.
- **Principio di accountability**[1]: (o di responsabilizzazione) i dati devono essere trattati in modo responsabilizzato da parte del Titolare che deve dimostrare, per ciascun trattamento, di aver agito in conformità alle disposizioni del Regolamento. Si tratta di un approccio proattivo risk based, cioè basato sulla valutazione del rischio del trattamento, con focus su obblighi e comportamenti finalizzati a prevenire e ridurre in modo effettivo ogni possibile danno. Il rischio inerente al trattamento è da intendersi sia per la sicurezza dei dati sia per gli impatti sulle libertà ed i diritti degli interessati. Tale approccio metodologico deve, quindi, seguire le logiche di Risk Assessment e Risk Management, al fine di individuare le misure tecniche ed organizzative idonee a garantire un adeguato livello di sicurezza.
- **Principio di finalità**: la raccolta dei dati deve essere collegata al fine del trattamento stesso. La finalità perseguita deve essere determinata, esplicita, legittima e non incompatibile con l'impiego dei dati.
- **Principio di liceità, correttezza e trasparenza:** i dati personali devono essere trattati in modo lecito, corretto e trasparente, sia con riguardo al contenuto delle informazioni sia alle modalità di raccolta e di utilizzo dei dati sia all'esercizio dei diritti da parte dell'interessato. Il trattamento dei dati personali deve avvenire in conformità alla legge, perseguire uno scopo legittimo, trovare fondamento in un'idonea base giuridica: necessità del trattamento, consenso dell'interessato (da esprimersi in relazione ad una o più finalità specifiche), adempimento di obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il Titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del Titolare o

[1] In particolare, l'accountability richiede l'aderenza ai principi generali del trattamento di cui all'art. 5, par. 1, GDPR. Inoltre, il Considerando 74 del GDPR definisce il contenuto del principio di responsabilizzazione attraverso la combinazione di due aspetti: 1) l'adozione da parte del Titolare del trattamento di misure adeguate - poste in essere tramite una valutazione concreta ex ante, ossia compiuta dal Titolare, caso per caso, prima di effettuare il trattamento - ed efficaci volte a rendere effettiva la protezione dei dati personali (cfr. art. 24, par. 1, GDPR); 2)la capacità del Titolare di dimostrare la conformità delle attività di trattamento alle disposizioni del Regolamento (e, qualora l'Autorità Privacy ne faccia richiesta, anche la concreta attuazione), il perché ha preso una determinata decisione e la documentazione delle scelte effettuate. Un secondo livello di responsabilità - oltre le norme imperative che introducono i requisiti minimi - invece, può rinvenirsi nell'adozione di misure volontarie, cioè quelle che rappresentano una garanzia aggiuntiva al rispetto dei principi fondamentali per la protezione dei dati, per ridurre ulteriormente i margini di rischio del trattamento.

di terzi cui i dati vengono comunicati. I dati trattati in violazione di questi principi non possono essere utilizzati. Sono vietati artifizi e raggiri nei confronti dell'interessato.

- **Principio di necessità del trattamento e di minimizzazione dei dati:** il Titolare deve trattare solo i dati di cui ha bisogno per raggiungere le finalità collegate a quel tipo di attività: la raccolta ed il trattamento dei dati, quindi, vanno effettuati limitatamente alle informazioni necessarie all'attività, riducendone al minimo l'utilizzo. Laddove le stesse finalità possano essere perseguite senza l'uso di dati personali, il trattamento deve riguardare solo dati anonimi oppure deve essere posto in essere adottando opportune modalità che permettano di identificare l'interessato solo in caso di necessità.
- **Principio di proporzionalità**: possono essere trattati i soli dati pertinenti e non eccedenti le finalità perseguite.
- **Principio di tutela dell'integrità del dato**: i dati personali devono essere trattati in modo da garantirne una sicurezza adeguata ai rischi di distruzione o perdita (anche accidentale), di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta. I dati devono essere custoditi e controllati in relazione alla natura dei dati stessi, alle specifiche caratteristiche del trattamento e alle conoscenze acquisite in base al progresso tecnico, attraverso l'adozione di adeguate misure tecniche ed organizzative.
- **Privacy by design**: necessità di prevedere sin dall'origine - cioè già in fase di ideazione e progettazione del trattamento dei dati e dei sistemi informatici e applicativi - una tutela dei dati personali attraverso logiche di minimizzazione e di disegno del trattamento, in linea con i principi del Regolamento. Il Titolare deve assicurare che i servizi/prodotti offerti che prevedono il trattamento dei dati personali siano, per impostazione predefinita, protetti da adeguate misure tecniche ed organizzative; in tal modo, si intende attuare efficacemente i principi di protezione dei dati e integrare le necessarie garanzie per soddisfare i requisiti del Regolamento e tutelare i diritti degli interessati (cfr. art. 25, par. 1, GDPR).
- **Privacy by default:** necessità di prevedere una tutela dei dati personali per impostazione predefinita, attraverso un processo che disciplini modalità di acquisizione, trattamento, protezione e diffusione dei dati personali. Il Titolare dovrà mettere in atto misure tecniche e organizzative adeguate in modo da garantire che, per impostazione predefinita, la raccolta dei dati personali sia limitata a quei dati strettamente necessari per ogni specifica finalità del trattamento (cfr. art. 25, par. 2, del GDPR). Inoltre, sin dall'inizio, sarà necessario determinare il periodo per il quale i dati personali raccolti dovranno essere conservati.

14.1 TRATTAMENTO DEI DATI PERSONALI

Ogni trattamento di dati personali deve avvenire nel rispetto dei seguenti principi carine:

- In primis, si può procedere ad un'attività di trattamento soltanto previo consenso espresso da parte dell'interessato o, in alternativa, nel caso in cui si rinvenga un fondamento normativo nel Regolamento o in un'altra fonte, sia essa nazionale o comunitaria. Infatti, secondo quanto disposto dall'art. 5, par 1, lett. a), GDPR e dal Considerando 39 GDPR, il trattamento dei dati personali deve essere lecito e corretto.
- Le modalità e la misura con cui vengono raccolti, utilizzati, consultati o comunque trattati i dati personali deve risultare trasparente alle persone fisiche (cc.dd. interessati) a cui tali dati appartengono; infatti, è necessario che le stesse informazioni e comunicazioni relative al trattamento dei dati personali siano facilmente accessibili e comprensibili, possibilmente attraverso l'impiego di un linguaggio che sia il più semplice e chiaro possibile. Lo stesso principio è applicabile all'identità del Titolare del trattamento, alle finalità perseguite e alle richieste formulate da parte delle persone fisiche interessate, relativamente all'esercizio dei loro diritti, quanto al trattamento di dati personali che le riguardano.
- Secondo quanto disposto dall'art. 5, par. 1, lett. d) GDPR, il Titolare del trattamento tratta i dati personali avendo cura che siano esatti e aggiornati; qualora non ricorressero tali caratteristiche, il Titolare deve mettere in atto tutte le misure ragionevoli affinché i dati inesatti siano rettificati o cancellati.
- Vi è l'obbligo a che il periodo di conservazione dei dati personali (c.d. data retention) sia limitato al tempo strettamente necessario. Ciò significa che il Titolare dovrà assicurarsi che i dati personali non siano conservati più del dovuto.

Infine, i dati personali dovrebbero essere sempre trattati in modo da garantirne integrità e riservatezza.

14.2 FINALITÀ DEL TRATTAMENTO

Secondo il disposto di cui all'art. 5, par. 1, lett. b) GDPR, i dati personali sono raccolti per finalità determinate, esplicite e legittime. Inoltre, i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento (c.d. principio di minimizzazione dei dati e secondo quanto riportato dal Considerando 39).

Non da ultimo, ai sensi dell'art. 5, par 1, lett. e) GDPR, i dati sono conservati in modo da permettere l'identificazione dell'interessato solo per il tempo necessario a conseguire le finalità del trattamento.

Ai sensi del Considerando 39, i dati personali dovrebbero essere trattati solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi. Inoltre, le finalità specifiche dovrebbero essere esplicite, legittime e precisate con chiarezza all'interessato al momento della raccolta dei suoi dati personali.

Si noti che il trattamento per finalità diverse da quelle per cui i dati personali sono stati raccolti in origine è consentito solo se compatibile con le finalità inizialmente previste per la raccolta di tali dati.

In particolare, per accertare la compatibilità di finalità di un ulteriore trattamento, spetterà al Titolare valutare:

- ogni nesso tra le finalità originarie e quelle successive (ad esempio, il contesto in cui i dati personali sono stati raccolti e le ragionevoli aspettative dell'interessato in base alla relazione che lo lega al Titolare del trattamento con riguardo all'ulteriore utilizzo);
- la natura dei dati personali trattati;
- le conseguenze dell'ulteriore trattamento sugli interessati;
- l'esistenza di garanzie adeguate nell'ulteriore trattamento previsto tanto quanto in quello originario.

Un'eventuale raccolta di dati successiva non potrà avvenire incompatibilmente con quella di finalità originarie. Tuttavia, tale divieto non opera nei seguenti casi:

- il trattamento ulteriore dei dati è necessario per perseguire finalità di archiviazione nel pubblico interesse o per finalità statistiche o di ricerca scientifica/storica;
- il trattamento trova fondamento in una norma di diritto internazionale, europeo o interno che costituisce una misura necessaria e proporzionata per salvaguardare obiettivi di interesse pubblico generale;
- il Titolare ha degli interessi legittimi che prevalgono su quelli dell'interessato.

14.3 INFORMATIVA

Quando necessario, Argentea consegnerà l'informativa all'interessato (disciplinata, nello specifico, dagli artt. 13 e 14 GDPR) prima di effettuare qualsiasi trattamento. Essa sarà comprensibile, trasparente e redatta in un linguaggio chiaro e semplice. Nel caso in cui i dati personali non siano raccolti direttamente presso l'interessato, l'informativa dovrà essergli fornita comunque entro un termine ragionevole – che non può superare un mese dalla raccolta – o al momento della comunicazione dei dati.

I contenuti dell'informativa sono elencati in modo tassativo. In particolare, il Titolare dovrà specificare:

- la propria identità e quella dell'eventuale rappresentante nel territorio italiano;
- i dati di contatto del Responsabile della protezione dei dati (RPD-DPO), ove esistente;
- le finalità del trattamento;
- la base giuridica del trattamento;
- le categorie dei dati personali oggetto di trattamento;
- il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione;
- l'identità del Responsabile del trattamento, ove esistente;
- quali sono i destinatari dei dati;
- se trasferisce i dati personali in Paesi terzi;
- se il trattamento comporta processi decisionali automatizzati (tra cui, anche la profilazione);
- i diritti degli interessati (compreso quello di presentare un reclamo all'Autorità di controllo).

14.4 REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

Ai sensi dell'art. 30 GDPR, Argentel, in qualità di Titolare del trattamento, nella persona del proprio Legale Rappresentante, dovrà tenere un registro delle attività del trattamento svolte sotto la propria responsabilità.

Dovrà inoltre tenere un registro in qualità di Responsabile del trattamento per quanto concerne le categorie di attività relative al trattamento svolto per conto del Titolare.

15. GESTIONE DEI FORNITORI

Argentea ha adottato un approccio sistematico per garantire un adeguato livello di sicurezza delle informazioni e di continuità su tutta la propria supply chain.

L'Organizzazione ha istituito un sistema di qualificazione dei fornitori tramite albo, gestito dall'ufficio competente, al fine di valutarne l'idoneità e condurre un'analisi dei rischi associati, incluse minacce e vulnerabilità.

La selezione dei fornitori di servizi IT e cloud avviene sulla base di criteri predefiniti e strutturati, che includono una due diligence approfondita volta a verificare l'aderenza ai requisiti di sicurezza dell'Organizzazione. Tali requisiti sono derivati dalla propria Information Security Policy, dai vincoli normativi applicabili (es. GDPR, ISO/IEC 27001) nonché dalle esigenze contrattuali e operative di business.

I contratti stipulati includono clausole specifiche relative alla protezione delle informazioni, obblighi di riservatezza, diritti di audit e controllo, nonché modalità di gestione degli incidenti di sicurezza.

Le prestazioni dei fornitori sono oggetto di monitoraggio continuo, con audit periodici focalizzati su quelli considerati critici, per verificarne la conformità ai requisiti di sicurezza e garantire la continuità operativa. In caso di non conformità o incidenti, vengono attivate tempestivamente azioni correttive e preventive, accompagnate da un'efficace comunicazione con i fornitori coinvolti.

16. INCIDENT MANAGEMENT

Gli incidenti – che possono consistere in violazioni della sicurezza, malfunzionamenti dei sistemi o interruzioni del servizio – sono eventi che possono compromettere in maniera significativa il corretto funzionamento delle attività aziendali. Possono comportare gravi perdite economiche, danni reputazionali, sanzioni da parte delle autorità e conseguenze legali.

L'Incident Management è un processo operativo che consente di affrontare, in modo sistematico e ordinato, gli eventi critici che possono compromettere la sicurezza delle informazioni o dei sistemi. Questo processo include tutte le fasi che vanno dall'individuazione dell'incidente fino alla sua completa risoluzione e all'analisi successiva, finalizzata a prevenire il ripetersi dello stesso tipo di evento.

Argentea si è dotata di un processo di Incident Management suddiviso in cinque fasi principali:

1. Rilevazione (Detection)
2. Analisi e Classificazione
3. Contenimento
4. Eradicazione (Eradication)
5. Ripristino (Recovery)

16.1 RILEVAZIONE (DETECTION)

La prima fase riguarda l'identificazione dell'incidente. Può avvenire attraverso diversi canali, come:

- il monitoraggio dei sistemi IT (tramite strumenti SIEM, firewall, antivirus, IDS/IPS, ecc.),
- la ricezione di segnalazioni da parte degli utenti
- il riscontro da parte di team interni, come il SOC (Security Operations Center).

Un evento inizialmente può essere classificato come **allarme** (alert) e non necessariamente come incidente: è necessaria una valutazione iniziale per comprenderne la natura.

16.2 ANALISI E CLASSIFICAZIONE

Una volta identificato un potenziale incidente, è necessario procedere con un'analisi dettagliata per capirne le cause, determinare il perimetro, valutare la gravità e le conseguenze possibili.

In questa fase vengono anche classificati:

- il **tipo di incidente** (es. malware, accesso non autorizzato, perdita di dati, ecc.),
- il **livello di criticità**, che va da 0 (allarme semplice) fino a 4 (disastro).

Si utilizza una **matrice di valutazione** che tiene conto dell'impatto su:

- persone (es. sicurezza fisica, benessere),
- aspetti economici (es. danni finanziari diretti e indiretti),
- reputazione dell'organizzazione.

16.3 CONTENIMENTO

Questa fase mira a limitare l'impatto dell'incidente e a impedire che si propaghi ad altri sistemi o reti. Le azioni di contenimento possono essere distinte in:

- **A breve termine**, come il blocco degli account compromessi, l'isolamento della macchina coinvolta, la disconnessione da internet, l'inserimento di regole temporanee nel firewall e il backup immediato dei dati.
- **A lungo termine**, come l'aggiornamento dei software vulnerabili, l'applicazione di patch, il rafforzamento delle policy di sicurezza o il cambiamento delle configurazioni critiche.

Durante il contenimento, la comunicazione è fondamentale. Devono essere avvisati i referenti interni e, se necessario, anche le autorità competenti o i clienti coinvolti.

16.4 ERADICAZIONE

Dopo aver contenuto l'incidente, bisogna eliminare la causa principale. L'eradicazione prevede:

- la rimozione di malware o software malevolo,
- la bonifica dei sistemi infetti,
- l'eliminazione di account non autorizzati,
- e il ripristino di configurazioni sicure.

Può includere anche un'**analisi forense** per comprendere l'origine e le modalità dell'attacco, oltre a verificare che non siano presenti ulteriori minacce latenti nel sistema.

16.5 RIPRISTINO (RECOVERY)

Una volta rimossa la minaccia, si passa al ripristino del normale funzionamento dei servizi. Questa fase include:

- il ripristino dei dati da backup affidabili,
- la riattivazione delle funzionalità compromesse,
- e l'effettuazione di test per assicurarsi che i sistemi siano sicuri e stabili.

Il ripristino deve avvenire **in modo controllato e graduale**, con test di verifica, per evitare di reinserire elementi compromessi nell'ambiente produttivo. È importante anche documentare tutte le azioni intraprese e informare gli utenti coinvolti.

Una volta risolto l'incidente, è importante condurre un'analisi "post-incident review". Questa fase serve a:

- raccogliere tutte le informazioni sull'accaduto,
- capire cosa ha funzionato e cosa no nella gestione,
- identificare eventuali carenze nei controlli o nelle procedure,
- e proporre **azioni correttive o migliorative**, come:
    - l'aggiornamento delle policy di sicurezza,
    - l'introduzione di nuovi strumenti di monitoraggio,
    - o la formazione mirata del personale.

Inoltre, se l'incidente ha coinvolto dati personali o sensibili, è necessario assicurarsi che siano rispettati gli obblighi previsti dal GDPR, come la notifica all'autorità garante o agli interessati.

16.6 FIGURE COINVOLTE

Nel processo di incident management partecipano diverse figure chiave, tra cui:

- **Responsabile del Monitoraggio dei Sistemi (RMS)**, che tiene traccia dei log e segnala eventuali anomalie.
- **Responsabile della Comunicazione**, che gestisce le comunicazioni interne ed esterne, incluse le relazioni con gli stakeholder e, se necessario, con i media.
- **Incident Response Team (IRT)**, composto da specialisti tecnici e referenti aziendali, attivato in base al tipo e alla gravità dell'incidente.
- **DPO**, nel caso di eventi che interessano dati personali

16.7 TIPOLOGIE E CLASSIFICAZIONE DEGLI INCIDENTI

La criticità dell'incidente viene espressa secondo una scala ordinale a quattro valori o livelli di impatto, secondo la seguente classificazione:

- Livello 0 = allarme;
- Livello 1 = Incidente endo-organizzativo;
- Livello 2 = Incidente sistemico;
- Livello 3 = Data Breach;
- Livello 4 = Disastro