

# INFORMATION SECURITY POLICY

---

<b>Stato</b>	<b>Redatto e aggiornato da</b>	<b>Rivisto e approvato da</b>
Approvato	RSGI	Amministratore Delegato
	30/03/2026	01/04/2026

## LISTA DI DISTRIBUZIONE

A tutti gli stakeholder



CLASSIFICAZIONE DOCUMENTO: **PUBBLICO**

## STORIA DELLE MODIFICHE APPORTATE

VERSIONE	DATA	PARAGRAFO	MODIFICHE
00	01/04/2026	-	Prima stesura nel nuovo sistema di gestione



## SOMMARIO

<b>1. SCOPO</b>	<b>5</b>
<b>2. CAMPO DI APPLICAZIONE</b>	<b>5</b>
<b>3. NORMATIVA</b>	<b>5</b>
<b>4. CERTIFICAZIONI E POLITICHE</b>	<b>5</b>
<b>5. RUOLI E RESPONSABILITÀ</b>	<b>6</b>
<b>6. ANALISI DEI RISCHI</b>	<b>8</b>
<b>7. MISURE PER IL PERSONALE DIPENDENTE</b>	<b>9</b>
7.1 FORMAZIONE E CONSAPEVOLEZZA	9
<b>8. CLASSIFICAZIONE DELLE INFORMAZIONI</b>	<b>9</b>
8.1 PRINCIPI GENERALI	9
8.2 CRITERI DI CLASSIFICAZIONE	10
8.3 CRITERI DI CLASSIFICAZIONE	11
8.3.1 CANCELLAZIONE DEI DATI	11
8.4 TRASFERIMENTO DELLE INFORMAZIONI	12
8.4.1 TRASMISSIONE SICURA SU RETI PUBBLICHE	12
8.4.2 CONDIVISIONE DEI DATI	12
8.5 CRITTOGRAFIA	12
8.5.1 CRITTOGRAFIA AT REST	12
8.5.2 CRITTOGRAFIA IN TRANSIT	13
<b>9. CONTROLLO DEGLI ACCESSI LOGICI</b>	<b>13</b>
9.1 PRINCIPI IN MATERIA DI CONTROLLO DEGLI ACCESSI	14
9.2 ASSEGNAZIONE, MODIFICA E REVOCA DELLE UTENZE DI DOMINIO	14
9.3 AMMINISTRATORI DI SISTEMA	15
9.4 ACCESSO DEI CLIENTI AI SERVIZI SAAS ARGENTEA	15
9.5 UTENZE DEI CLIENTI	15
<b>10. CONTROLLO DEGLI ACCESSI FISICI</b>	<b>15</b>
<b>11. SVILUPPO SICURO DEL SOFTWARE</b>	<b>16</b>
<b>12. GESTIONE DELL'INFRASTRUTTURA</b>	<b>16</b>
12.1 NETWORKING	17
12.2 BACKUP	17
12.3 DISASTER RECOVERY	17
12.4 CESSAZIONE DEL SERVIZIO CLOUD	17
<b>13. MONITORAGGIO DEI SISTEMI</b>	<b>18</b>
13.1 VULNERABILITY MANAGEMENT	18
13.2 GESTIONE DEI LOG	19
<b>14. PRIVACY POLICY</b>	<b>19</b>
14.1 TRATTAMENTO DEI DATI PERSONALI	20
14.2 FINALITÀ DEL TRATTAMENTO	21



14.3 INFORMATIVA	21
14.4 REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO	22
<b>15. GESTIONE DEI FORNITORI</b>	<b>22</b>
<b>16. INCIDENT MANAGEMENT</b>	<b>22</b>
16.1 RILEVAZIONE (DETECTION)	22
16.2 ANALISI E CLASSIFICAZIONE	23
16.3 CONTENIMENTO	23
16.4 ERADICAZIONE	23
16.5 RIPRISTINO (RECOVERY)	23
16.6 FIGURE COINVOLTE	24
16.7 TIPOLOGIE E CLASSIFICAZIONE DEGLI INCIDENTI	24



## 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	<ul style="list-style-type: none"><li>➤ 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).</li><li>➤ Progettazione, sviluppo, manutenzione, installazione, erogazione e assistenza di sistemi integrati di pagamento multibanca.</li><li>➤ Progettazione ed erogazione di servizi di Conservazione a norma di documenti informatici.</li></ul>
Sistema di Gestione per la prevenzione della corruzione (ISO 37001:2016)	2024	<ul style="list-style-type: none"><li>➤ 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).</li><li>➤ Progettazione, sviluppo, manutenzione, installazione, erogazione e assistenza di sistemi integrati di pagamento multibanca.</li><li>➤ Progettazione ed erogazione di servizi di Conservazione a norma di documenti informatici.</li></ul>
Sistema di Gestione della Sicurezza	2020	<ul style="list-style-type: none"><li>➤ Progettazione, sviluppo, manutenzione,</li></ul>



delle Informazioni (ISO 27001:2022)		<p>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).</p> <ul style="list-style-type: none"> <li>➤ Progettazione, sviluppo, manutenzione, installazione, erogazione e assistenza di sistemi integrati di pagamento multibanca.</li> <li>➤ Progettazione ed erogazione di servizi di Conservazione a norma di documenti informatici.</li> </ul>
Estensione alle linee guida 27017 e 27018	2020	<ul style="list-style-type: none"> <li>➤ 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).</li> <li>➤ Progettazione ed erogazione di servizi di Conservazione a norma di documenti informatici.</li> </ul>

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**
  - Predisporre 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 gestisce le comunicazioni in caso di violazioni
- **IRT – Incident Response Team (o Comitato di Crisi)**
  - 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 eradicazione, 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 il 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 practices di sicurezza e privacy.
- **Referente CSIRT (e sostituto)**
  - Si occupa di interloquire con CSIRT Italia, ed effettuare le notifiche di cui agli articoli 25 e 26 del Decreto NIS2:
    - Notificare tempestivamente l'incidente al CSIRT Italia;
    - Confrontarsi con le competenze interne ed esterne necessarie per:
    - Valutare le misure di sicurezza attualmente in essere,
    - Definire e pianificare le misure da implementare per la risoluzione dell'incidente;
    - Coordinare le attività di comunicazione con gli altri responsabili aziendali e l'ente governativo.
    - Chiudere l'incidente quando tutte le attività in carico sono state evase.
- **Punto di contatto (e sostituto)**
  - Figura designata per interfacciarsi con ACN e applicare le disposizioni del Decreto NIS2.
  - Supervisiona lo stato complessivo della sicurezza, rischi e continuità operativa.
  - Approva il piano di gestione degli incidenti (IRP Incidente Response Plan) e insieme alla Direzione lo rivede periodicamente e comunque almeno ogni due anni, nonché qualora si verificano incidenti significativi, integrando le relative lezioni apprese, o mutamenti dell'esposizione alle minacce e ai relativi rischi.
- **Business Continuity Manager (e sostituto)**
  - Identifica i processi aziendali critici e definisce i tempi di recupero necessari (RTO) e la tolleranza alla perdita di dati (RPO).
  - Analizza le minacce (cyber, indisponibilità di sedi, guasti tecnologici o assenza di personale) che potrebbero interrompere l'attività.
  - Definisce le soluzioni pratiche per continuare a operare durante un incidente (es. lavoro da remoto, siti di Disaster Recovery, procedure manuali).
  - Redige assieme al RSGI e mantiene aggiornata la documentazione ufficiale contenente le procedure di emergenza.
  - Coordina il Comitato di Crisi durante un evento avverso, fungendo da ponte tra la Direzione, l'IT e le altre funzioni aziendali.
  - Organizza esercitazioni periodiche per verificare che i piani siano efficaci e che il personale sappia come reagire.
  - Aggiorna i piani basandosi sui risultati dei test o sulle "lezioni apprese" dopo un incidente reale (Lessons Learned).
  - Assicura che le strategie di recupero siano allineate ai requisiti di sicurezza informatica e agli obblighi di notifica verso le autorità.

## 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 annuali) 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 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.

- **Segrete:** sono informazioni riguardanti dati personali dei Clienti o informazioni strategiche per il business (a titolo esemplificativo e non esaustivo: architetture di produzione che costituiscono il know-how aziendale, audit di terze parti o interni che evidenziano criticità, future acquisizioni, future assunzioni di manager strategici, ogni informazione che può essere usata da un attaccante contro l'Organizzazione);
- **Riservate:** sono i dati personali dell'Organizzazione e ogni informazione riguardante documenti che sono identificativi del modo di lavorare al nostro interno (a titolo esemplificativo e non esaustivo: audit interni o di terze parti effettuati per essere comunicati a clienti e che non evidenziano criticità se non in modo aggregato);
- **Pubbliche:** sono informazioni che possono essere divulgate sia internamente che esternamente all'Organizzazione.

Tale classificazione si applica a:

- Documenti di sistema (politiche, procedure, istruzioni di lavoro, modelli);
- Evidenze raccolte durante le attività di audit;
- Ogni tipo di documento redatto in esecuzione delle attività aziendali.

La classificazione viene fatta dal/dalla redattore/redattrice del documento.

In caso di contraddittorio sulla classificazione assegnata, sarà il/la Referente del Sistema di Gestione implementato a determinare la stessa.

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
Pubbliche	Nulla	Non significativo
Riservate	Media	Moderato
Segrete	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 dalle 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 cessa 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 viene debitamente tracciata e approvata.

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 dai reparti competenti 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 è prevista un'autenticazione a due fattori (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, Argentea, 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 e presente nel registro del trattamento.

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 rilevatori di fumo e strumenti antincendio che vengono controllati periodicamente;
- è garantita la sicurezza dei badge 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 di Argentea sono certificati:

- ISO 9001:2015
- ISO 27001:2013 con estensioni 27017:2015 e 27018:2019
- ISO 22301 - Business Continuity
- ISO/IEC 20000 - Service Management

e qualificati come Q12 su ACN Marketplace.

Essi 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 dai propri Cloud Service Provider (CSP).

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 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.

**Fornitore del servizio cloud:** GPI SpA

**Sede legale:** Via Ragazzi del '99, n.13

**Tipologia di servizio:** IaaS (Infrastructure as a Service)

**Certificazioni CSP:**

- certificazione ISO 9001:2015
- certificazione ISO 27001:2013
- certificazioni ISO 27017:2015 e 27018:2019
- certificazione ISO 22301 - Business Continuity
- certificazione ISO/IEC 20000 - Service Management
- conformità allo standard ISO 9001:2015
- conformità allo standard ISO 27001
- conformità allo standard ISO 22301 - Business Continuity
- conformità allo standard ISO/IEC 20000 - Service Management



- ACN Marketplace QI2 - Scheda IN-139

Localizzazione dei datacenter

- Italy, GPI SpA
- Italy, Elmec Informatica Spa
  - ACN Marketplace QI2 - IN-1791

**Fornitore del servizio cloud:** Zucchetti SpA

**Sede legale: Tipologia di servizio:** IaaS (Infrastructure as a Service)

**Certificazioni CSP:**

- certificazione ISO 9001:2015
- certificazione ISO 27001:2013
- certificazioni ISO 27017:2015 e 27018:2019
- conformità allo standard ISO 22301 - Business Continuity
- conformità allo standard ISO/IEC 20000 - Service Management
- ISO 14064-1:2018
- ISO/IEC 27701:2019
- BS 10012:2017
- ISO 14001:2015
- UNI/PDR 125:2022
- ACN Marketplace QI2 - Scheda IN-316

Localizzazione dei datacenter:

- Italy, Lodi – Via Solferino,1 (26900), Zucchetti Spa
- Italy, Roma - Via di Tor Cervara 28, Zucchetti Spa
- Italy, Siziano (PV) - Via Marche 8-10, 27010, Zucchetti Spa
- Italy, Lodi - Via Polenghi, 13 (26900), Zucchetti Spa

## 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 (definito su base contrattuale e nel registro del trattamento).



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
- Agent 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<sup>1</sup>:** (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'ideonea 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 di terzi cui i dati vengono comunicati. I dati trattati in violazione di questi principi non possono essere utilizzati. Sono vietati artifici 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

---

<sup>1</sup> 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.



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 ricorrerono 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, Argentea, 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.

<p><b>Incident</b></p>	<p>È <b>qualsiasi evento che compromette o ha il potenziale di compromettere</b> uno o più dei seguenti aspetti:</p> <ul style="list-style-type: none"> <li>● <b>Disponibilità</b> dei sistemi o dei dati,</li> <li>● <b>Integrità</b> delle informazioni,</li> <li>● <b>Riservatezza</b> dei dati,</li> <li>● <b>Autenticità</b> dei servizi e delle comunicazioni.</li> </ul>
<p><b>Incident significativo</b></p>	<p>Un incidente è considerato significativo se:</p> <ol style="list-style-type: none"> <li>a. ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato;</li> <li>b. ha avuto ripercussioni o è idoneo a provocare ripercussioni su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli.</li> </ol> <p>ACN identifica le seguenti tipologie di Incident significativo:</p> <ul style="list-style-type: none"> <li>● Perdita di riservatezza, verso l'esterno, di dati digitali di sua proprietà (del soggetto interessato) o sui quali esercita il controllo anche parziale.</li> <li>● Perdita di integrità, con impatto verso l'esterno, di dati di sua proprietà o sui quali esercita il controllo anche parziale.</li> <li>● Violazione dei livelli di servizio attesi dei suoi servizi e/o delle sue attività, sulla base dei livelli di servizio atteso (SL).</li> <li>● Accesso non autorizzato, o con abuso dei privilegi concessi, ai dati digitali di sua proprietà o sui quali esercita il controllo anche parziale.</li> </ul>
<p><b>Incident data breach</b></p>	<p>Violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.</p>

RUOLO	RESPONSABILITA'
CSIRT	Destinatario delle segnalazioni degli incidenti significativi.
Garante Privacy	Destinatario delle comunicazioni di data breach.



<b>Punto contatto/ sostituto punto contatto</b>	Figure designate per interfacciarsi con il CSIRT e applicare le disposizioni del Decreto NIS2 (rif. norm. art. 4 e 5 DetACN 19/09/2025). Supervisiona lo stato complessivo della sicurezza, rischi e continuità operativa. Approva il piano di gestione degli incident (IRP Incidente Response Plan) e insieme alla Direzione lo riasamina periodicamente e comunque almeno ogni due anni, nonché qualora si verificano incidenti significativi, integrando le relative lezioni apprese, o mutamenti dell'esposizione alle minacce e ai relativi rischi.
<b>Referente CSIRT/ Sostituti Referenti CSIRT</b>	È una persona fisica designata dal Punto di contatto. Ha il compito di interloquire con lo CSIRT Italia, ed effettuare le notifiche di cui agli articoli 25 e 26 del Decreto (rif. norm. art. 7 DetACN 19/09/2025).
<b>DPO</b>	Responsabile per la gestione di presunti data breach e data breach, nonché della comunicazione al Garante Privacy.
<b>Incident Response Team (IRT)</b>	E' composto dalla Direzione Tecnica di Argentea e il personale dedicato alla risoluzione dell'incidente. Rileva e analizza gli incidenti; Contiene e rimuove la minaccia; Ripristina sistemi e servizi; Raccoglie evidenze e produce report tecnici;
<b>Comitato di Crisi</b>	Valuta le situazioni di emergenza, dichiara lo stato di disastro; Valuta l'impatto sul business; Prende decisioni strategiche e gestisce la comunicazione con gli stakeholder; Richiede l'attivazione dello stato di disastro e le procedure di BC e DR.; Da supporto nel piano di eradication, contenimento e mitigazione dell'incidente; Gestisce i rapporti interni e risoluzione dei conflitti di competenza; Dichiara la conclusione dello stato di disastro.
<b>Operatore</b>	Dipendente o collaboratore che segnala l'incident
<b>Direzione</b>	Approva il piano di gestione degli incident e insieme al punto di contatto e relativo sostituto lo riasamina periodicamente e comunque almeno ogni due anni, nonché qualora si verificano incidenti significativi, integrando le relative lezioni apprese, o mutamenti dell'esposizione alle minacce e ai relativi rischi.

## 16.1 RILEVAZIONE INCIDENT

La prima fase riguarda l'identificazione dell'incidente. La segnalazione può giungere attraverso diversi canali, come:

- Sistemi di monitoraggio
- Fonti di cybersecurity esterne al Datacenter
- Servizio SOC (Security Operations Center)
- Rilevazione sistemistica
- Segnalazione pervenuta da cliente
- Segnalazione pervenuta da partner
- Segnalazione pervenuta da fornitore
- Segnalazione pervenuta da autorità pubblica
- Segnalazione pervenuta da reparti interni



All'atto della ricezione della segnalazione, ogni operatore è in grado di eseguire una catalogazione della richiesta attraverso lo strumento di assistenza utilizzato. Un evento inizialmente può essere classificato come allarme (alert) e non necessariamente come incidente: è necessaria una valutazione iniziale per comprenderne la natura.

## 16.1. GESTIONE INCIDENT

In caso di Incident, l'operatore approfondisce con la Direzione Tecnica di Argentea la valutazione della segnalazione in quanto è necessario attribuire una priorità per la relativa risoluzione.

La valutazione avviene basandosi su due elementi:

- **Impatto:** è la misura dell'effetto dell'incidente sull'ambiente applicativo dei Clienti;
- **Urgenza:** è la valutazione del tempo intercorso tra il problema/incidente e le ripercussioni sulla disponibilità, integrità e riservatezza.

Per la valutazione, l'operatore si riferisce alle seguenti tabelle.

**Tabella Impatti**

Tipologia	Gravità	Descrizione
Impatto 3	Alta	Intero ambiente applicativo del Cliente: ambiente bloccato o comunque non in condizioni tali da permettere una minima attività di business; seri rischi per disponibilità, integrità e riservatezza delle informazioni.  Blocco totale del servizio del cliente.
Impatto 2	Media	Limitazioni d'uso o blocchi di alcuni applicativi, sensibile calo di prestazioni, fruibilità per un numero inferiore di utenti rispetto a quelli previsti, potrebbero sorgere problemi di disponibilità, riservatezza e integrità.  Singolo utente bloccato o parte del servizio bloccato.
Impatto 1	Bassa	Situazioni non bloccanti, rallentamenti temporanei, alcune funzioni non pienamente fruibili, bassa probabilità di ripercussioni su disponibilità, integrità e riservatezza.

**Tabella Urgenze**

Tipologia	Livello	Descrizione
Urgenza 3	Alta	Ripercussioni immediate sul servizio
Urgenza 2	Media	Ripercussioni a breve termine– entro 8 ore.
Urgenza 1	Bassa	Ripercussioni oltre la giornata.

Il valore di Priorità della segnalazione viene definita in base all'incrocio dei due valori precedenti, come riportato nella seguente tabella.

**Tabella Priorità**

	Urgenza 1	Urgenza 2	Urgenza 3
Impatto 1	1	1	2
Impatto 2	1	2	3
Impatto 3	2	3	3

### FASE 1:

L'operatore identifica la segnalazione e gli attribuisce la categoria corretta definendone la priorità tramite apposito ticket.



#### **FASE 2:**

L'IRT a sua volta la segnalazione, identifica eventuali ulteriori gruppi da coinvolgere nel processo di analisi e insieme ad essi verifica anche la corretta attribuzione della categoria e la priorità assegnata.

#### **FASE 3:**

L'IRT a seconda della priorità assegnata, opera alla risoluzione della problematica nel rispetto dei tempi prefissati.

#### **FASE4:**

Una volta risolta la segnalazione e inviata la comunicazione di risoluzione al mittente e agli eventuali soggetti coinvolti, l'operatore che ha in carico la problematica può considerarla conclusa definendone il relativo stato nello strumento di post-vendita.

#### **Registrazione evento di incident**

Tutte le attività legate alla gestione dell'Incident, dal ricevimento della segnalazione, alla sua risoluzione e chiusura, sono registrate su appositi strumenti.

#### **Analisi Post Incident**

Al fine di curare il miglioramento continuo, periodicamente, per gli incident più rilevanti, viene effettuata un'analisi post-incidente per analizzare le cause dell'incidente ed eventuali risoluzioni definitive.

Lo storico degli incidenti intercorsi infatti può fornire una solida base per calcolare la probabilità di determinate tipologie di evento, rilevante altresì per l'analisi dei rischi. Inoltre, l'eventuale reiterazione di incidenti della stessa tipologia costituisce un allarme sintomatico di possibili vulnerabilità da analizzare. Le valutazioni operate e le azioni che si intende intraprendere devono essere documentate.

## **16.2. GESTIONE INCIDENT SIGNIFICATIVO**

### **VALUTAZIONE SULLA SIGNIFICATIVITÀ DELL'INCIDENTE**

Un incidente è considerato significativo se:

- **ha causato o è in grado di causare una grave perturbazione operativa dei servizi**
  - Impatto che compromette la continuità, disponibilità o funzionalità dei servizi essenziali erogati dall'organizzazione.
  - Un servizio è completamente non disponibile per migliaia di utenti

Ai fini dell'obbligo di notifica di cui all'articolo 25, nella definizione del livello di servizio atteso si considerano come incidenti significativi di base almeno i casi identificati nel documento NIS2\_Regola\_IncidenteSignificativo\_v0.

- **ha causato o è in grado di causare perdite finanziarie per il soggetto interessato;**
  - perdita finanziaria diretta per l'entità interessata superiore a **500.000 EUR o al 5%** del fatturato annuo totale dell'entità nell'anno finanziario precedente, a seconda di quale sia inferiore
  - l'incidente ha causato o può causare l'esfiltrazione di segreti commerciali

La perdita deve essere tale da influire in modo significativo sulla stabilità economica o operativa dell'organizzazione.

- **ha avuto ripercussioni o è idoneo a provocare ripercussioni su altre persone fisiche o giuridiche causando perdite materiali**
  - l'incidente ha causato o può causare la morte di una persona fisica;
  - l'incidente ha causato o può causare danni considerevoli alla salute di una persona fisica;
- **ha avuto ripercussioni o è idoneo a provocare ripercussioni su altre persone fisiche o giuridiche causando perdite immateriali considerevoli.**
  - si è verificato un accesso riuscito, sospettosamente malevolo e non autorizzato ai sistemi di rete e informazione, capace di causare gravi interruzioni operative;
  - gravi danni reputazionali;
  - violazione della privacy

### **NOTIFICA INCIDENTE SIGNIFICATIVO**



Se un operatore riceve la segnalazione di un incidente che può provocare gravi perturbazioni del servizio, gravi danni finanziari o danni materiali o immateriali a persone fisiche o giuridiche deve darne immediata comunicazione al referente CSIRT o al suo Sostituto. In questa fase e nelle successive, l'IRT convoca il Comitato di Crisi, che parteciperà attivamente e verrà coinvolta in tutte le fasi fino alla risoluzione del problema (anche tramite War Room).

È necessario attivare le seguenti fasi:

### **Fase 1: PREPARAZIONE ALLA NOTIFICA – PRE ALLARME**

A seguito della rilevazione di un incidente significativo, viene avviata immediatamente una fase preparatoria alla notifica con l'obiettivo di raccogliere le informazioni minime per garantire che la comunicazione permetta al CSIRT Italia un'attivazione proporzionata alla potenziale criticità ed ai potenziali impatti di natura sistemica derivanti dall'incidente stesso. Rientrano in tale fase le attività di preparazione della segnalazione dell'incidente, ove prevista.

La prenotifica deve essere inviata **entro 24 ore** senza indebito ritardo, da quando si è venuti a conoscenza.

La **pre-notifica deve contenere:**

1. Dati identificativi del soggetto che segnala.
2. Informazioni essenziali sull'incidente (tipo, tempistiche iniziali, sistemi coinvolti).
3. Eventuale sospetto di origine illecita/malevola.
4. Eventuale probabile impatto transfrontaliero.
5. Richiesta di assistenza, se necessaria.

Il CSIRT fornisce, entro 24 ore dal ricevimento del preallarme, un riscontro iniziale sull'incidente e offre, su richiesta, orientamenti e consulenza.

### **Fase 2: NOTIFICA AL CSIRT ITALIA**

Una volta raccolte le informazioni necessarie ad effettuare la segnalazione, ove prevista, e/o la notifica, si dovrà procedere, **senza ingiustificato ritardo e ove possibile entro 72 ore da quando si è venuti a conoscenza dell'incidente**, alla compilazione di un modulo online disponibile sul sito internet del CSIRT Italia: <https://www.csirt.gov.it/segnalazione> oppure all'invio di una PEC e fornire le seguenti indicazioni ad integrazione di quanto già comunicato nella prenotifica (FASE 1):

- tipologia di impatto
- date e ora di rilevamento dell'incidente;
- ulteriori dettagli dell'incidente, come ad esempio altri sistemi impattati o informazioni rilevanti;
- lista degli IOC (Indicator Of Compromise) raccolti fino al momento della notifica;
- evidenze rilevate (es. sample di malware, ransom note).

### **Fase 3: GESTIONE DELLA NOTIFICA**

Su richiesta del CSIRT, viene inviata una relazione intermedia sugli aggiornamenti dell'incidente

### **Fase 4: CHIUSURA DELL'INCIDENTE**

Una volta definite le attività di ripristino, viene data immediata comunicazione al CSIRT che ha la facoltà di richiedere una relazione tecnica dell'incidente riguardante gli aspetti significativi dell'incidente, quali:

- una valutazione delle conseguenze dell'impatto sui beni ICT;
- la descrizione delle azioni di recupero e ripristino intraprese.

Entro un mese dalla prima segnalazione, deve essere inviata al CSIRT una relazione finale (o, se l'incidente è ancora in corso, una relazione sui progressi fatti).

Il Referente CSIRT (o i suoi sostituti) ha la responsabilità di:

- Notificare tempestivamente l'incidente al CSIRT Italia;
- Confrontarsi con le competenze interne ed esterne necessarie per:
  - Valutare le misure di sicurezza attualmente in essere,
  - Definire e pianificare le misure da implementare per la risoluzione dell'incidente;
- Coordinare le attività di comunicazione con gli altri responsabili aziendali e l'ente governativo.

Il Referente CSIRT o suo sostituto ha il compito di chiudere l'incidente quando tutte le attività in carico sono state evase.



## 16.3. GESTIONE DATA BREACH

Ai sensi dell'art. 33 del Regolamento UE n. 2016/679, il Titolare del trattamento, in caso sia consapevole di una violazione dei Dati personali trattati, è tenuto:

- a informare il Garante Privacy entro e non oltre le 72 ore successive all'avvenuta conoscenza della violazione (a meno che non sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà degli Interessati);
- nel caso in cui tale violazione sia suscettibile di comportare un rischio elevato per i diritti e le libertà degli interessati, a informare senza ritardo anche gli stessi interessati.

Nel caso in cui il Garante dovesse presentare reclamo in merito a quanto sopra, lo stesso dovrà essere registrato nell'apposito registro secondo il modello MOD Registro reclami garante.

### Rilevazione e segnalazione del presunto data breach

Ciascun incaricato del trattamento (dipendente e/o collaboratore) è obbligato a segnalare tempestivamente ogni caso di incidente informatico e/o ad archivi cartacei di cui sia venuto a conoscenza e ogni evento che potrebbe potenzialmente condurre ad una violazione di dati personali.

La segnalazione deve essere fatta al Responsabile della Comunicazione di Argentea oppure all'Amministratore Delegato che coinvolgono il DPO, inviando una e-mail all'indirizzo: [dpo@zucchetti.it](mailto:dpo@zucchetti.it), contenente una descrizione di quanto rilevato. Deve inoltre essere tracciata la segnalazione tramite ticket QUAL – Data Breach.

### Analisi del presunto data breach

A seguito della segnalazione, il DPO congiuntamente al segnalatore, al Responsabile della Comunicazione o all'AD e al Incident Response Team (IRT) di Argentea, elaborano una valutazione al fine di verificare se nell'incidente rilevato siano stati effettivamente violati dati personali trattati dalla società, in qualità di Titolare del trattamento.

Se la violazione è relativa all'azienda come Titolare, sarà il DPO a fare le comunicazioni agli enti preposti; se la violazione riguarda l'azienda come responsabile del trattamento, si passa al punto successivo.

Nel caso in cui, dall'analisi effettuata, emerga che siano stati effettivamente violati dati personali, il DPO compila il modulo "MOD Comunicazione incident responsabile".

### Risposta e notifica del data breach

La precedente fase di analisi fornisce gli strumenti necessari a identificare e valutare le conseguenze negative e gli impatti causati dall'incidente rilevato.

*Titolare del trattamento:* nel caso in cui risulti improbabile che l'incidente presenti rischi per i diritti e le libertà degli interessati, la notifica all'Autorità Garante e la comunicazione agli interessati risultano essere non obbligatorie. Tale valutazione è condivisa con il DPO.

Qualora, al contrario, dovesse risultare possibile che l'incidente abbia determinato una violazione dei dati che presenti rischi per i diritti e le libertà degli Interessati il DPO, procede alla notifica all'Autorità Garante,

attraverso l'iter presente sull'apposito canale web reperibile al seguente link: <https://servizi.gdpd.it/databreach/s/scelta-auth>.

La notifica viene effettuata all'Autorità Garante entro 72 ore dal momento in cui il Data Breach è stato rilevato.

Oltre a notificare il Data Breach all'Autorità Garante, deve essere valutata l'esigenza di procedere con la notifica anche ai soggetti interessati i cui dati siano stati violati: nel caso, il DPO predispone l'eventuale comunicazione all'interessato/agli interessati, a firma del titolare, da inviarsi nei tempi e nei modi che lo stesso, individuerà come più opportuna come specificato nell'art. 34 del GDPR e tenendo conto di eventuali indicazioni fornite dall'Autorità Garante.

Qualora non sia stato possibile fornire contestualmente tutte le informazioni obbligatorie, il DPO raccoglie, quanto prima, le informazioni supplementari e provvede a integrare, senza ritardo, la notifica già inoltrata all'Autorità di Controllo.



### **Registrazione**

L'ufficio privacy dovrà registrare il data breach o presunto data breach nel Registro delle violazioni (MOD Registro violazioni sicurezza privacy) .

