Manuale per la sicurezza delle informazioni e della privacy Norme ISO/IEC 27001

GHS Media S.r.l.
Via Donato Menichella, 268/D
Cap. 00156 - ROMA (RM)
P.IVA 09745721002

Rev.00 del 04/02/2020

Sommario

Manuale per la sicurezza delle informazioni e della privacy
Norme ISO/IEC 27001

1. Introduzione

La tutela dei dati personali è regolamentata in Italia dal Decreto Legislativo 196 del 2003 “Codice in materia di protezione dei dati personali” (indicato anche come “Codice privacy”), e successivamente sostituito dal Regolamento Europeo 679/16, e dalla normativa secondaria ad esso collegata ed emessa dal Garante per la protezione dei dati personali (indicato anche come Garante privacy). Il Codice privacy italiano costituisce il recepimento della Direttiva Europea 95/46/CE.

Le norme più importanti in quest’area e a cui questo Quaderno fa riferimento sono le seguenti:

- D.lgs. 196/03 (Codice in materia di protezione dei dati personali) e successivo Regolamento Europeo 679/16
- Allegato B del D.lgs. 196/03;
- Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema – Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 (con modifiche introdotte dai Provvedimenti del 12 febbraio 2009 e 25 giugno 2009).

Nell’ultima parte del 2011 e nei primi mesi del 2012, la normativa italiana è stata investita da modifiche che hanno cambiato e cambieranno, almeno in parte, le modalità di trattamento dei dati personali e la valutazione della loro liceità. Si prevede che ulteriori modifiche saranno apportate nel corso del 2012 e 2013. Non ci soffermiamo sulle motivazioni che hanno indotto il legislatore ad introdurre queste modifiche; possiamo però affermare che sono orientate alla semplificazione, a una maggiore armonizzazione a livello UE e all’adeguamento allo sviluppo tecnologico.

Le principali modifiche introdotte sono:

- nuova definizione di dato personale, ora applicabile alle sole persone fisiche;
- eliminazione dell'obbligo di redigere e aggiornare periodicamente il Documento Programmatico per la Sicurezza (DPS).

Per quanto riguarda gli scenari futuri, la Commissione europea ha presentato la proposta di un *Regolamento generale sulla protezione dei dati*, che andrà a sostituire, oltre alla direttiva 95/46/CE, lo stesso Codice privacy; introducendo identiche regole nei Paesi che compongono la UE. Infatti, i Regolamenti UE, a differenza delle direttive, sono immediatamente esecutivi e non necessitano di recepimento da parte degli Stati membri.

Il nuovo Regolamento, al momento solo in bozza, non è previsto che apporterà riduzioni o stravolgimenti dei requisiti rispetto all'attuale Codice privacy, ma semplificazioni nell'applicazione e miglioramenti degli effetti generali.

La normativa privacy si occupa, come è noto, di sicurezza delle informazioni, anche se limitatamente a quelle di carattere personale. E' quindi naturale volerla associare allo standard internazionale ISO/IEC 27001, che definisce i requisiti di un Sistema di gestione per la sicurezza delle informazioni (SGSI). Questo standard è applicabile in modo generale ad aziende di qualsiasi dimensione e riguarda la sicurezza di qualunque tipo di dato e informazione.

Questo Manuale ha l'obiettivo di facilitare la realizzazione di un Sistema di gestione per la sicurezza delle informazioni (SGSI) che integri al suo interno le misure di sicurezza, incluse le procedure documentate o non documentate, previste dalla normativa italiana sulla tutela dei dati personali e costituisca un quadro di riferimento per mantenerle e migliorarle nel tempo.

Il sistema organizzativo e gestionale per la sicurezza delle informazioni della GHS Media S.r.l. è mirato a garantire lo svolgimento delle attività aziendali nel rispetto della normativa vigente.

Nell'ottica della pianificazione e gestione delle attività aziendali tese all'efficienza, alla correttezza, alla trasparenza ed alla qualità, l'Impresa ha adottato ed attua le misure organizzative, di gestione e di controllo descritte nel presente documento, di seguito indicato come Modello.

Un secondo obiettivo, non meno importante, è quello di mostrare come la costruzione di un SGSI, anche in contesti aziendali di ridotte dimensioni (piccole e medie imprese, PMI), preponderanti nel tessuto economico del nostro Paese, sia un obiettivo raggiungibile con uno sforzo modesto. Tale sforzo, se correttamente indirizzato, può trasformare da costo a valore l'impegno per l'adeguamento al Codice privacy e la realizzazione e manutenzione delle misure di sicurezza delle informazioni.

La realizzazione di un SGSI e la sua integrazione con quanto descritto nel presente Quaderno non assicura la completa conformità al Codice privacy né ai diversi Provvedimenti emanati dal Garante; può tuttavia costituire un valido modo per dimostrare di aver affrontato in modo coerente e sistematico l'individuazione e la gestione delle misure di sicurezza minime e idonee (di cui agli artt. 31-36 del Codice).

E' importante ricordare che *la protezione dei dati personali*, come regolata dalle disposizioni contenute nel D.lgs. 196/03, e successivamente sostituito dal Regolamento Europeo 679/16, *non attiene solamente alla gestione della sicurezza dei dati personali* per garantirne riservatezza, integrità e disponibilità, ma anche alla definizione di specifiche modalità di trattamento che ne determinano la liceità. In questo Manuale sono presi in considerazione ed approfonditi gli aspetti che riguardano la sicurezza dei dati personali e aziendali ricevuti e autorizzati.

In questo documento è utilizzato il termine "azienda" al posto di altri termini più generali perché ritenuto di più facile comprensibilità.

Il Modello è sottoposto a verifica periodica e viene modificato nel caso in cui siano scoperte significative violazioni delle prescrizioni o si verifichino mutamenti dell'organizzazione o delle attività dell'Impresa, ovvero delle norme di riferimento. Le responsabilità e le modalità di aggiornamento del Modello sono disciplinate dal presente documento.

E' fatto obbligo a chiunque operi nell'Impresa o collabori con essa di attenersi alle pertinenti prescrizioni del Modello ed in specie di osservare gli obblighi informativi dettati per consentire il controllo della conformità dell'operato alle prescrizioni stesse.

L'originale del Modello, dei documenti ad esso allegati e dei suoi aggiornamenti è depositato presso la sede dell'Impresa in Via Donato Menichella, 268/D a Roma (RM) ed è a disposizione di chiunque abbia titolo a consultarla. Copia conforme a quella approvata dal Consiglio di

Amministrazione è inoltre pubblicata nel sito web aziendale https://www.ghsmedia.it, con eccezione dei protocolli e del regolamento disciplinare che sono distribuiti in modo controllato a tutti gli enti preposti alla loro conoscenza.

L'Impresa provvede a notificare a ciascun soggetto tenuto a rispettare il Modello le pertinenti prescrizioni riferite alla specifica attività o funzione e ad erogare formazione alle funzioni interessate affinché i precetti siano noti e perseguiti in modo efficace.

Il presente documento è il Manuale della Conservazione della GHS Media Srl redatto ai sensi dell' 'art. 8 DPCM del 3 dicembre 2013.

Il manuale ha lo scopo di specificare le regole e le procedure per la conservazione a norma dei documenti informatici e riporta dettagliatamente le informazioni sull' organizzazione e i soggetti coinvolti nel processo di conservazione. Descrive inoltre il processo di conservazione nelle sue fasi operative e tutte le attività svolte per rispettare gli standard di riferimento, nonché le misure di sicurezza adottate (si veda il documento "Piano per la Sicurezza" e la "Politica di classificazione delle informazioni – ISPD").

Eventuali particolarità legate alle singole forniture del Servizio di Conservazione, condivise con il singolo Cliente, sono descritte nel documento "Specificità del contratto".

Si evidenzia che Il servizio viene erogato nel rispetto dei requisiti di continuità, sicurezza fisica e logica, monitoraggio, che i Data Center garantiscono e descrivono negli specifici documenti di certificazione.

La società ha implementato nel suo Sistema di Gestione della Sicurezza delle Informazioni (SGSI), un impianto di policy che rappresenta il contesto di riferimento costante nella gestione del servizio di conservazione.

Glossario

Termine	Definizione
accesso	operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici
accreditamento	riconoscimento, da parte dell'Agenzia per l'Italia digitale, del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza ad un soggetto pubblico o privato, che svolge attività di conservazione o di certificazione del processo di conservazione
aggregazione documentale informatica	aggregazione di documenti informatici o di fascicoli informatici, riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente
archivio informatico	archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico
autenticità	caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico
ciclo di gestione	arco temporale di esistenza del documento informatico, del fascicolo informatico, dell'aggregazione documentale informatica o dell'archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo
classificazione	attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici metadati
codice eseguibile	insieme di istruzioni o comandi software direttamente elaborabili dai sistemi informatici
conservazione	insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato e descritto nel manuale di conservazione

copia analogica del documento informatico	Documento analogico avente contenuto identico a quello del documento informatico da cui è tratto
copia di sicurezza	copia di backup degli archivi del sistema di conservazione prodotta ai sensi dell'articolo 12 delle presenti regole tecniche per il sistema di conservazione
documento informatico	La rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
documento analogico	La rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti
duplicazione dei documenti informatici	Produzione di duplicati informatici
ente produttore	persona fisica o giuridica che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con responsabile della gestione documentale.
esibizione	operazione che consente di visualizzare un documento conservato e di ottenerne copia
evidenza informatica	una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica
firma elettronica	L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica
firma elettronica avanzata	Insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, create con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se I dati stessi siano stati successivamente modificati
firma digitale	Un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un Sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici

formato	modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file
funzione di hash	una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti
impronta	la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash
interoperabilità	capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi
leggibilità	insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti
marca temporale	È il risultato di una procedura informatica – detta servizio di marcatura temporale – grazie alla quale si attribuisce a un documento informatico un riferimento temporale opponibile a terzi
memorizzazione	processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici
metadati	insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione; tale insieme è descritto nell'allegato 5 del DPCM 3/12/2013
pacchetto di archiviazione	detto anche PdA, pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato 4 del DPCM 3/12/2013 e secondo le modalità riportate nel manuale di conservazione

pacchetto di distribuzione	detto anche PdD, pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta
pacchetto di versamento	Detto anche PdV, pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato e descritto nel manuale di conservazione
pacchetto informativo	contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare
presa in carico	accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione
processo di conservazione	insieme delle attività finalizzate alla conservazione dei documenti informatici di cui all'articolo 10 delle regole tecniche del sistema di conservazione
rapporto di versamento	documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore
responsabile della conservazione	Soggetto responsabile dell'insieme delle attività elencate nell'art. 8, comma 1 delle regole tecniche del sistema di conservazione
responsabile del trattamento dei dati	La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente associazione od organismo preposti dal titolare al trattamento di dati personali
responsabile della sicurezza	Soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza
riferimento temporale	informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento
sistema di conservazione	detto anche SdC, sistema di conservazione dei documenti informatici di cui all'articolo 44 del Codice

Titolare	Il Titolare è soggetto produttore dei documenti informatici da conservare individuato come definito dall'art. 5, co.2, lett. a) del DPCM 3 dicembre in materia di sistemi di conservazione.
utente	Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse

Acronimi

Abbreviazione	Significato
AgID	Agenzia per l'Italia Digitale
AMM	Responsabile Amministrazione, Servizi Generali, Personale
CA	Certification Authority, cioè ente accreditato per l'emissione e la gestione di certificati di firma qualificata
CAD	Codice dell'amministrazione digitale, Decreto.Legislativo 7 marzo 2005, n. 82 e successive modifiche/integrazioni
COMM	Responsabile Commerciale
CRL	certificate revocation list, liste di certificati digitali revocati
CS	Responsabile della funzione Norme e progetti di Conservazione Digitale
CS_OP	Responsabile Operazioni Conservazione
DIR	Direzione
DLgs	Decreto Legislativo
DM	Decreto Ministeriale
DMEF	Decreto Ministero dell'Economia e delle Finanze
DPCM	Decreto Presidente del Consiglio dei Ministri
DPR	Decreto del Presidente della Repubblica
HASH	una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti
IDV	Indice di Versamento
IMPRONTA	a sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash
ISPD	Information. Security Policy Document
P7M	Estensione dei file firmati con standard PKCS#7
PAdES	PDF Advanced Electronic Signature, formato standard di firma su PDF, con informazioni aggiuntive rispetto al formato base (PADES-BES) per includere la marca temporale
PdA	Pacchetto di Archiviazione
PdD	Pacchetto di Distribuzione

PdV	Pacchetto di Versamento
PDF	Portable Document Format
PKCS#7	Standard della sintassi dei messaggi crittografici, usato per firmare o criptare messaggi in una infrastruttura a chiave pubblica (PKI).
PKI	Public Key Infrastructure, cioè l'infrastruttura che crea e gestisce i certificati (qualificati) di firma elettronica basati su crittografia a chiave pubblica
PROG	Responsabile Area Progetti
RDC	Responsabile della conservazione
RSDC	Responsabile del servizio di conservazione
RFAC	Responsabile della funziona archivistica
RP	Responsabile del trattamento dei dati personali
RSIC	Responsabile dei sistemi Informatici per la conservazione
RSSC	Responsabile Sicurezza dei sistemi per la conservazione
SdC	Sistema di Conservazione
SI	Sistemi Informativi
SinCRO	Supporto all'interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI11386:2010) - Standard nazionale in linguaggio XML, riguardante la struttura dell'insieme di dati a supporto del processo di conservazione
SMC	Responsabile dello sviluppo e della manutenzione del SdC
UD	Unità Documentaria
UTC	Universal Time Coordinated (Misura del tempo come stabilito dall'International Radio Consultative Committee –CCIR)
WORM	Write Once Read More

Normativa di riferimento

Di seguito sono elencati, in ordine cronologico, i principali riferimenti normativi a livello nazionale per l'attività di conservazione.

1) **Riferimenti normativi**
    - Codice civile [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;
    - Decreto del Presidente della Repubblica del 26/10/1972 n. 633 e s.m.i. Istituzione e disciplina dell'imposta sul valore aggiunto;
    - Legge 7 agosto 1990 n 241 e s.m.i. nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi
    - Decreto del Presidente della Repubblica del 28/12/2000 n. 445 Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (G.U. n. 42 del 20 febbraio 2001)
    - Decreto legislativo 30 giugno 2003, n. 196 e s.m.i. Codice in materia di protezione dei dati personali e successivamente sostituito dal Regolamento Europeo 679/16,
    - Decreto legislativo 22 gennaio 2004 n. 42 e s.m.i. Codice dei beni culturali e del paesaggio – modificato al 22 luglio 2014.
    - Decreto Legislativo 7 marzo 2005 n.82 Codice dell'amministrazione digitale (G.U. n.112 del 16 maggio 2005)
    - Circolare Agid 10 aprile 2014 n. 65. Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n.82.
    - Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014 - Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41,

e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.

2) Riferimenti tecnici

- **Decreto del Presidente del Consiglio dei Ministri del 13 gennaio 2004** Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione ,la riproduzione e la validazione, anche temporale, dei documenti informatici (G.U. n. 98 del 27 aprile 2004)
- **DPCM 22 febbraio 2013** Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71. (13A04284) (GU n.117 del 21-5-2013)
- **DMEF 3 aprile 2013, n. 55** Regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica da applicarsi alle amministrazioni pubbliche ai sensi dell'articolo 1, commi da 209 a 213, della legge 24 dicembre
- **DPCM 3 dicembre 2013** Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20 commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1 del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005

Eventuali norme specifiche relative alle diverse tipologie di documenti riguardanti il contratto di erogazione del servizio di conservazione sono riportate nell'allegato "Specificità del contratto".

3) Standard di riferimento

Gli standard di riferimento per l'attività di conservazione di IDC corrispondono a quelli elencati nell'allegato 3 del DPCM 03 Dicembre 2013 – Regole Tecniche in materia di Sistema di Conservazione:

- **ISO 14721:2012 OAIS** (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- **ISO/IEC 27001:2013**, Information technology - Security techniques - Information security management systems Requirements, Requisiti di un ISMS (Information Security Management System);
- **ETSI TS 101 533-1 V 1.3.1** (2012-04) Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- **ETSI TR 101 533-2 V 1.3.1 (2012-04**) Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- **UNI 11386:2010 Standard SInCRO** - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- **ISO 15836:2009 Information and documentation** - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.

2. Sistema di gestione della sicurezza - Introduzione

Il modello noto come “Plan-Do-Check-Act” (PDCA) è caratterizzato dalla ripetizione ciclica delle fasi di pianificazione, realizzazione, verifica e adozione di azioni ed è orientato al miglioramento continuo. Esso si colloca alla base di tutti i moderni sistemi di gestione, da quelli per la qualità a quelli per la sicurezza delle informazioni.

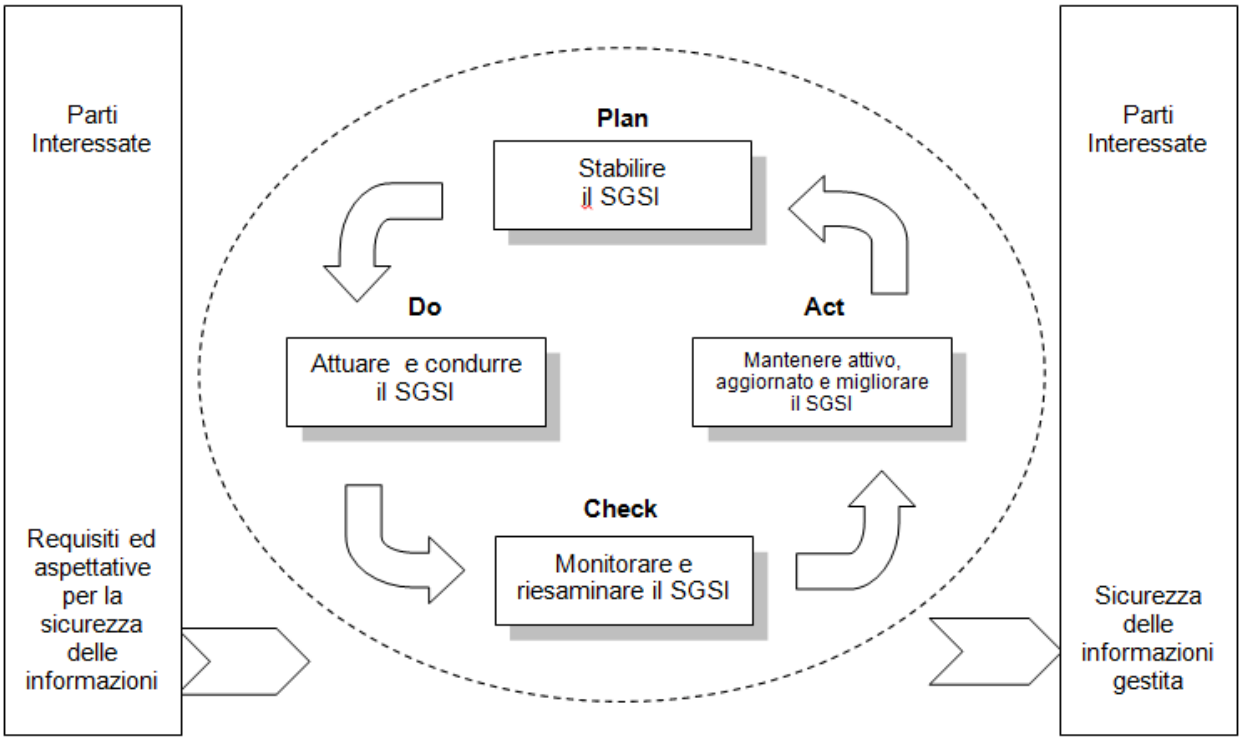


Figura 1 - Modello PDCA

I sistemi di gestione sono finalizzati a stabilire delle politiche e degli obiettivi e a operare per il loro raggiungimento nel tempo, anche attraverso la modifica delle attività aziendali. Un sistema di gestione, perché sia tale, richiede che le attività siano strutturate in una serie di processi opportunamente correlati tra loro, in modo da organizzar e correttamente e coerentemente quanto necessario per raggiungere gli obiettivi stabiliti.

L'applicazione di un sistema di gestione, a maggior ragione in contesti aziendali snelli e flessibili, può e deve essere un fattore abilitante e non un fattore debilitante. Per forza di cose esso richiede degli sforzi e delle attenzioni, ma questi devono essere coerenti ai rischi d'impresa e bilanciare l'efficacia con l'efficienza nella gestione delle informazioni, inclusi i dati personali, in conformità ai requisiti normativi e alle aspettative delle parti interessate.

Un Sistema per la gestione della sicurezza delle informazioni, quindi, può e dovrebbe includere i requisiti per la sicurezza dei dati personali, di cui fanno parte quelli stabiliti per legge. Nel caso di sistemi che intendono essere conformi alla UNI CEI ISO/IEC27001, tale scelta non è opzionale.

3. Elementi fondamentali per la gestione dei dati personali

La gestione dei dati personali, come già detto, è regolata in Italia da un insieme di normative e provvedimenti emessi sia dal Parlamento sia dal Garante per la Privacy. Questi documenti fissano dei requisiti senza però inserirli in un quadro organico, con il rischio concreto che i principi stessi a cui si ispirano vadano disattesi anche in caso di loro completo adempimento.

Per questa ragione sono elencati di seguito alcuni elementi considerati fondamentali per stabilire un quadro organico che garantisca la coerenza dell'approccio seguito con i principi sottostanti la tutela dei dati personali:

- ✓ coordinamento delle diverse aree aziendali in materia di gestione dei dati personali;
- ✓ definizione di regole interne per la gestione dei dati personali, da rispettare nelle procedure, formalizzate o meno, seguite nell'operatività;
- ✓ chiara e precisa definizione dei trattamenti di dati personali, specificandone le finalità, le modalità di trattamento e le categorie di interessati e predisponendo le relative informative e notifiche, se necessario;
- ✓ gestione delle attribuzioni di responsabilità interne ed esterne e delle comunicazioni rese da esse necessarie;
- ✓ controllo e dimostrabilità sia delle azioni sia dell'approccio complessivo mantenuto per la gestione dei dati personali.

Sono di seguito riportate le raccomandazioni, suddivise per fase del ciclo PDCA, da tenere in considerazione per raggiungere e mantenere nel tempo un'adeguata gestione della sicurezza delle informazioni, tra cui i dati personali.

3.1. Plan

3.1.1 Ruoli e responsabilità

Il primo passaggio propedeutico alla creazione di un Sistema per la gestione della sicurezza delle informazioni, compresi i dati personali, una volta definita in modo preliminare la sua estensione rispetto ai processi aziendali, consiste nell'individuare un membro della Direzione con adeguate competenze relative al tema della privacy e della sicurezza delle informazioni, a cui assegnare la responsabilità di coordinamento (d'ora innanzi citato come *Responsabile del sistema* o del SGSI).

Questa figura può essere dedicata completamente o meno a questo compito. Può però capitare che egli oltre l'assegnazione della responsabilità ad una persona interna, che si appoggia, anche con continuità, ad un esperto esterno.

Qualunque sia la scelta adottata, non dovrà mancare al Responsabile il pieno sostegno della Direzione e la necessaria autorità per garantire una corretta ed efficace gestione del sistema. Il primo passo è la formalizzazione della sua nomina.

Va sottolineato che non dovrà mai mancare da parte della Direzione, che ha comunque la titolarità dei trattamenti, un adeguato e visibile supporto anche economico alle azioni proposte dal Responsabile del sistema, un continuo monitoraggio del suo operato e una costante condivisione degli obiettivi e delle finalità del SGSI.

E ' d'uso associare alla nomina di Responsabile del sistema la nomina a Responsabile del trattamento. Poiché al Responsabile del sistema potrebbe non essere assegnato alcun particolare trattamento, tale scelta può essere intesa come non prevista dal Codice. Cionondimeno, il comma 2 dell'articolo 29, in virtù dell'elevato livello di responsabilità assegnato al soggetto, rende giustificata la prima interpretazione. Si ricorda inoltre che la nomina del Responsabile del sistema, anche ai sensi del comma 3 dell'articolo 29 del Codice, non impedisce la nomina di altri Responsabili del trattamento, mediante opportuna suddivisione dei compiti.

Ulteriori responsabilità, ricoperte dal Responsabile di sistema in contesti aziendali di ridotte dimensioni o da personale a suo supporto, possono essere introdotte in base alla dimensione e alla complessità dei trattamenti effettuati e comprendono:

- verifica periodica (audit interno) dello stato di conformità del SGSI;
- gestione della documentazione del SGSI e del suo aggiornamento;
- supporto all'applicazione delle procedure del SGSI
- erogazione di interventi di formazione e consapevolezza;
- gestione delle comunicazioni in materia di privacy con gli interessati;
- risposta alle richieste di informazione, cancellazione o modifica di dati personali da parte degli interessati (esterni e interni all'azienda);
- sorveglianza dei nuovi obblighi normativi e delle sentenze in materia.

Gli altri ruoli aziendali normalmente coinvolti nella sicurezza delle informazioni sono il responsabile del Sistema informativo, il responsabile dell'Ufficio personale, e nel caso ci siano trattamenti di dati personali che presentano rischi specifici o per i quali è richiesta la notifica, i responsabili delle aree aziendali coinvolte da tali trattamenti (eventualmente anche loro nominati Responsabili di tali trattamenti, ai sensi dell'art. 29 del Codice).

E' importante sottolineare che non devono necessariamente essere coinvolti tutti i responsabili delle funzioni aziendali, ma solo coloro che sono specificamente dedicati a garantire, in vari modi e con diverse professionalità, la sicurezza delle informazioni e la protezione dei dati personali. In altri termini, l'*organigramma della sicurezza* non deve necessariamente replicare la struttura dell'organigramma aziendale. E' indispensabile però che il Responsabile del sistema sia un efficace canale di comunicazione con la Direzione aziendale che, a sua volta, deve fornire tutto il proprio appoggio affinché i diversi Responsabili dei trattamenti abbiano risorse e autorità adeguate a garantire un efficiente funzionamento del sistema.

Le attività sono assegnate in base ai ruoli aziendali definiti, conformemente a quanto previsto nel documento “profili professionali” pubblicato da AgID.

Il sistema di conservazione digitale della GHS Media è fisicamente e logicamente separato dal sistema documentale, la cui gestione ricade sotto la responsabilità dell'Ente produttore, sia esso il Cliente o un terzo delegato dal Cliente stesso.

Il processo di conservazione, qui presentato in dettaglio e secondo le indicazioni fornite dalla norma, mostra una struttura e un'organizzazione, nonché una politica gestionale, atte a garantire l'aderenza alla normativa vigente in materia di conservazione digitale. Il Responsabile del servizio di conservazione, insieme alle altre figure professionali individuate ed elencate in questo manuale, ha definito l'operatività e le attività di conservazione secondo quanto dettato dalla normativa vigente, coerentemente alle politiche di efficienza gestionale e di risorse dell'azienda GHS Media Srl, per far in modo che tutte le attività per arrivare alla conservazione digitale siano organizzate per produrre massima efficienza nell'ambito del processo globale di conservazione digitale.

Il personale coinvolto nel servizio sono previste, ad esempio, le seguenti attività di formazione:

- il corretto utilizzo dei sistemi IT impiegati a supporto dell'attività quotidiana (e-mail, software ecc.);
- la responsabilità ed il ruolo;
- sessioni di formazione ove si tratti di personale in nuovo ingresso
- aggiornamento professionale dimostrabile con attestato di partecipazione rilasciato internamente o da ente esterno, a seguito di modifiche a norme e/o funzionalità e/o processi gestionali, e/o requisiti di sicurezza

L'analisi di eventuali problematiche viene assegnata dal RSDC alla funzione o alle funzioni competenti. Il risultato delle analisi viene condiviso con le funzioni coinvolte nella risoluzione, e le azioni correttive vengono coordinate e supervisionate dal RSDC.

Ove necessario è cura del RSDC coinvolgere nel processo di analisi e risoluzione il RDC dell'archivio di riferimento.

Il RSDC, inoltre, pianifica nel dettaglio, insieme alle funzioni da lui delegate a tali compiti, gli interventi di manutenzione necessari per garantire il mantenimento delle condizioni di sicurezza ed il minore impatto sulla produzione.

Di seguito lo schema che descrive sinteticamente il processo di conservazione e il coinvolgimento delle singole funzioni all'interno delle diverse fasi:

Attività	Descrizione	Referente
definizione e attuazione delle politiche complessive e di gestione del Sistema	predisposizione e aggiornamento del Manuale di conservazione in funzione delle tipologie documentali da conservare; pianificazione dei progetti di sviluppo del sistema di conservazione	RSDC – RSSC – CS
attivazione del servizio di conservazione	gestione della parte contrattuale, compresi documenti di delega a RSDC, Privacy, credenziali di firma, deleghe, ecc. ecc.	COMM - CSOP – RP
attivazione del servizio di conservazione	redazione del documento Specificità del contratto che contiene le tipologie documentali oggetto di conservazione, le modalità di trasferimento da parte dell'ente produttore, la descrizione archivistica dei documenti e delle aggregazioni documentali; definizione del set di metadati di conservazione	RDC – PROG – RFAC - CSOP
acquisizione, verifica e gestione dei pacchetti di versamento presi in carico e generazione del rapporto di versamento	presa in carico dei PdV così come trasmessi dal Produttore; verifica della conformità del PdV agli standard condivisi nel documento Specificità del contratto; applicazione dei seguenti controlli: verifica di leggibilità dei file, presenza dati minimi obbligatori, verifica presenza e validità della firma digitale (ove prevista); trasmissione e memorizzazione del rapporto	RSDC – RSMC - CSOP

	di versamento, comprensivo di eventuali anomalie	
preparazione e gestione del pacchetto di archiviazione	aggregazione dei documenti secondo quanto previsto nel documento Specificità del contratto, nel rispetto della normativa vigente in materia di conservazione digitale di documenti informatici e documenti fiscalmente rilevanti; applicazione di specifici controlli di conformità definiti in base alla classe di appartenenza del documento trattato, del formato di conservazione, della sua rilevanza fiscale, ecc. ecc.; creazione degli indici di conservazione nel formato UNI SinCRO e chiusura del PdA tramite apposizione della firma digitale del RDC e della Marca Temporale	RSDC – CS – RSNC – CS_OP
preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta	assicurare assistenza al Cliente in occasione di verifiche da parte delle Amministrazioni competenti o da parte di organismi di controllo interni	RSDC – CS - RFAC
predisposizione della presenza di un Pubblico Ufficiale qualora si renda necessario	valutare e pianificare la necessità della presenza di un Pubblico Ufficiale in tutti i casi in cui sia richiesta la sua presenza, garantendo l'assistenza e le risorse necessarie utili alle attività di controllo e certificazione	RSDC – CS - RFAC
scarto dei pacchetti di archiviazione	individuazione e segnalazione al Titolare dell'archivio dei PdA che hanno raggiunto i limiti di conservazione previsti dalla normativa vigente;	RSDC – RFAC - RSIC

	eliminazione degli stessi previa autorizzazione da parte del Titolare degli archivi e/o autorizzazione delle Soprintendenze Archivistiche provinciali di competenza, qualora necessario.	
chiusura del servizio di conservazione (al termine di un contratto)	predisposizione delle copie dei documenti conservati; predisposizione di un verbale di consegna con l'elenco dei documenti restituiti. Il verbale deve essere controfirmato dal Cliente, o da terzo soggetto delegato. Viene definito un tempo limite di 60 gg all'interno del quale il Cliente può segnalare eventuali anomalie o irregolarità	RSDC – RP - COMM – RSIC
conduzione e manutenzione del sistema di conservazione	verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi; creazione delle copie di sicurezza; migrazione dei documenti conservati su supporti tecnologici più evoluti, qualora si renda necessario;	RSSC – RSIC - RSMC
monitoraggio del sistema di conservazione	coordinare lo sviluppo e la manutenzione delle componenti software del SdC; verificare la funzionalità del SI e dei SW aziendali direttamente o indirettamente coinvolti nel processo di conservazione; garantire la sicurezza fisica e logica dei sistemi informatici che operano nel SdC e delle copie di sicurezza prodotte	RSSC – RSIC - RSMC
change management	i processi sono gestiti in conformità al Piano della	DIR – RSDC – AMM – RSIC - RSMC - CS

	Sicurezza e alle procedure ISO 27001:2014 Le esigenze possono essere determinate da richieste dirette del Cliente (condivise attraverso il documento Specificità del contratto), da modifiche al quadro giuridico e normativo di riferimento, da evoluzioni tecnologiche. Vengono sempre identificati i ruoli e i processi coinvolti e assegnate le responsabilità, così come vengono valutate e messe a disposizione le risorse necessarie: personale, piani di formazione, HW, ecc. ecc.	
verifica periodica di conformità a normativa e standard di riferimento	aggiornamento e formazione continua delle funzioni interessate relativamente alle novità normative in materia di conservazione e dematerializzazione;	RSDC - CS
Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali	Assicurare che i processi di conservazione rispettino quanto previsto dalla normativa	RP

Di seguito viene evidenziata una matrice delle responsabilità con i principali attori coinvolti nel processo di conservazione a norma:

Area del processo	**Attività**	**RDC** o suo	**RSDC** o suo delegato	**Produttore** o suo delegato

		delegato		
Emissione documento informatico	Imputazione dei dati contabili sul gestionale			**O - V - R**
	Estrazione e produzione dei metadati del documento	**V**		**O - V - R**
	Eventuale invio a Indicom del flusso dati tramite canale sicuro	**V**		**O - V - R**
	Produzione del documento in formato PDF e invio a Deliverti tramite canale sicuro	**V**		**O - V - R**
	Eventuale elaborazione flusso dati e produzione documento informatico	**V**		**O - V - R**
	apposizione della firma digitale tramite HSM sicuro e certificato	**V**		**O - R**
	Eventuale apposizione della Marca Temporale (dove richiesto/previsto)	**V**		**O - R**

	Produzione e invio del PdV (Pacchetto di Versamento)	**V**		**O - R**
Processo di conservazione	Download dei dati e dei documenti su DB	**V**	**O-R**	
	Controlli di conformità alla normativa vigente	**V**	**O-R**	
	Produzione del PdA (Pacchetto di Archiviazione)	**V**	**O-R**	
	Apposizione di firma digitale e marca temporale sull' Pacchetto di Archiviazione conforme all'UNISINCRO 11386:2010	**V**	**O-R**	
Altre attività	Pagamento imposta di bollo (ove richiesto)			**O - V - R**
	Verifica periodica leggibilità documenti conservati	**V**	**O-R**	
	Aggiornamento Manuale CS	**V**	**O-R**	

LEGENDA:

O = Opera

R = Responsabile

V = Verifica

3.1.2 Documentazione per la sicurezza delle informazioni

Definire e documentare una *Politica per la gestione della sicurezza delle informazioni e dei dati personali*, finalizzata a definire gli indirizzi e le regole generali da applicare in materia all'interno di tutta l'azienda è la base di partenza di tutto il sistema di gestione. La politica, sintetica ed estremamente comprensibile nella sua stesura, deve includere:

- ✓ una definizione di cosa si intende come *sicurezza delle informazioni*, dei suoi obiettivi e della sua importanza, in linea con gli obiettivi aziendali e la normativa sulla privacy;
- ✓ un indirizzo generale e i principi di azione concernenti la protezione dei dati personali;
- ✓ la descrizione dei processi necessari alla gestione della sicurezza delle informazioni e dei dati personali;
- ✓ la formalizzazione di ruoli e responsabilità;
- ✓ i criteri rispetto ai quali ponderare i rischi.

Tale Politica deve essere riesaminata almeno con cadenza annuale e venire approvata dalla Direzione affinché sia garantito e visibile il necessario appoggio.

Alla Politica deve essere associato un *Elenco della documentazione aziendale* (procedure) rilevante sul tema.

Il Documento programmatico per la sicurezza, se già presente, può essere convenientemente aggiornato e inserito nel suddetto elenco, anche se non più richiesto dall'attuale normativa privacy. Si raccomanda comunque di descrivere in un documento i meccanismi di sicurezza implementati.

Le procedure operative che guidano in maniera puntuale l'attuazione di quanto indicato nella politica possono essere definite in modo informale nelle aziende di più ridotte dimensioni mentre, con il crescere del numero delle persone, delle sedi e della complessità del business, aumenta la necessità di averle formalizzate all'interno di un unico documento o come oggetti separati per un più facile aggiornamento. Anche tali procedure dovrebbero essere riesaminate con cadenza annuale, in occasione degli audit interni.

I temi da trattare nelle procedure sono legati alla realtà aziendale e ai rischi che incombono su di essa. Quelli più frequentemente indirizzati sono:

- gestione della documentazione;
- gestione degli asset;
- controllo degli accessi fisici e logici;
- gestione delle utenze;
- gestione degli incidenti;
- back-up e ripristino;
- modalità di conduzione degli audit interni.

E' opportuno sottolinear e come le procedure siano funzionali all'esecuzione di azioni specifiche, sovente legate a flussi operativi. In tale prospettiva possono anche essere formalizzate in modo estremamente schematico indicando la sequenza delle attività e i corrispondenti ruoli degli attori coinvolti.

Si ricorda che l'Allegato B del D.lgs. 196/03 e s.m.i ,e successivamente sostituito dal Regolamento Europeo 679/16, richiede esplicitamente la descrizione scritta di alcune attività: si raccomanda di includerle nelle procedure sopra elencate.

Si raccomanda inoltre di documentare per iscritto le regole per la corretta gestione delle informazioni e dei dati personali e degli strumenti aziendali connessi al loro trattamento. Esse dovrebbero essere mantenute aggiornate e distribuite a tutti gli incaricati o ai soggetti interessati dove rilevante. Tali regole, aggregabili anche in un solo documento, possono includere:

- le modalità di classificazione e etichettatura dei dati (vanno ad esempio identificati i dati personali di natura sensibile o le informazioni rilevanti per garantire la loro

disponibilità, integrità o riservatezza) considerando i diversi supporti (per esempio, cartacei ed elettronici) su cui possono essere mantenuti;
- le regole di trattamento di informazioni e dati personali lungo tutto il loro ciclo di vita;
- le regole di accesso fisico e logico e le relative richieste ed assegnazioni dei diritti di accesso alle informazioni;
- le regole per l'uso di Internet e della posta elettronica;
- le regole per l'uso di computer, telefoni e altre tecnologie in dotazione.

Le suddette regole dovrebbero trovare applicazione nelle procedure operative.

Il SdC adottato da IDC è conforme a quanto previsto dalle regole tecniche di cui al DPCM 3 dicembre 2013 ed allo standard ISO 14721:2012 OAIS (Open Archival Information System) e successive modifiche.

Il processo prevede quindi l'utilizzo di Pacchetti Informativi, che rappresentano lo stato della documentazione nelle fasi di vita all'interno del SdC:

- ✓ immissione in archivio;
- ✓ archiviazione e conservazione;
- ✓ distribuzione ed esibizione.

Come previsto dalle "Regole tecniche in materia di sistema di conservazione" dell'art. 3, c. 1 del Decreto della Presidenza del Consiglio dei Ministri 3 dicembre 2013, il sistema di conservazione IDC assicura dalla presa in carico fino all'eventuale scarto, la conservazione tramite l'adozione di regole, procedure e tecnologie degli oggetti in esso conservati, garantendone oltre all'autenticità, all'integrità, all'affidabilità e alla leggibilità anche la reperibilità.

La GHS Media s.r.l. ha definito una policy per assicurare la conservazione nel tempo delle informazioni, la tipologia degli oggetti sottoposti a conservazione, comprensiva dell'indicazione dei formati gestiti. Sono descritte e verificate le caratteristiche e le proprietà degli oggetti preservati, al fine di confermare l'autenticità od individuare errori rispetto a tali oggetti. E' mantenuta la documentazione delle tipologie degli oggetti sottoposti a conservazione, per rendere chiari ai fruitori le caratteristiche e le proprietà degli oggetti preservati. Il servizio di conservazione permette di associare a ciascun documento che compone l'unità documentaria un set di metadati. Quest'ultimi rendono agevole la ricerca di

un documento, permettono di identificarli, collocarli e fornire un riferimento alla struttura di ogni documento e al suo formato. I metadati permettono inoltre di individuare gli elementi che possono attestare l'integrità e l'autenticità dei documenti versati.

Avremo pertanto:

- metadati identificativi dell'unità documentaria da versare
- metadati che descrivono il documento principale versato
- metadati che descrivono ogni singolo allegato/annesso/annotazione versata (se presenti)

Oltre a questi metadati il sistema memorizzerà anche gli indici associati al processo di conservazione.

In fase di versamento ogni unità documentaria viene descritta da una serie di metadati, raggruppati in macro classi.

Il processo di conservazione digitale si effettua sugli aggregati logici definiti unità documentarie (UD). Queste sono composte da uno o più documenti, di cui almeno un documento principale. In aggiunta a questo sono presenti n documenti allegati, n documenti annessi (documenti prodotti generalmente in un momento successivo rispetto al documento principale) e n documenti annotazioni.

L'Unità Documentaria è identificata univocamente dai seguenti valori:

a) AZIENDA
b) TIPO DOCUMENTO
c) ANNO
d) IDENTIFICATIVO

L'identificativo per alcune classi documentali consiste in una combinazione di metadati che identificano univocamente il documento (es: per i LUL l'identificativo univoco è composto dai metadati 'anno', 'pagina da' e 'pagina a')

Le UD sono formate da uno o più documenti considerati come un tutto unico e costituiscono le unità elementari di cui si compone l'archivio dell'Ente produttore.

Tutti gli oggetti della conservazione sono trattati dal sistema di conservazione in pacchetti informativi che si distinguono in:

A. pacchetti di versamento;
B. pacchetti di archiviazione;
C. pacchetti di distribuzione.

All'interno del documento Specificità del contratto vengono definiti:

- l'elenco dei documenti conservati, i formati e la loro natura
- il formato del PdV e le modalità di versamento nel SdC da parte del Produttore
- l'elenco e la descrizione di eventuali metadati specifici associati ai documenti
- il periodo di conservazione e le modalità di scarto dei PdA
- qualsiasi altra informazione ritenuta utile a definire e regolamentare lo specifico processo di conservazione

I formati gestiti dal sistema per la conservazione di specifiche tipologie documentarie sono concordati con il Produttore ed esplicitati all'interno del documento Specificità del contratto

I principali formati previsti per i documenti sono:

- ✓ XML: SDI 1.0, SDI 1.1
- ✓ PDF (in diverse versioni, principalmente 1.3 e 1.4)
- ✓ PDF/A

I principali formati previsti per gli Indici di Versamento - IdV contenuti nel PdV sono:

- ✓ XML
- ✓ TXT

I formati di firma ammessi sono:

- ✓ PAdES: ETSI TS 102 778
- ✓ CAdES: ETSI TS 101 733
- ✓ XAdES: ETSI TS 101 903

Queste le principali tipologie documentali conservate attraverso la piattaforma della GHS Media s.r.l.:

Documenti sottoposti a conservazione digitale	Processo di conservazione	Documenti sottoposti a conservazione digitale	Processo di conservazione	Documenti sottoposti a conservazione digitale
Fatture attive PA	Conservazione digitale di documento elettronico	XML con firma CAdES o XAdES	almeno annuale	-Cognome -Nome -Denominazione -Codice fiscale -Partita Iva -Data -Associazioni logiche dei campi
Fatture Attive	Conservazione digitale di documento elettronico o analogico	PDF con firma PAdES o CAdES	almeno annuale	-Cognome -Nome -Denominazione -Codice fiscale -Partita Iva -Data -Associazioni logiche dei campi
Fatture Passive	Conservazione digitale di documento elettronico o analogico	PDF con firma PAdES o CAdES	almeno annuale	-Cognome -Nome -Denominazione -Codice fiscale -Partita Iva -Data -Associazioni logiche dei campi
Libri e Registri Contabili	Conservazione digitale di documento elettronico o analogico	PDF con firma PAdES o CAdES	almeno annuale	Funzione “ricerca” del formato PDF
LUL	Conservazione digitale di	PDF con firma PAdES o CAdES	Mensile	Cognome Nome CF

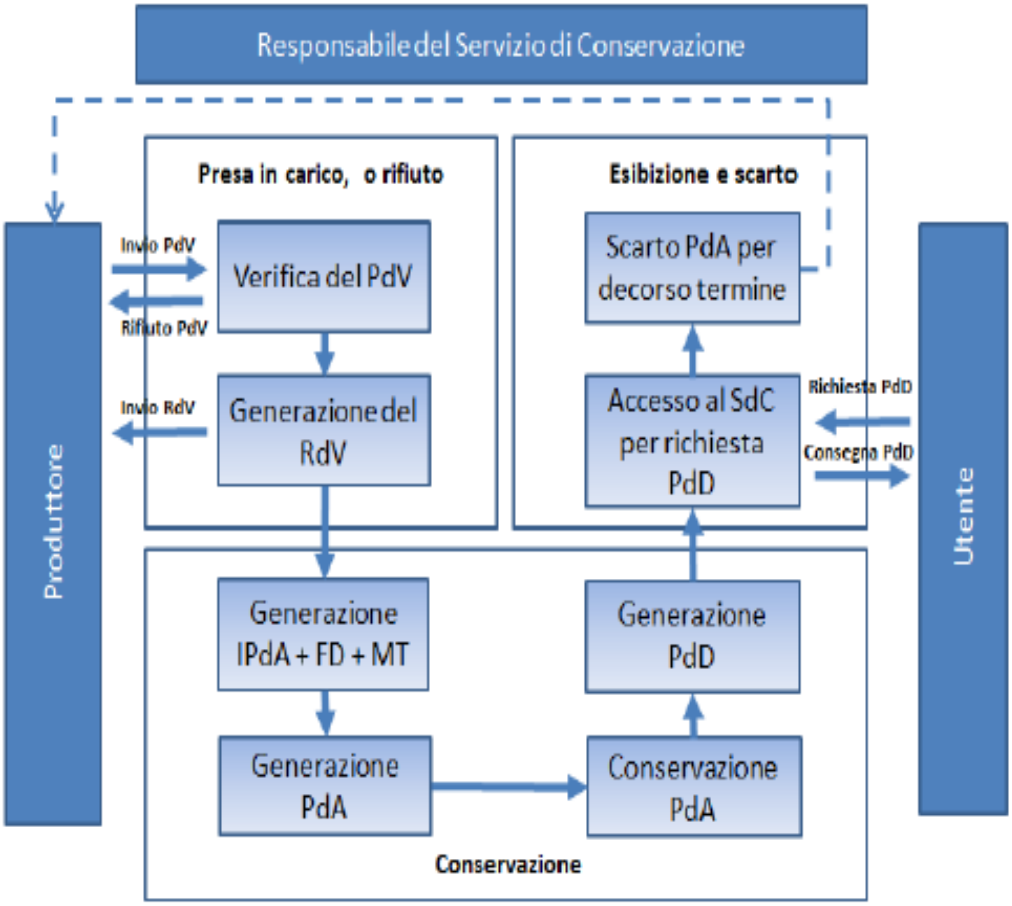
	documento elettronico			Anno Mese

Le tipologie sopra rappresentate sono quelle maggiormente trattate dal sistema di conservazione; le procedure qui descritte valgono anche per le altre tipologie documentali, indipendentemente dalla loro natura contabile, amministrativa o sanitaria.

3.1.2.1 Processo di conservazione

Il processo di conservazione digitale si effettua sugli aggregati logici definiti unità documentarie (UD): queste ultime sono formate da uno o più documenti considerati come un tutto unico e costituiscono le unità elementari di cui si compone l'archivio dell'Ente produttore.

Il processo di conservazione digitale avviene secondo le modalità sintetizzate nei seguenti punti:



- Presa in carico, acquisizione o rifiuto
- ✓ L' Ente produttore invia in conservazione le unità documentarie aggregate in Pacchetti di Versamento (PdV). Il sistema esegue i controlli automatici di congruenza sui PdV versati, che ne determinano la presa in carico.
- ✓ Il sistema genera il Rapporto di Versamento (RdV) che viene messo a disposizione dell'Utente, esternamente al SdC per eventuali esigenze applicative

- Conservazione
    - Il sistema, con cadenza opportuna, definisce il Pacchetto di Archiviazione (PdA) che consiste in una o più UD costituito secondo criteri totalmente configurabili che ne determinano i rispettivi contenuti e le dimensioni, ai quali si applica unitariamente il processo di conservazione digitale. Il sistema di conservazione gestisce esclusivamente PdA omogenei, ovvero composti da UD della stessa tipologia.
    - Il sistema è configurato per effettuare controlli automatici di congruenza del PdA; in aggiunta è possibile prevedere una ulteriore fase di verifica manuale operata dal responsabile della conservazione o da un suo delegato.
- ✓ La procedura di chiusura prevede:
    - la generazione dell'Indice Pacchetto di Archiviazione (IPdA - SinCRO)
    - la firma digitale del Responsabile del Servizio di conservazione che attesta il regolare svolgimento del processo di conservazione
    - l'apposizione della marca temporale.
    - Il PdA è archiviato nell'archivio di conservazione
    - Per ogni operazione di conservazione il sistema genera il relativo Pacchetto di Distribuzione (PdD), per consentire l'esibizione e la fruizione dei archiviati documenti conservati
- ✓ Esibizione
    - gli utenti autorizzati possono acceder alla piattaforma e ricercare, visualizzare e scaricare i PdA

Alla decorrenza dei termini di conservazione viene effettuato lo scarto dei PdA.

Il versamento dei documenti viene effettuato in modalità asincrona e prevede che il sistema versante possa inviare una singola Unità Documentaria (UD).

L'unita minima di versamento è l'Unità Documentaria. Ogni unità documentaria è composta da uno o più documenti, di cui almeno un documento principale. In aggiunta a questo, è possibile gestire documenti allegati, documenti annessi (documenti prodotti generalmente in un momento successivo rispetto al documento principale) e annotazioni.

Più in dettaglio il processo si compone dei seguenti passi operativi:

Il Produttore produce il PdV così come definito del documento Specificità del Contratto e lo trasferisce al SdC (Pacchetto di versamento).

Un processo gestito dal sistema effettua il versamento delle UD attivando, in modalità sincrona e in un contesto transazionale, i sotto-processi:

- Acquisizione dei metadati che caratterizzano la UD, così come definiti nel documento Specificità del Contratto;
- esecuzione dei controlli operati dal sistema di conservazione in fase di versamento.

La comunicazione con il servizio di versamento utilizza prevalentemente lo scambio di messaggi XML strutturati, il cui contenuto viene sottoposto alla validazione attraverso appositi XSD. L'utilizzo degli XSD permette:

- la validazione del contenuto di un elemento o di un attributo rispetto a un determinato tipo di dato;
- la verifica della presenza dei metadati definiti come obbligatori (se questi sono assenti, l'XML non sarà validato nell'applicativo);
- la validazione di espressioni regolari (es. la verifica che un determinato attributo preveda l'immissione di una stringa composta da un numero predefinito di valori).

Ogni XML sarà composto da alcune parti fisse (comuni a tutte le tipologie versate, quindi si definisce uno schema XSD generale) e di altre specifiche per la tipologia documentaria di riferimento.

Nel caso l'indice del pacchetto di versamento consista in un file di testo, il controllo formale consisterà nella verifica della struttura del file sulla base delle specifiche contenute nel documento Specificità del Contratto.

In fase di versamento il sistema opera i seguenti controlli formali, specifici per ogni tipo di documento:

1. la verifica della presenza dei metadati definiti come obbligatori per ciascuna tipologia di documento;
2. la validazione dei tipi di dato.
3. controllo dell'univocità della chiave (il sistema controlla che l'unità documentaria non sia stata già versata)

Di seguito i controlli applicati ai principali documenti aventi rilevanza fiscale:

Metadato	Descrizione del controllo	Applicazione
Codice Azienda	Non può essere vuoto	Tutte le tipologie di documento
Produttore	Non può essere vuoto Deve essere coerente con quanto definito nel documento Specificità del contratto	Tutte le tipologie di documento
Tipo Documento	Non può essere vuoto	Tutte le tipologie di documento
Anno	non può essere vuoto	Tutte le tipologie di documento
Numero Documento (Numero Fattura / Protocollo Iva …)	non può essere vuoto	Tutte le tipologie di documento
Numero Documento (Numero Fattura / Protocollo Iva …)	E' possibile configurare la formattazione del numero fattura e il sistema verifica che il progressivo sia un campo numerico	Tutte le tipologie di documento
Partita IVA	controlli di congruenza sul formato	Fattura Cliente e Fattura Fornitore
Data Documento / Data Registrazione	non può essere vuoto	Tutte le tipologie di documento
Congruenza metadati-documenti	Ad ogni set di metadati associati ad una UD deve corrispondere un oggetto digitale (pdf o tif) e viceversa (eventuali eccezioni vengono segnalate nella base dati di staging presente in Oracle)	Fattura Cliente e Fattura Fornitore

Tutte le operazioni di versamento effettuate dal Produttore, identificato in modo certo verso il sistema di conservazione, vengono tracciate in specifici log applicativi direttamente sul database di conservazione, in una tabella specifica riservata appunto ai log di versamento e indicando le tipologie delle informazioni contenute nel pacchetto di versamento.

Le informazioni sui PdV sono rese disponibili agli operatori attraverso il modulo “registro di Versamento”. All’interno del Registro sono disponibili i seguenti Tab:

1. Dati Operazione: Codice Versamento, Azienda, Descrizione, Data Versamento, numero anomalie, dettaglio documenti scartati, totale documenti
2. Documenti: elenco dei documenti contenuti nel PdV
3. Annessi: Indice del PdV, RdV
4. Procedimento: da utilizzarsi per l’eventuale lancio manuale di attività pre-configurate
5. Visibilità: profilo dell’utente collegato
6. Note: consente l’inserimento di eventuali annotazioni operative
7. Anomalie: registro delle anomalie rilevate dalla piattaforma
8. Storico: registro delle attività legate al PdV

I log memorizzati su database vengono mantenuti online per tutta la durata del periodo di conservazione ed esportati ogni notte tramite una procedura automatica sul Syslog centrale da cui giornalmente viene prodotto un file firmato digitalmente dal RSDC.

L’accesso al database dei log è consentito solo agli amministratori del sistema e al responsabile del servizio di conservazione, che hanno la possibilità di effettuare un export del log ricercato, firmato e marcato dal responsabile.

Durante la presa in carico del PdV viene eseguita la verifica di conformità delle firme presenti.

Eventuali accordi specifici sono riportati nel documento Specificità del contratto.

Segue l'elenco dei possibili controlli operati dal sistema:

a) Controllo di obbligatorietà: il controllo ha lo scopo di appurare la presenza di una firma digitale che attesti la provenienza e l'autenticità del documento. Il controllo viene svolto su tutti i documenti aventi rilevanza fiscale. Qualora, in seguito a specifici accordi con il Cliente, la firma sul documento debba essere apposta nell'ambito del processo di conservazione, le verifiche verranno eseguite contestualmente alla creazione del PdA. Per le altre tipologie documentali il controllo può essere attivato sulla base degli accordi condivisi con il Cliente. Se il controllo fallisce l'UD viene scartata.
b) Controllo di conformità della firma (embedded o detached): verifica se la sua struttura è conforme rispetto a uno dei formati riconosciuti (CAdES, PAdES o XAdES). Se il controllo fallisce l'UD viene scartata.
c) Controllo di tipo crittografico: verifica l'autenticità del documento. Se il controllo fallisce l'UD viene scartata.
d) controllo di tipo catena-trusted: verifica che il certificato utilizzato per la sottoscrizione del documento sia stato emesso da una Certification Authority accreditata per la PA. Se il controllo fallisce l'UD viene scartata.
e) controllo sul tipo certificato: verifica gli attributi del certificato che deve essere abilitato per la sottoscrizione. Se il controllo fallisce l'UD viene scartata.
f) controllo di tipo certificato: verifica la scadenza del certificato. Se il controllo fallisce l'UD viene scartata o accettata sulla base di specifici accordi con il Cliente.
g) controllo di tipo CRL: l'ultimo controllo viene effettuato solo sul primo documento di ciascun PdV ed ha lo scopo di verificare che il certificato non sia stato revocato. Se il controllo fallisce l'UD viene scartata o accettata sulla base di specifici accordi con il Cliente.

Se in un PdV è presente almeno una UD che viene scartata, il sistema effettua lo scarto della singola UD o dell'intero PdV, sulla base di specifici accordi con il Cliente

3.1.3 Consolidamento dell'ambito ed Analisi del rischio

La definizione iniziale dei processi aziendali da considerarsi in ambito, effettuata prima dell'assegnazione dei ruoli e delle responsabilità, deve essere consolidata, sotto la guida del Responsabile del sistema, con maggiore precisione ed approfondimento.

Prima di effettuare le azioni successive è necessario infatti definire e documentare schematicamente le informazioni, tra cui i dati personali (indicando se sensibili), e i relativi trattamenti, in termini di processi, persone coinvolte e strumenti utilizzati.

Questo lavoro permetterà ad ogni responsabile di avere la visione d'insieme necessaria per poter gestire correttamente le informazioni, tra cui i dati personali, trattati dalla sua area di responsabilità secondo le indicazioni della politica e con il coordinamento del responsabile del SGSI.

Dovrebbe essere garantito l'aggiornamento, su base periodica e in occasione di modifiche organizzative, degli ambiti di trattamento individuati.

L'analisi del rischio può avere diverse finalità, tra le quali: determinare i rischi strategici dell'azienda, quelli finanziari, quelli sulla sicurezza dei lavoratori e, ovviamente, quelli sulla sicurezza dei dati e delle informazioni. In questo documento si tratta di quest'ultima. E' comunque necessario avere ben chiara tale finalità, in modo da individuare i corretti metodi da seguire e non rendere il lavoro troppo oneroso perché non ben finalizzato.

Per quanto riguarda l'analisi del rischio per la sicurezza delle informazioni, seguono i seguenti passi:

- *Stabilire il contesto:* descrivere lo scenario di riferimento (ossia, l'azienda analizzata specificando le attività svolte, le responsabilità designate, i confini fisici e informatici, le relazioni con terze parti, le tecnologie in uso) utilizzando anche quanto definito nel paragrafo precedente in merito al consolidamento dell'ambito;
- *Identificare i rischi:*
    - elenco di tutte le minacce che incombono sulle informazioni e valutare la loro verosimiglianza di accadimento: l'esperienza della Direzione e dei responsabili dei sistemi informativi normalmente rende veloce questo compito (possono considerare

casi già successi nella stessa azienda o in imprese vicine geograficamente o dello stesso settore merceologico);

- identificare le possibili conseguenze di ogni minaccia (per esempio, quale potrebbe essere il danno per l'azienda nel caso in cui si manifestino dei virus sulla rete aziendale o nel caso in cui si danneggino dei file contenenti dati personali o i documenti dei progetti);
- stabilire il livello di vulnerabilità o, viceversa, la robustezza delle misure di sicurezza (in particolare quelle richieste dalla normativa applicabile); questo ultimo passaggio richiede alle persone coinvolte la massima oggettività nell'attribuzione dei valori, senza sottostimare eventuali carenze o sovrastimarle per ottenere più risorse economiche per i progetti di loro riduzione;

➢ *Calcolare i livelli dei rischi:* combinare la verosimiglianza delle minacce, le possibili conseguenze e il livello di vulnerabilità, in modo da assegnare dei valori per ciascun rischio.

3.1.4 Trattamento del rischio

Affinché l'analisi del rischio sia poi utile al processo decisionale, deve essere seguita dai seguenti passi:

1. *Ponderare i rischi:* valutare se i rischi individuati sono accettabili;

2. *Identificare e ponderare le opzioni di trattamento dei rischi*: a fronte dei rischi valutati come inaccettabili, è necessario individuare le possibili azioni da intraprendere e valutarne la fattibilità (per esempio, in alcuni casi le azioni potrebbero introdurre più rischi di quelli attuali oppure avere costi eccessivi);

3. *Pianificare il trattamento dei rischi*: stabilire scadenze, budget e responsabilità per le azioni che si è deciso di intraprendere.

Le azioni di miglioramento individuate sono elencate in un unico documento, detto *Piano di trattamento dei rischi,* per avere un quadro d'insieme delle attività in corso. E' importante

mantenere il collegamento tra azioni intraprese e minacce contrastate, anche al fine di fornire una giustificazione per le scelte compiute.

Le misure di sicurezza dovranno essere controllate nel tempo; in particolare, ne dovrà essere verificata la corretta realizzazione e, periodicamente, il loro buon funzionamento, anche attraverso attività di manutenzione ordinaria o straordinaria (per esempio, a seguito di incidenti).