DigitalSuite Italia S.r.l.
Via Luigi Razza, 8- 20124 Milano
Email: dsi@digitalsuitegroup.com
P.IVA: 09345520960

Regolamento UE 2016/679 (GDPR)

# Misure Tecniche e Organizzative

## sulla sicurezza dei dati e sulla privacy adottate nell'ambito dei Servizi Cloud DigitalSuite erogati ai Clienti.


# GDPR Compliance - White Paper

7 gennaio 2019 - Versione 1.1

Cod. Doc.: DIGITALSUITE-MTO-Sicurezza-GDPR_UE 2016-679-V.1.1.docx

# Indice



## Disclaimer

Questo documento non fornisce alcun diritto legale a qualsiasi proprietà intellettuale in alcun prodotto DIGITALSUITE+. È possibile copiare e utilizzare questo white paper esclusivamente per scopi interni e di riferimento.

# Introduzione

*Il presente documento redatto da DIGITALSUITE ITALIA SRL (nel seguito anche "DIGITALSUITE") illustra le Misure Tecniche, Organizzative e di Sicurezza (MTO) applicate in materia di Data Privacy in applicazione del REGOLAMENTO UE 2016/679 (GDPR) nell'ambito delle proprie piattaforme applicative afferenti ai Servizi Cloud nelle modalità IAAS, PAAS, SAAS e altri analoghi Servizi (nel seguito anche "Servizi") erogati ai propri Clienti.*

## Trattamento dei Dati Personali

Nell'ambito delle disposizioni per il regolamento generale sulla protezione dei dati dell'Unione europea (REGOLAMENTO UE 2016/679 - GDPR) descritte nel presente documento, si specifica che:

- ✓ Le disposizioni afferenti al Responsabile del Trattamento ("Data Processor") secondo il GDPR si applicano al trattamento dei Dati del Cliente nell'ambito del GDPR da parte di DIGITALSUITE, per conto del Cliente.
- ✓ Ai fini delle disposizioni afferenti al Responsabile del Trattamento ("Data Processor") in ambito del GDPR, il Cliente e DIGITALSUITE concordano che il Cliente è il Titolare del Trattamento ("Data Controller") dei dati del Cliente e che DIGITALSUITE è il Responsabile del Trattamento ("Data Processor") di tali dati; quando il Cliente agisce come Responsabile del Trattamento ("Data Processor"), DIGITALSUITE ha il ruolo di Sub-responsabile del Trattamento ("Sub-processor").
- ✓ Le disposizioni afferenti al Responsabile del Trattamento ("Data Processor") in ambito del GDPR non si applicano quando DIGITALSUITE ha il ruolo di Titolare del Trattamento ("Data Controller") dei dati del cliente.

In tale contesto il Cliente quindi normalmente costituisce il Titolare del Trattamento dei propri Dati Personali, ovvero dichiara di aver ricevuto istruzioni ed essere stato autorizzato dagli eventuali altri Titolari a consentire a DIGITALSUITE il Trattamento dei Dati Personali secondo quanto stabilito nel relativo Contratto dei Servizi afferenti i Servizi IAAS, PAAS, SAAS e altri analoghi servizi di DIGITALSUITE sottoscritti. Il Cliente nomina DIGITALSUITE quale Responsabile del Trattamento dei Dati Personali del Cliente. Qualora ci fossero altri Titolari del Trattamento dei Dati Personali, il Cliente li identificherà e ne informerà DIGITALSUITE prima di fornire i loro Dati Personali.

- ✓ DIGITALSUITE tratterà i Dati Personali del Cliente secondo le istruzioni scritte del Cliente. L'ambito del Trattamento dei Dati Personali del Cliente è definito nel relativo Contratto dei Servizi.
- ✓ DIGITALSUITE si impegna a rispettare tutte le leggi e normative in materia di trattamento dei dati personali imposte dagli Stati dello Spazio Economico Europeo (SEE) e applicabili ai Responsabili del Trattamento dei Dati in relazione ai Servizi (Normative vigenti sulla Protezione dei Dati).

## Conformità al GDPR

DIGITALSUITE mette in atto tutte le Misure Tecniche e Organizzative adeguate a garantire che il trattamento è effettuato conformemente al REGOLAMENTO UE 2016/679 (GDPR). Tali misure sono riesaminate ed aggiornate qualora sia necessario.

DIGITALSUITE garantisce in particolare che:

- ✓ I trattamenti effettuati in qualità di Responsabile del Trattamento sono disciplinati da relativo Contratto del Servizio ed eventuali allegati, che vincola il Responsabile del Trattamento (DIGITALSUITE) al Titolare del Trattamento (il Cliente) e che stipula la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento e gli ulteriori aspetti previsti in tale materia.

- ✓ I dati personali vengono trattati su esclusiva istruzione documentata del Titolare del Trattamento (il Cliente), anche nel caso di eventuale trasferimento di dati verso un paese terzo o un'organizzazione internazionale.
- ✓ Tutte le persone di DIGITALSUITE ed eventuali propri Subresponsabili autorizzati al trattamento dei dati personali si sono impegnati alla riservatezza, oppure è stato instaurato un adeguato obbligo legale di riservatezza.
- ✓ Provvede a fornire idonea assistenza al Titolare del Trattamento (il Cliente) mediante misure tecniche ed organizzative adeguate allo scopo di soddisfare l'obbligo di dare seguito alle richieste per l'esercizio dei diritti dell'Interessato.
- ✓ Applica quanto ulteriormente previsto dall'Articolo 28: "Responsabile del trattamento" del REGOLAMENTO UE 2016/679 (GDPR).

DIGITALSUITE applica inoltre quanto previsto dall'Articolo 32: "Sicurezza del trattamento" del REGOLAMENTO UE 2016/679 (GDPR) e in particolare:

- ✓ Mette in atto misure tecniche ed organizzative adeguate al fine di garantire un idoneo livello di sicurezza adeguato al rischio. Tali misure comprendono se del caso:
  - la pseudonimizzazione e la cifratura dei dati personali;
  - la capacità di garantire permanentemente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e servizi di trattamento;
  - nel caso di incidente fisico o tecnico, la capacità del ripristino tempestivo della disponibilità ed accesso dei dati personali;
  - sono applicate idonee procedure di test, verifica e valutazione periodica in ambito dell'efficacia delle misure tecniche ed organizzative allo scopo di garantire l'adeguata sicurezza del trattamento.
- ✓ Il livello di sicurezza applicato è adeguato in particolare ai rischi afferenti al trattamento derivati in particolare dalla distruzione, perdita, modifica, divulgazione non autorizzata o accesso, accidentali oppure illegali, ai dati personali gestiti (trasmessi, conservati o comunque oggetto di trattamento).

# Misure Tecniche e Organizzative applicate

DIGITALSUITE implementa e mantiene le misure tecniche e organizzative (MTO) stabilite e qui descritte per garantire un livello di sicurezza adeguato al rischio connesso alle attività di diretta responsabilità di DIGITALSUITE. Le MTO sono soggette al progresso e ad ulteriore sviluppo tecnico e tecnologico. Pertanto, DIGITALSUITE si riserva il diritto di modificare le MTO a condizione che il funzionamento e la sicurezza dei Servizi qui in argomento erogati ai propri Clienti non vengano degradati.

Le misure tecniche e organizzative (MTO) si applicano a tutto il Contenuto, inclusi i Dati Personali del Cliente. Il Cliente si impegna a implementare le MTO appropriate nell'ambito della propria area di responsabilità come richiesto dalle Leggi sulla Protezione dei Dati in vigore.

## Misure di sicurezza

DIGITALSUITE in qualità di Responsabile del Trattamento dei Dati Personali, per quanto di propria competenza, è tenuto in forza di legge e del relativo Contratto dei Servizi sottoscritto dal cliente, per sé e per le persone autorizzate al trattamento che collaborano con la sua organizzazione, a dare attuazione alle misure di sicurezza previste dalla normativa pro tempore vigente in materia di trattamento di dati personali fornendo assistenza al Cliente nel garantire il rispetto della medesima. DIGITALSUITE, tenendo conto dello stato dell'arte e dei costi di

attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, deve assicurarsi che le misure di sicurezza predisposte ed adottate siano adeguate a garantire un livello di sicurezza adeguato al rischio, in particolare contro:

- ✓ distruzione, perdita, modifica, divulgazione non autorizzata o accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
- ✓ trattamento dei dati non consentito o non conforme alle finalità delle operazioni di trattamento.

Ciò premesso, DIGITALSUITE adotta tutte le preventive misure previste dalle norme e dalle prassi internazionali o comunque ritenute idonee al fine di ridurre al minimo i rischi di distruzione, perdita anche accidentale, accesso non autorizzato o comunque trattamento non consentito dei dati.

In base al regolamento GDPR, i rispettivi titolari del trattamento e della elaborazione dei dati devono implementare misure tecniche e organizzative appropriate per garantire un livello di sicurezza adeguato al rischio.

DIGITALSUITE gestisce una infrastruttura tecnologica globalmente progettata per fornire un livello di sicurezza all'avanguardia durante tutto il ciclo di vita dell'elaborazione delle informazioni.

Tale infrastruttura garantisce:

- ✓ La implementazione sicura dei servizi,
- ✓ L'archiviazione sicura dei dati con l'adozione di misure protettive per la privacy degli utenti,
- ✓ Comunicazioni protette tra i vari servizi,
- ✓ Comunicazioni protette e private con i Clienti su Internet
- ✓ Gestione sicura da parte dei relativi amministratori.

I Servizi di DIGITALSUITE vengono erogati mediante tale infrastruttura.

La sicurezza in ambito della infrastruttura tecnologica e di comunicazione ospitante le piattaforme applicative afferenti all'erogazione dei Servizi è progettata in base a vari livelli sovrapposti, a partire dal livello fisico afferente i data center che ospitano le piattaforme applicative a quello relativo alle risorse hardware, software e di comunicazione, fino ai processi utilizzati per il supporto della sicurezza operativa. Tale protezione multilivello è alla base di tutte le applicazioni ed i servizi erogati da DIGITALSUITE

## Disponibilità, integrità e resilienza

DIGITALSUITE progetta le componenti delle proprie piattaforme applicative afferenti all'erogazione dei Servizi in modo tale che implementino una ridondanza elevata. In caso di guasti all'hardware, al software o alla rete, i servizi vengono spostati automaticamente e immediatamente da una struttura fisica ad un'altra, in modo tale che le operazioni possano continuare senza interruzioni. Grazie a tale ridondanza della infrastruttura tecnologica e di comunicazione i Clienti sono protetti da possibili perdite di dati. Sono inoltre eseguiti backup automatici dei dati in base ad opportune rules in ambito di retention e relative modalità applicate.

## Test

DIGITALSUITE esegue periodicamente una serie di test, almeno annualmente, relativi al ripristino di emergenza ("Disaster Recovery") delle proprie piattaforme applicative afferenti all'erogazione dei Servizi. Ciò consente ai team delegati alla gestione dell'infrastruttura e delle applicazioni in ambito di coordinare le attività mirate a testare piani di comunicazione, scenari di failover, transizione operativa e altre misure da adottare in caso di emergenza. Tutti i team che partecipano alle operazioni per il ripristino di emergenza sviluppano ed applicano piani di test e analisi post-evento per documentare le informazioni ed i risultati ottenuti mediante i test.

## Crittografia

DIGITALSUITE utilizza in ambito delle proprie piattaforme applicative afferenti all'erogazione dei Servizi la crittografia HTTPS, attivata per impostazione predefinita per tutti gli utenti, per proteggere i dati in transito afferenti sia l'accesso degli utenti al portale web dei sistemi quanto nell'erogazione di Web Services (W3C).

## Controlli dell'accesso

I privilegi ed i livelli di accesso dei dipendenti di DIGITALSUITE applicative afferenti all'erogazione dei Servizi si basano sulla rispettiva mansione e ruolo operativo, utilizzando i principi del "privilegio minimo" ("least-privilege") e della "necessità di conoscere" ("need-to-know"), in funzione delle responsabilità definite per lo specifico dipendente. Le richieste di ulteriore accesso seguono un processo formale che prevede l'approvazione da parte del Titolare del trattamento oppure da parte di responsabili o altri dirigenti a seconda dei criteri di sicurezza stabiliti da DIGITALSUITE.

## Gestione delle vulnerabilità

Allo scopo di rilevare eventuali vulnerabilità relative alle piattaforme applicative afferenti all'erogazione dei Servizi, viene utilizzata una combinazione di strumenti sia disponibili in commercio sia realizzati internamente e specificatamente da DIGITALSUITE, nonché di test automatici e manuali per la verifica di possibili violazioni, applicazione di processi di controllo della qualità, analisi della sicurezza del software e audit. Tali strumenti ed attività sono finalizzati a rilevare eventuali problemi di progettazione e implementazione che potrebbero mettere a rischio i dati dei Clienti.

## Sicurezza dei servizi

I Clienti possono sfruttare le funzioni e le configurazioni previste nelle piattaforme applicative afferenti all'erogazione dei Servizi per proteggere ulteriormente i dati personali da possibili elaborazioni non autorizzate o illegali.

- ✓ *Password di Accesso:* La protezione delle credenziali di accesso rappresenta uno dei principi fondamentali della sicurezza delle informazioni, in particolare la creazione e la gestione delle password che costituiscono la principale contromisura agli accessi non autorizzati. Le password di accesso ai servizi utilizzate dagli utenti devono essere composte da minimo 6-8 caratteri e contenere almeno un carattere maiuscolo, una lettera minuscola, un numero ed un carattere speciale; le password richiedono il rinnovo obbligatorio almeno ogni sei mesi, inoltre il Cliente può richiedere che per le password degli utenti appartenenti alla propria organizzazione il termine della scadenza sia più restrittivo.

- ✓ *Amministrazione dei privilegi:* gli utenti del Cliente che detengono privilegi di amministrazione in ambito del servizio utilizzato possono gestire i privilegi afferenti gli utenti della propria organizzazione, sia in ambito di autorizzazione all'utilizzo dei vari servizi fruiti e quindi le relative informazioni elaborate, quanto alla rispettiva configurazione per l'utilizzo di tali servizi.

Su eventuale specifica richiesta, il Cliente può ottenere ulteriori informazioni ed approfondimenti in ambito della sicurezza afferente la progettazione dell'infrastruttura tecnologica ospitante i servizi fruiti, documentata mediante appositi white paper specifici. Le misure tecniche e organizzative sono soggette al progresso tecnico e all'ulteriore sviluppo. DIGITALSUITE verifica periodicamente l'adeguatezza delle misure di sicurezza adottate, valutando eventuali modifiche delle stesse in base alle mutate tecnologie. DIGITALSUITE comunica al Cliente/Titolare eventuali casi di accesso non autorizzato o non consentito o non conforme alle istruzioni ricevute ai dati nel termine di 72 ore o comunque senza ritardo.

DIGITALSUITE applica le misure di sicurezza, qui in precedenza descritte, al fine di garantire:

- ✓ se del caso, la pseudonimizzazione e la cifratura dei dati personali;

- ✓ la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- ✓ la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.

DIGITALSUITE nel suo ruolo di Responsabile del Trattamento, su richiesta del Cliente, coadiuva quest'ultimo nelle procedure davanti all'Autorità di Controllo competente e all'Autorità Giudiziaria in relazione alle attività rientranti nella sua competenza.

## Cancellazione e Restituzione dei Dati Personali del Cliente

Al termine delle operazioni di trattamento affidate, nonché all'atto della cessazione per qualsiasi causa del trattamento da parte di DIGITALSUITE, a discrezione del Cliente e su specifica richiesta di quest'ultimo, DIGITALSUITE sarà tenuta a:

- ✓ restituire al Titolare i dati personali oggetti del trattamento, oppure
- ✓ provvedere alla loro integrale distruzione salvi solo i casi in cui la conservazione dei dati sia richiesta da norme di legge od altri fini (contabili, fiscali, ecc.).

In entrambi i casi DIGITALSUITE provvederà a rilasciare al Cliente, dietro sua richiesta, apposita dichiarazione per iscritto contenente l'attestazione che presso DIGITALSUITE non esista alcuna copia dei dati personali e delle informazioni di titolarità del Cliente. Il Cliente si riserva il diritto di effettuare controlli e verifiche volte ad accertare la veridicità della dichiarazione.

# Approfondimenti sulle misure di sicurezza

In linea di principio la Sicurezza dei sistemi in ambito delle piattaforme applicative afferenti all'erogazione di Servizi Cloud nelle modalità IAAS, PAAS, SAAS e altri analoghi servizi viene garantita dalla robustezza del software di base e applicativo e dalla affidabilità delle apparecchiature e degli ambienti in cui essi sono collocati.

Le piattaforme applicative in ambito rispondono alle moderni criteri di security che sinteticamente possono essere così suddivisi:

| **Ambito di sicurezza** | **Caratteristiche** |
|---|---|
| **Sicurezza passiva** ***(sicurezza fisica)*** | Applicazione delle tecniche e strumenti di tipo *difensivo*, ovvero il complesso di soluzioni tecnico-pratiche il cui obiettivo è quello di impedire che utenti non autorizzati possano accedere a risorse, sistemi, impianti, informazioni e dati di natura riservata.<br>Il concetto di sicurezza generalmente è pertinente ad esempio all'accesso fisico a locali protetti, l'utilizzo di porte di accesso blindate congiuntamente all'impiego di sistemi di identificazione personale i quali sono da considerarsi quindi componenti di *sicurezza passiva*. |
| **Sicurezza attiva** ***(sicurezza dati e applicazioni)*** | Applicazione di tutte quelle tecniche e strumenti mediante i quali le informazioni ed i dati di natura riservata sono resi intrinsecamente sicuri, proteggendo gli stessi sia dalla possibilità che un utente non autorizzato possa accedervi *(confidenzialità)*, sia dalla possibilità che un utente non autorizzato possa modificarli *(integrità)*. In tale categoria rientrano sia strumenti hardware che software. |

È evidente che la sicurezza passiva e quella attiva sono tra loro complementari ed entrambe indispensabili per raggiungere il desiderato livello di sicurezza dell'infrastruttura.

Più nel dettaglio, i criteri di sicurezza applicati si riferiscono ai seguenti ambiti e relative caratteristiche:

| Ambito | Caratteristiche |
|---|---|
| **Data Center (DC)** | ▪ L'infrastruttura tecnologica costituente il sistema in argomento è ospitata presso Data Center certificati ISO 27001 per soluzioni *Cloud computing*.<br>▪ La struttura è dotata di doppio accesso in fibra ottica ed impianti di condizionamento e di protezione elettrica ridondati, così da garantire la continuità di servizio anche in caso di guasti o di eventi calamitosi.<br>▪ Sono altresì presenti sistemi antincendio, mentre la pavimentazione sopraelevata e speciali sensori garantiscono un elevato grado di sicurezza del Data Center anche in caso di allagamenti. |
| **Report di controllo prodotto in ambito outsourcing** | Livello di sicurezza con attestazioni SOC 1 tipo II (SSAE 16 e ISAE 3402) e SOC 2 tipo II [1] |
| **Ulteriori caratteristiche di sicurezza in ambito delle soluzioni Cloud** | ▪ I dati critici risiedono su servers all'interno di una DMZ (Demilitarized Zone) predisposta su rete privata protetta da firewall fisico.<br>▪ Nel DC sono presenti sistemi di allarme anti-intrusione e di monitoraggio basati su dispositivi televisivi a circuito chiuso presidiati 24/7 da personale tecnico altamente qualificato.<br>▪ Implementazione Business Continuity Planning con bassi valori di RPO e di RTO garantito da procedure automatiche di ripristino perfettamente funzionanti. |
| **Sicurezza della trasmissione dati** | ▪ Trasmissione dati sicura mediante l'utilizzo del protocollo SSL V3.<br>▪ La comunicazione con l'esterno in ingresso avviene mediante un server dedicato di Virtual Host che ridirige il traffico al server di competenza su un IP Address e porta privata. |

## Sicurezza logica

La sicurezza logica consiste principalmente in misure tecniche. Alcune misure di sicurezza logica comuni si applicano all'infrastruttura di rete, ai server e alle workstation del personale. Queste misure includono i controlli di accesso (ulteriori dettagli nelle sezioni di seguito) e le misure tecniche per affrontare la propagazione o l'esecuzione di codice non approvato (ad es. Virus e altro malware). Gli aggiornamenti vengono eseguiti automaticamente laddove possibile (ad esempio gli aggiornamenti dell'antivirus della workstation) o periodicamente su una pianificazione prestabilita e prioritaria. Esempi di sicurezza logica includono:

- ✓ Scansioni periodiche di vulnerabilità e test di penetrazione.

[1] Lo "Statement on Standards for Attestation Engagements" no. 16 (SSAE 16), è l'ultima generazione di standard AICPA (American Institute of Certified Public Accountants) per il reporting sui controlli alle organizzazioni che forniscono servizi in outsourcing. Lo "SSAE 16" richiede all'Auditor indipendente (Membro qualificato AICPA) di produrre un'affermazione scritta (Management Assertion Letter) sulla gestione per quanto concerne l'efficacia dell'implementazione e del funzionamento dei controlli in corso di auditing. SSAE 16 fornisce inoltre il migliore allineamento con lo standard internazionale ISAE 3402.

- ✓ La gestione delle patch deve essere eseguita in modo tempestivo, in base a uno schema di classificazione dei sistemi e al livello di gravità della patch, e talvolta anche in base al tipo o alla versione del sistema operativo.
- ✓ Controlli tecnici per prevenire attacchi Denial Of Service (principalmente applicabili all'infrastruttura di rete e ai server).
- ✓ Applicazione di specifiche misure di sicurezza per l'accesso remoto ai sistemi di DIGITALSUITE dall'esterno del firewall logico, incluso l'utilizzo di client VPN obbligatorio. Tutti questi accessi sono crittografati. (misure applicate a workstation e dispositivi mobili);
- ✓ Utilizzo di indirizzi IP statici (in genere non sono consentiti DHCP / DDNS, ad eccezione di alcuni casi approvati e documentati per i server e generalmente per le workstation). Tutti gli indirizzi IP statici sono registrati in un database sicuro.

## Infrastruttura

DIGITALSUITE si appoggia a data center distribuiti geograficamente e memorizza tutti i dati di produzione in data center fisicamente sicuri.

## Ridondanza

I sistemi di infrastruttura sono progettati per eliminare singoli punti di guasto e minimizzare l'impatto dei rischi ambientali previsti. Doppi circuiti, interruttori, reti o altri dispositivi necessari aiutano a fornire questa ridondanza. I Servizi sono progettati per consentire a DIGITALSUITE di eseguire determinati tipi di manutenzione preventiva e correttiva senza interruzioni. Tutte le attrezzature e le attrezzature ambientali hanno documentato procedure di manutenzione preventiva che dettagliano il processo e la frequenza delle prestazioni in conformità con le specifiche del produttore o interne.

## Energia

I sistemi di alimentazione elettrica del data center sono progettati per essere ridondanti e manutenibili senza impatto sulle operazioni continue, 24 ore al giorno e 7 giorni alla settimana. Nella maggior parte dei casi, viene fornita una fonte di alimentazione primaria e una alternativa, ciascuna con pari capacità, per i componenti di infrastruttura critici nel data center. L'alimentazione di backup è fornita da vari meccanismi, come le batterie di continuità (UPS), che forniscono una protezione di alimentazione costantemente affidabile durante i periodi di inattività, blackout, sovratensione, sottotensione e condizioni di frequenza fuori tolleranza. Se l'alimentazione di rete viene interrotta, L'alimentazione di backup è progettata per fornire energia transitoria al data center, a piena capacità, per un massimo di 10 minuti fino a quando i sistemi di generatori diesel prendono il sopravvento. I generatori diesel sono in grado di avviarsi automaticamente in pochi secondi per fornire sufficiente energia elettrica di emergenza per far funzionare il data center a piena capacità in genere per un periodo di giorni.

## Sistemi operativi server

I server di DIGITALSUITE utilizzano un'implementazione basata su Linux e Microsoft Windows Server idonei all'ambiente applicativo. I dati vengono archiviati utilizzando soluzioni tecniche atte ad aumentare la sicurezza e la ridondanza dei dati. DIGITALSUITE impiega un processo di revisione del codice per aumentare la sicurezza del codice utilizzato per fornire i Servizi e migliorare i prodotti di sicurezza negli ambienti di produzione.

## Business Continuity

DIGITALSUITE replica i dati su più sistemi per aiutare a proteggere da distruzione o perdita accidentale. DIGITALSUITE ha progettato e pianifica e collauda regolarmente i programmi di pianificazione della continuità operativa / di Disaster Recovery.

## Trasmissione dati

I data center sono in genere collegati tramite collegamenti privati ad alta velocità per garantire un trasferimento sicuro e rapido dei dati tra i data center. Questo è progettato per impedire la lettura, la copia, la modifica o la rimozione dei dati senza autorizzazione durante il trasferimento o il trasporto elettronico o durante la registrazione su supporti di memorizzazione dei dati. DIGITALSUITE trasferisce i dati tramite i protocolli standard di Internet.

## External attack surface

DIGITALSUITE impiega più livelli di dispositivi di rete e rilevamento delle intrusioni per proteggere la propria infrastruttura tecnologica da attacchi esterni. DIGITALSUITE prende in considerazione i potenziali vettori di attacco e incorpora apposite tecnologie in tale ambito.

## Rilevamento delle intrusioni

Il rilevamento delle intrusioni ha lo scopo di fornire informazioni sulle attività di attacco in corso e fornire informazioni adeguate a rispondere agli incidenti. Il rilevamento delle intrusioni di DIGITALSUITE implica:

- ✓ Adozione di misure preventive in ambito delle tipologie di attacco;
- ✓ Impiego di speciali controlli di rilevamento nei punti di ingresso dati; e
- ✓ Utilizzo di tecnologie che rimuovono automaticamente determinate situazioni pericolose.

## Risposta agli incidenti

DIGITALSUITE monitora una varietà di canali di comunicazione in ambito degli incidenti di sicurezza e il personale di sicurezza di DIGITALSUITE reagisce prontamente nel caso di incidenti noti.

## Tecnologie di crittografia

DIGITALSUITE applica la crittografia HTTPS (indicata anche come connessione SSL o TLS).

---

# Metodologie applicate

## Privacy by design e by default

**La disciplina introdotta dal GDPR in materia di protezione dei dati personali si caratterizza per l'attenzione che viene posta sulla responsabilizzazione ("accountability") dei Titolari e dei Responsabili del trattamento dei dati personali.**

In particolare, il quadro normativo delineato dal legislatore europeo delinea un sistema "risk-based" nel quale la valutazione dei rischi per i diritti e per le libertà degli interessati, derivanti dalle specifiche attività di trattamento di dati personali, e tutte le misure concrete che andranno poste in essere sulla base di tale valutazione sono rimesse direttamente in capo a ciascun titolare.

Con l'espressione **"privacy by design"**, il Regolamento Europeo richiamare l'attenzione dei titolari sull'esigenza che la protezione dei dati personali venga garantita "fin dalla progettazione".

## Le Misure Tecniche e Organizzative

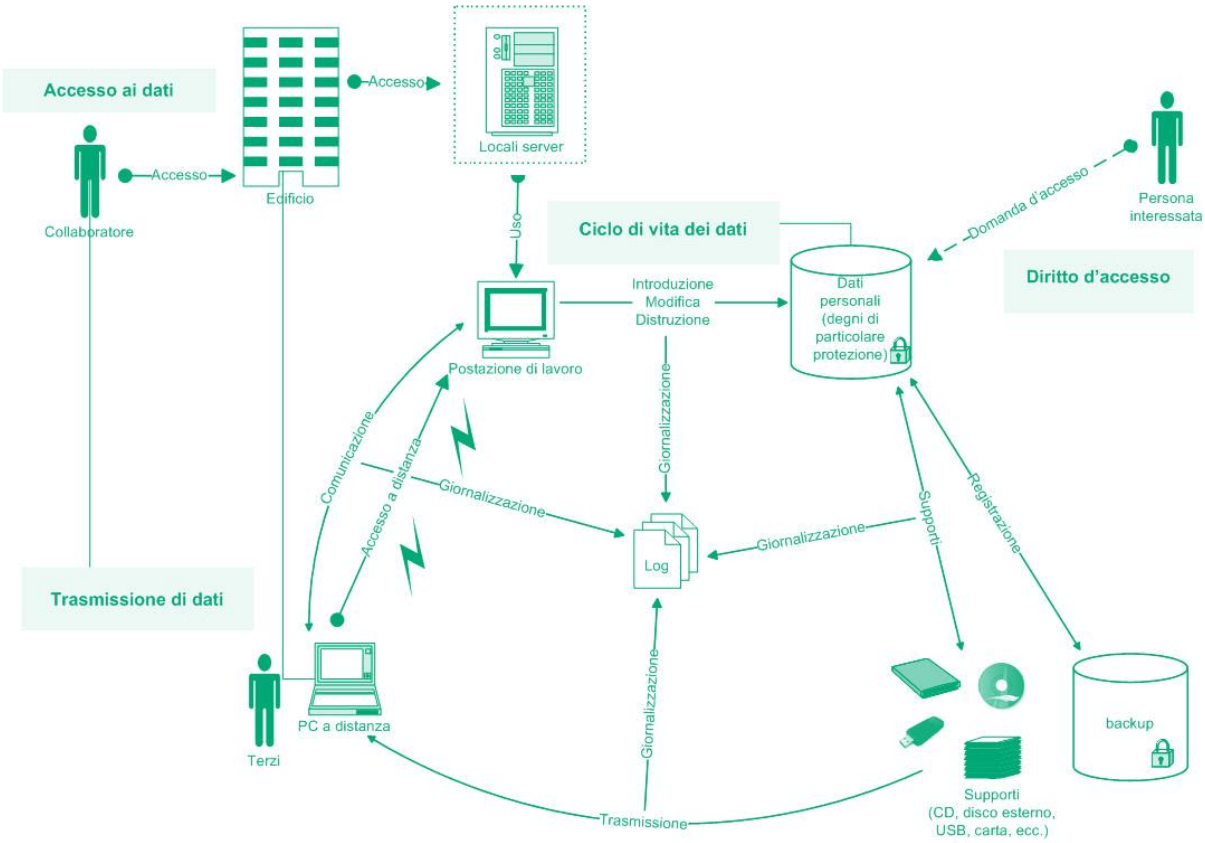
L'adozione di provvedimenti tecnici e organizzativi consente di minimizzare i rischi connessi a un sistema d'informazione. Un sistema d'informazione che contiene dati personali deve cioè essere conforme a determinati criteri al fine di garantire la sicurezza dei dati. L'attuazione di questi provvedimenti consente di offrire una garanzia di sicurezza.

- ✓ I provvedimenti tecnici sono legati direttamente al sistema d'informazione e interessano soltanto quest'ultimo.
- ✓ I provvedimenti organizzativi hanno invece a che fare solo indirettamente con il sistema d'informazione, interessando per esempio le persone che lo utilizzano.

Entrambe le categorie di provvedimenti sono indispensabili. Soltanto la loro adozione combinata consente di evitare la distruzione o la perdita di dati, gli errori, le falsificazioni, l'accesso non autorizzato, ecc. Questi provvedimenti si iscrivono nel ciclo di vita di un sistema d'informazione e sono applicati a tutti i livelli del sistema.

## Ciclo di vita di un sistema d'informazione

Nel seguente schema è raffigurato il ciclo di vita di un sistema d'informazione; esso illustra varie operazioni (l'immissione dei dati, il loro trattamento, la loro comunicazione e registrazione, ecc.) nonché i livelli a cui possono intervenire terze persone (collaboratori, persone adibite al trattamento o persone i cui dati sono contenuti nel sistema).

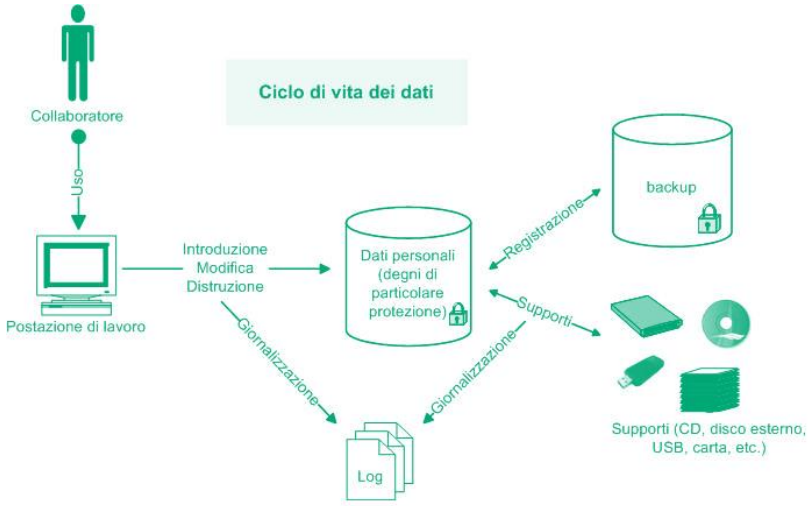


## Ciclo di vita dei dati

I provvedimenti riportati nella sezione precedente garantiscono l'accesso sicuro ai dati, consentendo di proteggere l'infrastruttura informatica sia contro le intrusioni fisiche sia contro i trattamenti illeciti. La fase successiva consiste nel garantire la sicurezza dei dati durante il loro ciclo di vita. I dati devono cioè rimanere integri e affidabili dal momento in cui sono immessi nel sistema fino a quando vengono distrutti e, ovviamente, in tutte le fasi di elaborazione intermedie (incluse la loro anonimizzazione e archiviazione).

In generale, i trattamenti di dati sono effettuati mediante procedure applicative e/o da collaboratori autorizzati all'interno dell'organizzazione, ma possono anche essere subappaltati a terzi.

Di seguito uno schema riassuntivo:




## Sviluppo sicuro del software

Vengono applicati i seguenti criteri generali in ambito dello sviluppo di software sicuro (Protezione in base alle caratteristiche progettuali, Protezione per impostazione predefinita, Protezione nella distribuzione + Comunicazioni). Di seguito una sintesi di tali criteri:

- ✓ *Protezione in base alle caratteristiche progettuali:* il software viene architettato, progettato e implementato per proteggere sé stesso e le informazioni che elabora e per resistere agli attacchi.
- ✓ *Protezione per impostazione predefinita:* ad esempio il software viene eseguito con il minor numero possibile di privilegi, e i servizi e le caratteristiche che non sono necessari su larga scala vengono disattivati per impostazione predefinita o resi accessibili solo a un piccolo gruppo di utenti.
- ✓ *Protezione nella distribuzione:* il software viene corredato di strumenti e istruzioni per consentire agli utenti e/o agli amministratori di utilizzarlo in modo sicuro. Inoltre, gli aggiornamenti sono di facile distribuzione.
- ✓ *Comunicazioni:* gli sviluppatori del software sono adeguatamente formati per scoprire vulnerabilità del prodotto e nel caso sono adottate idonee procedure di comunicazione tempestiva agli utenti finali supportandoli nell'adozione di misure protettive (quali applicazione di patch o distribuzione di soluzioni alternative).

### Progettazione

Nella fase di progettazione vengono individuati i requisiti e la struttura complessiva del software. Dal punto di vista della protezione, i fattori chiave della fase di progettazione sono:

- ✓ *Definizione dell'architettura di protezione e delle linee guida di progettazione*: definizione della struttura complessiva del software dal punto di vista della protezione e identificazione di quei componenti il cui funzionamento corretto è essenziale per la protezione (la cosiddetta "base informatica attendibile"). Identificazione delle tecniche di progettazione applicabili al software nel suo complesso, quali layering, utilizzo di linguaggio tipizzato in modo sicuro, applicazione di meno privilegi e riduzione al minimo della superficie d'attacco. (Layering fa riferimento all'organizzazione del software in componenti ben definiti e strutturati in modo da evitare dipendenze circolari tra di essi: i componenti sono organizzati in livelli e un livello superiore può dipendere dai servizi dei livelli inferiori, mentre ai livelli inferiori è vietato dipendere dai livelli superiori.) Le specifiche dei singoli elementi dell'architettura verranno descritte dettagliatamente nelle specifiche del progetto, ma l'architettura di protezione fa riferimento a una prospettiva globale del progetto di protezione.

- ✓ *Documentazione degli elementi della superficie d'attacco del software*. Dato che il software non raggiungerà un grado di protezione perfetto, è importante che solo le funzionalità che verranno utilizzate da gran parte degli utenti siano disponibili per tutti gli utenti per impostazione predefinita, e che le funzionalità siano installate con il livello minimo possibile di privilegi. La misurazione degli elementi della superficie d'attacco fornisce al team del prodotto un criterio di valutazione continuo della protezione predefinita e consente di rilevare le istanze in cui il software è più esposto agli attacchi. Sebbene alcune istanze di aumento della superficie d'attacco possano essere giustificate dalle funzioni e dall'utilizzabilità migliorate del prodotto, è importante rilevare e mettere in discussione ciascuna di queste istanze durante la progettazione e l'implementazione, in modo che il software venga fornito in una configurazione predefinita che sia la più sicura possibile.

- ✓ *Esecuzione della modellazione dei pericoli*. Il team del prodotto esegue la modellazione dei pericoli a livello dei singoli componenti. Utilizzando una metodologia strutturata, il team dei componenti identifica le risorse che il software deve gestire e le interfacce dalle quali è possibile accedere a tali risorse. Il processo di modellazione dei pericoli identifica i pericoli che possono danneggiare ogni risorsa e la probabilità che il danno si verifichi (valutazione dei rischi). Il team dei componenti identifica quindi le contromisure atte a ridurre i rischi (o sotto forma di funzionalità di protezione come la crittografia o sotto forma di funzionamento corretto del software che protegge le risorse da eventuali danni). La modellazione dei pericoli consente pertanto al team del prodotto di identificare i requisiti delle funzionalità di protezione nonché le aree in cui occorre eseguire in modo particolarmente accurato le revisioni del codice e i test di protezione.

## Implementazione

Durante la fase di implementazione, il team del prodotto codifica, esegue test e integra il software. Le operazioni effettuate per eliminare i difetti di protezione o prevenire il loro inserimento iniziale durante questa fase sono ampiamente utilizzate perché riducono in modo significativo le probabilità che eventuali vulnerabilità della protezione si verifichino nella versione definitiva del software che verrà fornito ai clienti.

I risultati della modellazione dei pericoli forniscono indicazioni particolarmente importanti durante la fase di implementazione. Gli sviluppatori prestano particolare attenzione alla correttezza del codice volto a ridurre i rischi ad alta priorità e i tester si concentrano sui test per assicurarsi che tali rischi vengano di fatto bloccati o ridotti.

Le attività applicabili alla fase di implementazione sono:

- ✓ *Applicazione degli standard di codifica e test.* Grazie agli standard di codifica, gli sviluppatori evitano di introdurre difetti che possono provocare vulnerabilità della protezione. Ad esempio, l'utilizzo di una gestione delle stringhe più sicura e coerente e dei costrutti di manipolazione dei buffer consente di ridurre l'introduzione delle vulnerabilità associate al sovraccarico dei buffer. Gli standard dei test e le procedure consigliate garantiscono che i test si incentrino sul rilevamento delle possibili vulnerabilità della protezione e non solo sul funzionamento corretto delle funzioni e caratteristiche del software.

- ✓ *Applicazione degli strumenti per i test della protezione*, compresi gli strumenti di fuzzing. La tecnica del "fuzzing" fornisce input strutturati ma non validi alle API (Application Programming Interface) e

alle interfacce di rete in modo da aumentare al massimo la probabilità di rilevare errori che potrebbero causare vulnerabilità nel software.

- ✓ *Applicazione degli strumenti per l'analisi statica del codice*. Gli strumenti possono rilevare alcuni tipi di errori nel codice che danno origine a vulnerabilità, compresi sovraccarichi dei buffer, sovraccarichi dei numeri interi e variabili non inizializzate.
- ✓ *Esecuzione di revisioni del codice*. Le revisioni del codice completano i test e gli strumenti automatizzati poiché consentono di applicare gli sforzi di sviluppatori qualificati all'esame del codice sorgente per rilevare ed eliminare possibili vulnerabilità della protezione. Sono fondamentali nel processo di eliminazione delle vulnerabilità della protezione dal software durante il suo sviluppo.

---

# Misure organizzative e di sicurezza interna di DIGITALSUITE

Descrizione delle misure tecniche, organizzative e di sicurezza in materia di Data Privacy applicate nell'ambito delle infrastrutture interne di DIGITALSUITE di tipo fisico e tecnologico, oltre che al proprio personale coinvolto.

## Sicurezza ambientale

L'accesso ai computer, che fungono quindi da interfaccia verso i dati, viene controllato. Soltanto le persone autorizzate accedono agli edifici e agli uffici. Poiché queste persone possono svolgere funzioni diverse, per poter definire diritti d'accesso specifici, si tiene conto di tutte le possibili funzioni (collaboratore dell'organizzazione, personale addetto alla manutenzione, ecc.).

Inoltre, i server ed i sistemi afferenti all'erogazione dei Servizi sono fisicamente ospitati presso Data Center in cui sono applicate idonee misure di Sicurezza passiva (sicurezza fisica) e Sicurezza attiva (sicurezza dati e applicazioni) descritte in seguito nel presente documento.

Principali misure adottate:

- ✓ L'accesso agli edifici è soggetto a determinati controlli: le persone che desiderano entrare devono possedere un apposito badge associato a un codice d'accesso, per poter essere identificate.
- ✓ I visitatori sono soggetti a misure di controllo specifiche e sono accolti secondo una procedura prestabilita, volta ad evitare che possano aggirarsi indisturbati all'interno dell'edificio.
- ✓ Al di fuori degli orari di presenza, gli uffici sono chiusi a chiave.
- ✓ Nei locali strategicamente più importanti sono installati degli allarmi, attivati al di fuori degli orari di presenza.
- ✓ Su tutti i computer è stato installato e attivato un programma antivirus, aggiornato a intervalli regolari.

## Sicurezza dell'accesso ai dati

I dati sono conservati nei server centrali. In linea generale, i collaboratori non hanno bisogno di accedere a tutti i dati. L'accesso dei collaboratori è pertanto limitato ai soli dati necessari al loro lavoro così da ridurre i rischi di un uso scorretto, sia questo intenzionale o meno. Allo scopo di prevenire eventuali abusi vengono definite regole di accesso nonché meccanismi d'autorizzazione in base alle funzioni svolte dai singoli collaboratori.

Principali misure adottate:

- ✓ Il sistema d'informazione è organizzato in modo tale da accordare agli utenti accessi differenziati.
- ✓ Il diritto d'accesso dei singoli collaboratori è definito internamente all'organizzazione secondo una matrice dei diritti di accesso.
- ✓ Il collaboratore procede alla propria autenticazione ogni volta che avvia il sistema. Il livello di autenticazione è direttamente proporzionale al grado di protezione dei dati.

### Accessi remoti

Gli accessi remoti possono essere di diversi tipi e per ogni situazione distinta si prevedono determinate misure di protezione.

I collaboratori che anche occasionalmente lavorano esternamente all'organizzazione devono richiedere appositamente l'autorizzazione all'accesso remoto ai sistemi informativi. Tale accesso viene disciplinato secondo le apposite policy aziendali e in considerazione della tipologia dei dati cui accedere.

Principali misure adottate:

- ✓ Le persone che desiderano o devono connettersi a distanza si avvalgono di un accesso sicuro.
- ✓ Server centrali e computer personali sono protetti da firewall.
- ✓ Gli accessi vengono registrati su appositi file di log.

## Procedure interne volte alla gestione dei codici di identificazione

Si applicano le seguenti misure tecniche e organizzative in ambito:

- ✓ Il trattamento dei dati personali, con strumenti elettronici, è consentito esclusivamente agli Incaricati dotati di credenziali di autenticazione. Le credenziali di autenticazione sono individuali ed identificano univocamente l'Incaricato sui sistemi di elaborazione cui ha accesso.
- ✓ Ad ogni Incaricato è associato un profilo che gli consente l'accesso ad uno o più specifici trattamenti in base alle funzioni cui egli è preposto.
- ✓ È compito degli Amministratori di Sistema approntare gli strumenti ed i controlli mediante cui verificare il corretto uso delle credenziali di autenticazione, nonché monitorare e vigilare sui tentativi di accesso non autorizzato.
- ✓ In caso di perdita della qualità che consente all'Incaricato l'accesso ai dati personali, si procede alla verifica del profilo (cessazione attività o cambio di ruolo).
- ✓ Le credenziali di autenticazione non utilizzate da almeno 6 mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
- ✓ Esiste una procedura di disattivazione delle credenziali in caso di dimissioni di un Incaricato al trattamento dei dati personali.

## Gestione, custodia e aggiornamento della parola chiave (Password)

Tutte le stazioni di lavoro sono protette da una username e password, così come per l'accesso ai server, che rispetta i requisiti minimi di complessità (8 caratteri alfanumerici con lettere maiuscole e minuscole) e che viene regolarmente cambiata ogni 6 mesi.

La password di accesso presenta le seguenti caratteristiche:

- ✓ Non corrisponde al nome utente o ai dati personali dell'utente;
- ✓ Ha una lunghezza di almeno otto caratteri alfa-numerici;

Modalità di attivazione, variazione e gestione delle password:

- ✓ l'attivazione della password è eseguita dagli incaricati all'amministrazione del sistema e l'utente è obbligato a modificarla al primo utilizzo;
- ✓ è sempre possibile la modifica in via autonoma della password da parte dell'utente;
- ✓ è possibile il reset della parola chiave da parte degli incaricati all'amministrazione del sistema portando a conoscenza dell'utente di tale operazione.
- ✓ Il processo di autenticazione consente di ottenere agli Incaricati uno specifico insieme di privilegi di accesso ed utilizzo rispetto alle risorse del sistema informatico.

## Policy e istruzioni

Gli Incaricati al trattamento dei dati, osservano le seguenti istruzioni per l'utilizzo degli strumenti informatici descritte più dettagliatamente in appositi documenti di policy opportunamente consegnati:

- ✓ obbligo di custodire i dispositivi di accesso agli strumenti informatici (username e password);
- ✓ obbligo di non lasciare incustodito e accessibile lo strumento elettronico assegnato durante una sessione di trattamento;
- ✓ obbligo assoluto di riservatezza;
- ✓ divieto di divulgazione della password di accesso al sistema (non solo a soggetti esterni, ma neppure a persone appartenenti all'organizzazione, siano essi colleghi, responsabili del trattamento, amministratori di sistema, etc.).

Ad ogni Incaricato è imposto l'aggiornamento periodico della password con sistema automatico.

## Sistema di assegnazione e controllo dei profili

Ogni Incaricato ha un proprio profilo di autorizzazione e può accedere ai soli dati a lui consentiti o per semplicità di gestione amministrativa, può accedere ai soli dati consentiti alla classe omogenea di incarico alla quale appartiene. Tali profili autorizzativi sono configurati sugli appositi strumenti di sicurezza e di controllo delle autorizzazioni, delle piattaforme elaborative elettroniche.

I profili di autorizzazione, per ciascun Incaricato o per classi omogenee di Incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento. Il processo di assegnazione del profilo di autorizzazione avviene con le seguenti modalità:

- ✓ consegna dell'informativa e delle policy sull'uso appropriato delle credenziali utente;
- ✓ creazione del profilo di autorizzazione sui sistemi;
- ✓ consegna delle credenziali e password.

In base alle relative policy, gli Incaricati debbono adottare le necessarie cautele per assicurare la segretezza della parola chiave e custodire diligentemente ogni altro dispositivo che gli è stato affidato per i sistemi di autenticazione informatica.