La gestione dell'Information Security e la normativa di riferimento degli Enti Locali

MODULO 2

LA SICUREZZA DEI PROCESSI DEMATERIALIZZATI E I REQUISITI DELLA NORMATIVA

Agenda

- Impatto della dematerializzazione dei processi e scenari a tendere
- I requisiti richiesti dalla normativa attuale
- La gestione dei processi dematerializzati
- I ruoli e le responsabilità dei processi operativi e di conservazione
- Approccio concreto alla sicurezza standard e modelli di riferimento
- La normativa privacy e focalizzazione sulle tematiche riguardanti gli Enti Locali
- Casi di studio
- Domande e risposte

Impatto della dematerializzazione dei processi e scenari a tendere

Uno degli obiettivi principali della

DEMATERIALIZZAZIONE DOCUMENTALE CON RILEVANZA GIURIDICA

vale a dire la sostituzione del supporto cartaceo con quello informatico nel ciclo di vita dei documenti aventi rilevanza giuridica

E' IL RECUPERO DI EFFICIENZA NEI PROCESSI AMMINISTRATIVI sia della PA sia del settore privato

Impatto della dematerializzazione dei processi e scenari a tendere

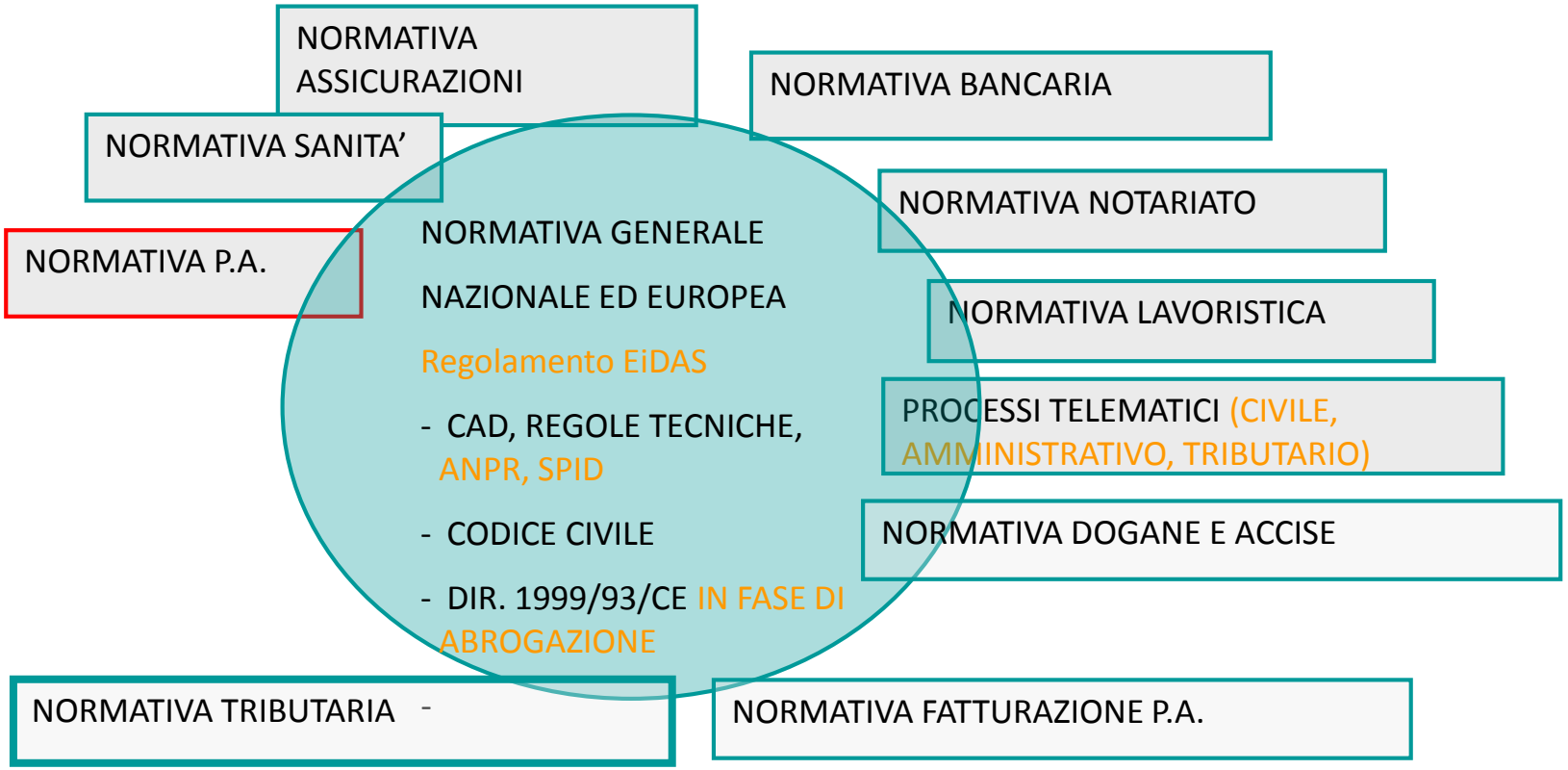
La dematerializzazione viene vista come una risposta fondamentale alle istanze di miglioramento dell'efficienza e di incremento della competitività provenienti dal sistema economico nel suo insieme, quali:

- riduzione dei costi amministrativi e delle spese generali
- integrazione ed ottimizzazione dei flussi documentali
- accelerazione delle transazioni
- riduzione degli errori e dei tempi di risoluzione delle anomalie
- disponibilità di dati più accurati ed aggiornati

- incremento dell'utilizzo dell'ICT nella PA e nelle PMI;
- integrazione con i servizi di e-payment
- supporto allo sviluppo di e-commerce, e-procurement ed e-contract
- creazione di nuovi servizi
- trasparenza, certezza, compliance

Impatto della dematerializzazione dei processi e scenari a tendere

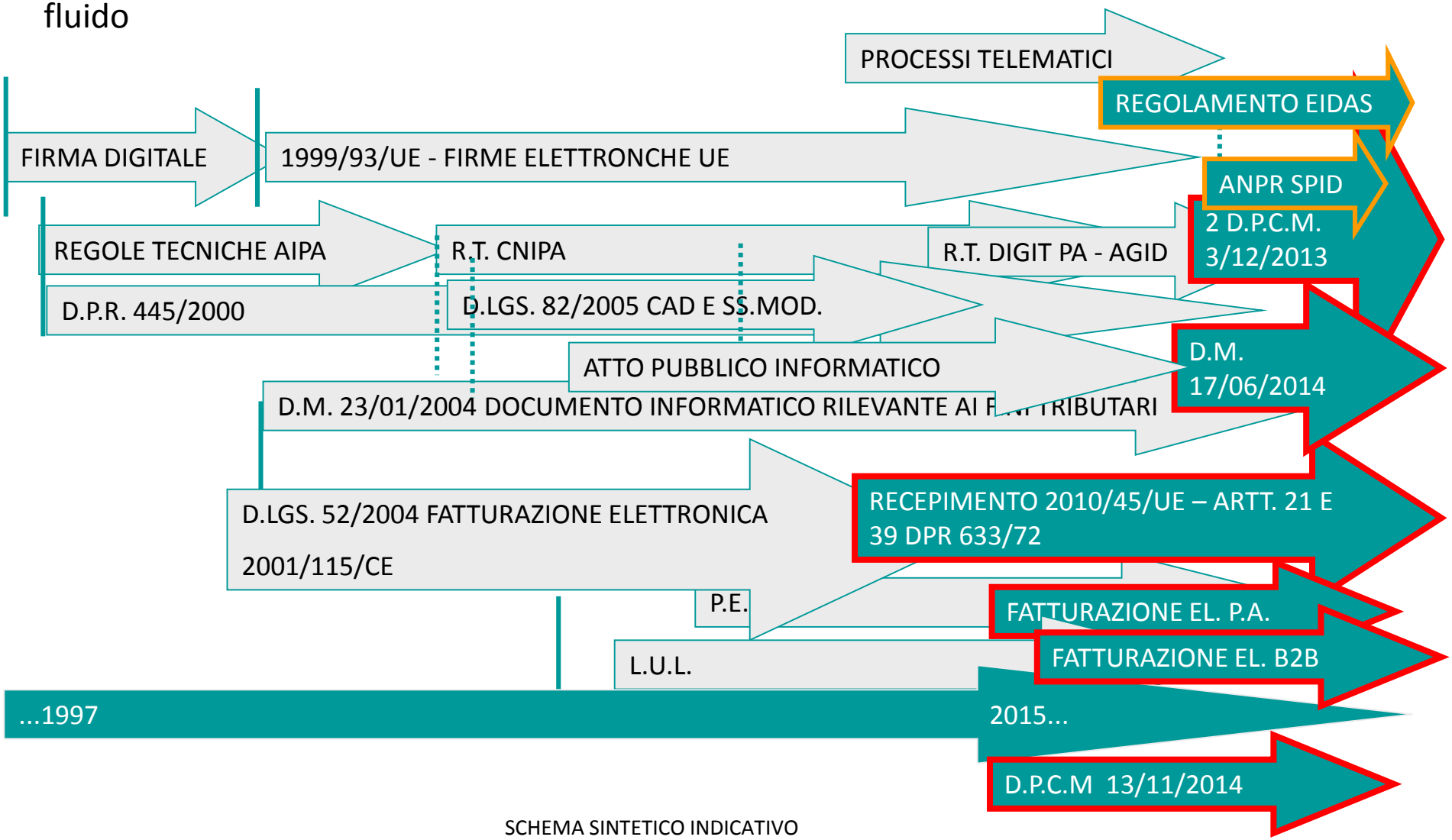
- La normativa vigente in tema di **"dematerializzazione documentale"** consente di attribuire **pieno valore giuridico** al documento informatico
- tuttavia si compone di un **"ceppo comune" generale, dell'Unione e nazionale**, da coniugare e coordinare con le **normative speciali** (settoriali), che, a loro volta, possono integrarsi e intersecarsi



SCHEMA SINTETICO INDICATIVO

Impatto della dematerializzazione dei processi e scenari a tendere

Questo quadro è non solo in continua e irreversibile espansione, ma anche costantemente fluido



SCHEMA SINTETICO INDICATIVO

Impatto della dematerializzazione dei processi e scenari a tendere

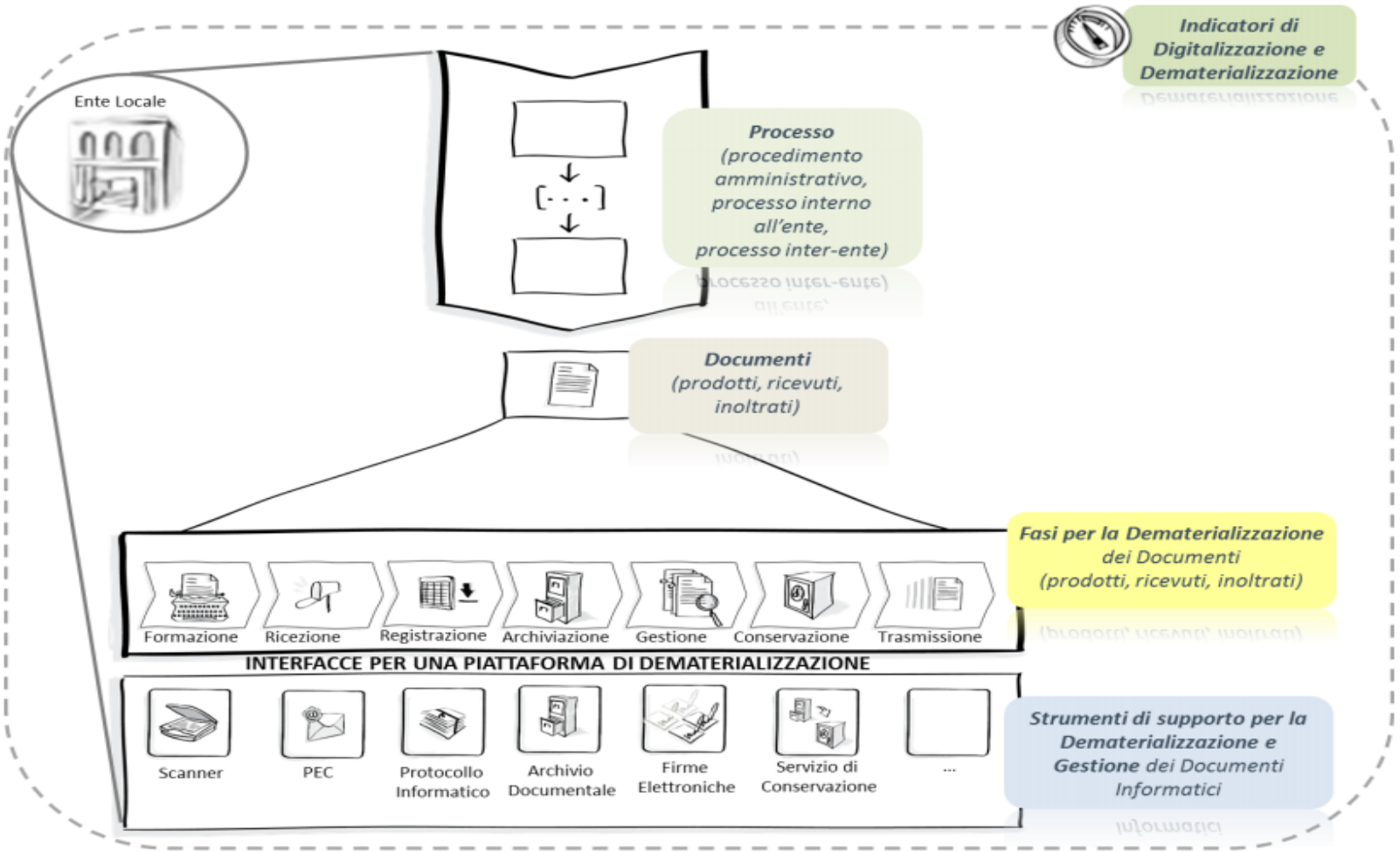
La complessità giuridica si giustifica con la necessità di attribuire al documento informatico una **rilevanza giuridica pre-progettata.**
E' quindi necessario il rispetto delle precise regole stabilite per ogni fase del **ciclo di vita del documento**, **rispetto ai contesti nei quali deve essere utilizzato**

Le principali fasi del ciclo di vita di un documento

- **formazione** (contesto, forma e contenuti obbligatori)
- **imputabilità** della formazione (**autenticità, paternità, integrità**)
- modalità di **tenuta**
- modalità di **emissione, trasmissione, notifica, ricezione**
- modalità di **memorizzazione** e **archiviazione**
- modalità di **conservazione**
- modalità di **riproduzione, duplicazione, modificazione del formato**
- modalità di **rinnovazione**, di **annullamento/estinzione**, di **distruzione**

Impatto della dematerializzazione dei processi e scenari a tendere

La vision della Regione Lombardia per la dematerializzazione negli Enti Locali



Fonte: Dematerializzazione: Linee Guida per gli Enti Locali, Agenda digitale Lombarda

I requisiti richiesti dalla normativa attuale

Le principali disposizioni normative di riferimento per la dematerializzazione

- **D.lgs. 42/2004 e s.m.i.** – Codice dei Beni Culturali e del Paesaggio;
- **D.lgs. n. 82/2005 e s.m.i.** – Codice dell'amministrazione digitale (CAD);
- **D.p.c.m. 3 dicembre 2013** – Regole tecniche in materia di sistema di conservazione;
- **D.p.c.m. 3 dicembre 2013** – Regole tecniche per il protocollo informatico;
- **D.p.c.m. 13 novembre 2014** – Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici;
- Altre regole tecniche su firme elettroniche, validazioni temporali, PEC ecc..

I requisiti richiesti dalla normativa attuale

La dematerializzazione per la PA: un obbligo ineludibile

- ***CAD Articolo 40: Formazione di documenti informatici***

  In vigore dal 25 gennaio 2011 (nella forma originaria dal 2005)

  "Le pubbliche amministrazioni formano gli originali dei propri documenti con mezzi informatici secondo le disposizioni di cui al presente codice e le regole tecniche di cui all'articolo 71."

- ***DPCM 13 novembre 2014 Art. 17***

  In vigore dal 11 febbraio 2015

  "Le pubbliche amministrazioni adeguano i propri sistemi di gestione informatica dei documenti entro e non oltre diciotto mesi dall'entrata in vigore del presente decreto" (AGOSTO 2016)

- ***CAD Articolo 42: Dematerializzazione dei documenti delle pubbliche amministrazioni***

  "Le pubbliche amministrazioni valutano in termini di rapporto tra costi e benefici il recupero su supporto informatico dei documenti e degli atti cartacei dei quali sia obbligatoria o opportuna la conservazione e provvedono alla predisposizione dei conseguenti piani di sostituzione degli archivi cartacei con archivi informatici, nel rispetto delle regole tecniche….."

I requisiti richiesti dalla normativa attuale

- ***CAD Articolo 44: Requisiti per la conservazione dei documenti informatici***

  Il sistema di conservazione dei documenti informatici deve assicurare:

  a) l'identificazione certa del soggetto che ha formato il documento e dell'amministrazione o dell'area organizzativa omogenea di riferimento;

  b) l'integrità del documento;

  c) la leggibilità e l'agevole reperibilità dei documenti e delle informazioni identificative, inclusi i dati di registrazione e di classificazione originari;

  d) il rispetto delle misure di sicurezza previste dal D.lgs. n. 196/2003 (Codice in materia di protezione dei dati personali

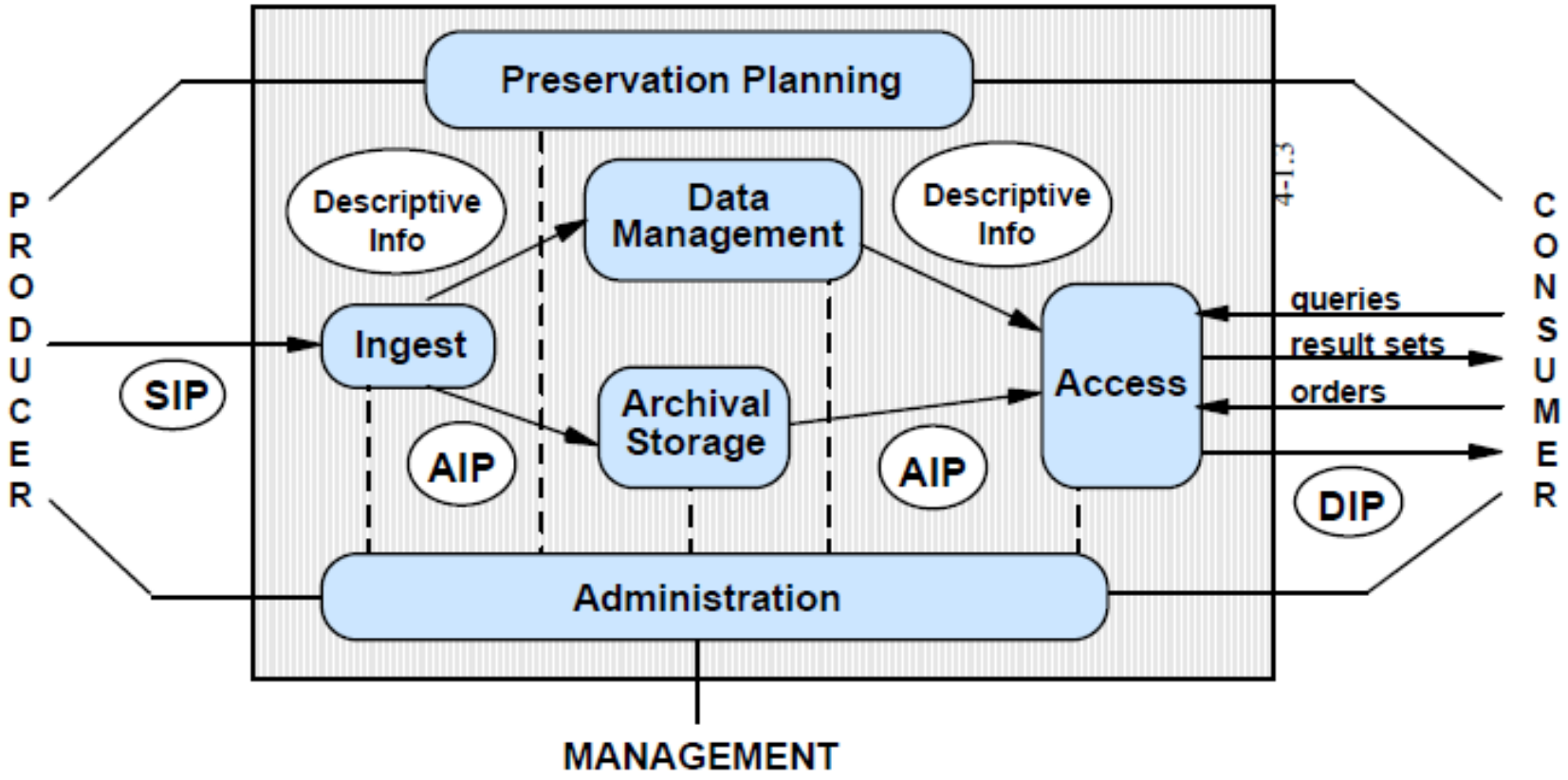
- Il sistema di conservazione assicura, dalla presa in carico dal produttore fino all'eventuale scarto, la conservazione, tramite l'adozione di regole, procedure e tecnologie, degli oggetti in esso conservati, garantendone le caratteristiche di **autenticità, integrità, affidabilità, leggibilità, reperibilità**.

  (art. 3 d.p.c.m. 3 dicembre 2013)

I requisiti richiesti dalla normativa attuale

Il Dpcm 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione

Quale modello di riferimento?
OAIS (open archival information system) Iso 14721:2001



I requisiti richiesti dalla normativa attuale

le principali figure coinvolte nel sistema di conservazione

Nel sistema di conservazione si individuano almeno i seguenti ruoli:

a) Produttore

persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle PA, tale figura si identifica con responsabile della gestione documentale.

b) 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

c) Responsabile della conservazione

soggetto responsabile dell'insieme delle attività elencate nell'articolo 8, comma 1 delle regole tecniche del sistema di Conservazione (DPCM 3 DICEMBRE 2013)

I requisiti richiesti dalla normativa attuale

I modelli organizzativi per la conservazione dei documenti informatici

Il sistema di conservazione opera secondo modelli organizzativi esplicitamente definiti che garantiscono la sua distinzione logica dal sistema di gestione documentale, se esistente.

la conservazione può essere svolta:

a) **all'interno della struttura organizzativa** del soggetto produttore dei documenti informatici da conservare;

b) **affidandola, in modo totale o parziale, ad altri soggetti**, pubblici o privati che offrono idonee garanzie organizzative e tecnologiche, anche accreditati come conservatori presso l'Agenzia per l'Italia digitale.

Le PA realizzano i processi di conservazione all'interno della propria struttura organizzativa o **affidandoli a conservatori accreditati, pubblici o privati presso AGID**

La gestione dei processi dematerializzati

Il **d.p.c.m. 13 novembre 2014** è di importanza fondamentale, in quanto è andato a colmare una lacuna normativa assoluta, finalmente fornendo le regole per la gestione di alcune fasi essenziali del ciclo di vita del documento informatico diverse dalla conservazione. Gli artt. da 3 a 8 stabiliscono regole generali, che poi vengono declinate nel contesto della P.A. dagli artt. da 9 a 16.

- **Art. 3. Formazione del documento informatico**
- **Art. 4. Copie per immagine su supporto informatico di documenti analogici**
- **Art. 5. Duplicati informatici di documenti informatici**
- **Art. 6. Copie e estratti informatici di documenti informatici.**
- **Art. 7. Trasferimento nel sistema di conservazione.**
- **Art. 8. Misure di sicurezza**

---------- CONTESTO P.A. ----------

- **Art. 9. Formazione del documento amministrativo informatico**
- **Art. 10. Copie su supporto informatico di documenti amministrativi analogici**
- **Art. 11. Trasferimento nel sistema di conservazione**
- **Art. 12. Misure di sicurezza**
- **Art. 13. Formazione dei fascicoli informatici**
- **Art. 14. Formazione dei registri e repertori informatici**
- **Art. 15. Trasferimento in conservazione**
- **Art. 16. Misure di sicurezza**

I ruoli e le responsabilità dei processi operativi e dei processi di conservazione

Pubbliche amministrazioni

Responsabile della gestione documentale (e suoi Vicari) già Responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi

Coordinatore della gestione documentale (e suoi Vicari) [eventuale]

Responsabile della sicurezza

Responsabile dei sistemi informativi

Soggetti privati

Conservatori accreditati

Responsabile del servizio di conservazione (e suoi delegati)

Responsabile della funzione archivistica di conservazione

Responsabile della sicurezza dei sistemi per la conservazione

Responsabile dei sistemi informativi per la conservazione

Responsabile dello sviluppo e della manutenzione del sistema di conservazione

Responsabile della conservazione (e suoi delegati)

Responsabile del trattamento dei dati personali

Altri responsabili vengono individuati da normative speciali e settoriali o possono essere individuati in base a norme e principi giuridici di carattere generale

I requisiti richiesti dalla normativa attuale

Sicurezza del sistema di conservazione

Nelle PA vi è l'obbligo predisporre il piano della sicurezza del sistema di conservazione.

il "Piano della Sicurezza del Sistema di conservazione" si pone l'obiettivo di garantire, monitorare e controllare la sicurezza dei sistemi informativi a supporto del Sistema di conservazione, minimizzando il rischio residuo, assicurando la continuità del business e il soddisfacimento dei requisiti relativi alla privacy e alla protezione dei dati personali trattati dall'organizzazione.

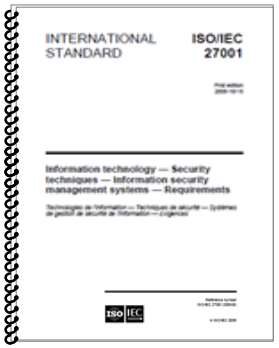
I documenti informatici delle pubbliche amministrazioni devono essere custoditi e controllati con modalità tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alle finalità della raccolta. (CAD Art. 51 comma 2)

Approccio alla sicurezza e modelli di riferimento

Standard di sicurezza

Processi e governo

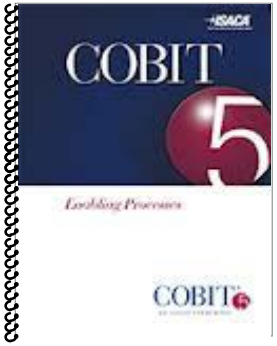
Soluzioni



International Standard ISO/IEC 27001:2005 Information Security Management System Requirements

Standard internazionale (certificabile) per la gestione della sicurezza delle informazioni attraverso l'implementazione e il controllo di un sistema di gestione della sicurezza basato sui principi del miglioramento continuo e definito in base a valutazioni di rischio

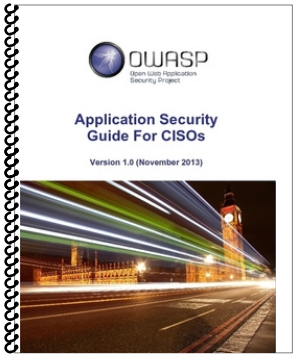
Aggiornamento 2013



COBIT "Control Objectives for Information and related Technology" (modello di riferimento per il governo dell'IT)

Modello per la gestione dei sistemi informativi definito da parte dell'associazione internazionale internal auditor (ISACA) volto a organizzare processi e controlli per il governo dell'IT

Aggiornamento 2013



OWASP (Open Web Application Security Project)

Fornisce indicazioni pratiche ed utili per lo sviluppo sicuro e per la verifica della sicurezza delle applicazioni. Le informazioni sono costantemente oggetto di aggiornamento in funzione dell'evoluzione del contesto tecnologico e delle minacce.

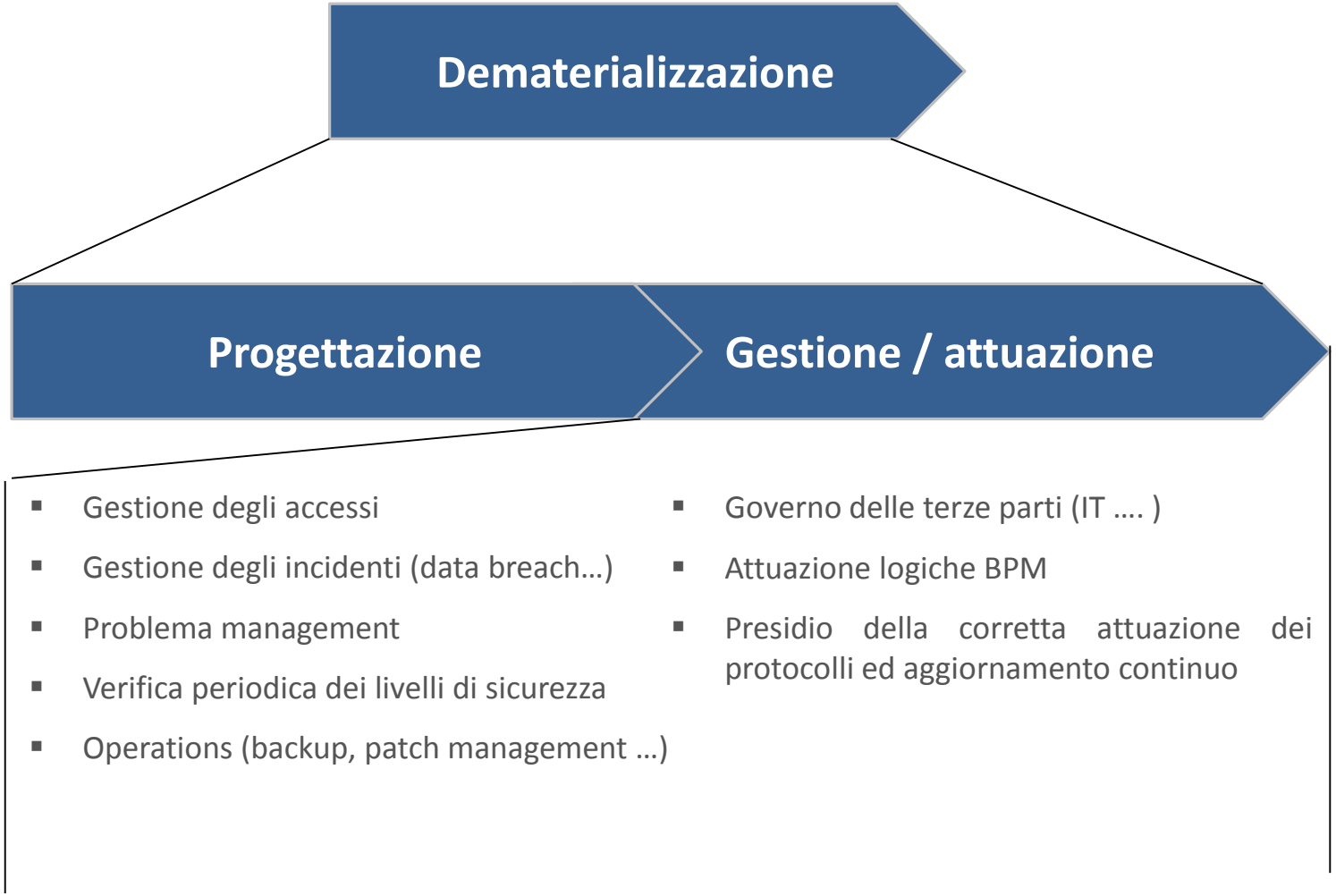
Open source

Le aree della sicurezza da tenere in considerazione

L'attuazione dei processi di dematerializzazione e di gestione dei documenti correlati richiede il governo di alcune aree di sicurezza solo in parte indirizzate puntualmente a livello normativo ….

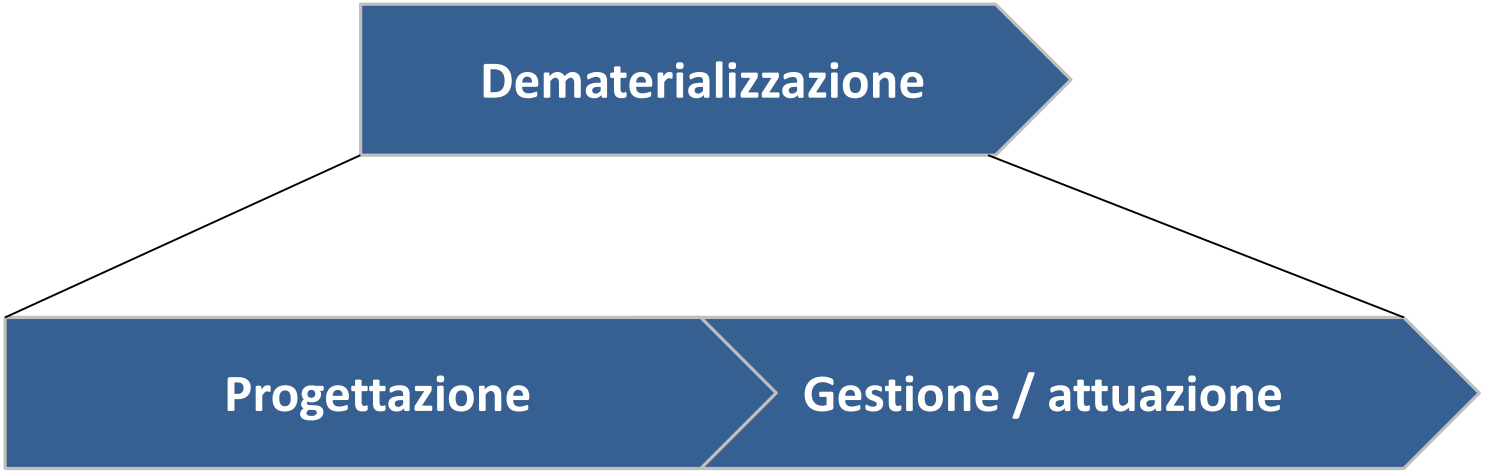
Le aree della sicurezza da tenere in considerazione

L'attuazione dei processi di dematerializzazione e di gestione dei documenti correlati richiede il governo di alcune aree di sicurezza solo in parte indirizzate puntualmente a livello normativo ….



Le aree della sicurezza da tenere in considerazione

L'attuazione dei processi di dematerializzazione e di gestione dei documenti correlati richiede il governo di alcune aree di sicurezza solo in parte indirizzate puntualmente a livello normativo ….



ALCUNI PUNTI CHIAVE PER UNA DEMATERIALIZZAZIONE SICURA

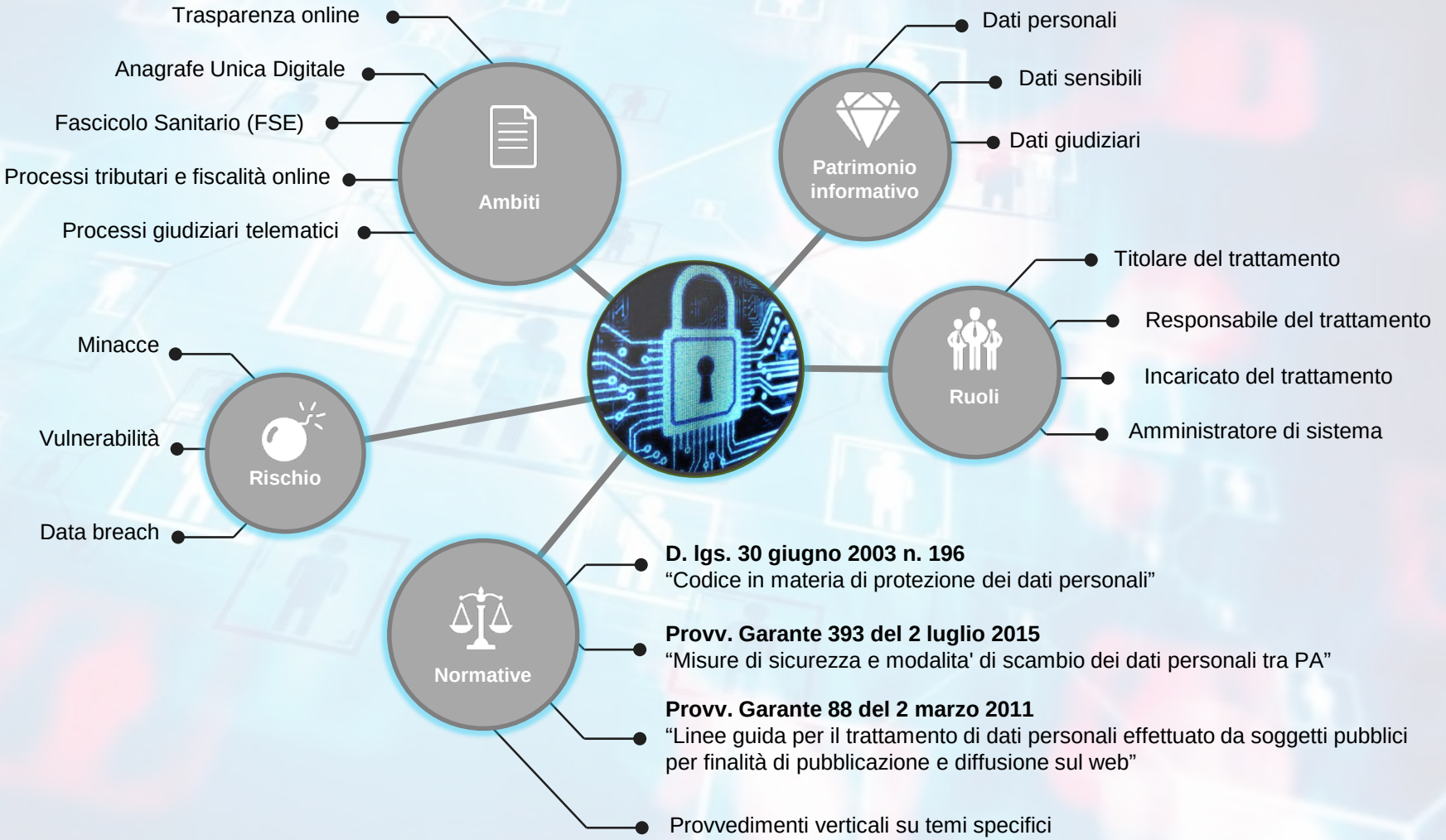
- Considerare tutto il ciclo di vita dei documenti… dalla loro creazione alla loro dismissione…
- Determinare preliminarmente il perimetro di applicazione del processo di dematerializzazione e di gestione dematerializzata in termini di aree funzionali e soggetti esterni coinvolti, ulteriori processi correlati (e requisiti di sicurezza correlati),
- Identificare le normative cogenti e mantenere un presidio
- Attuare un processo di miglioramento continuo, attraverso la promozione di attività di verifica periodica
- Progettare il processo in maniera integrata rispetto al contesto operativo e tecnologico
- Definire da subito il modello di funzionamento a regime … e tutti gli aspetti correlati

La normativa privacy e la focalizzazione sulle tematiche riguardanti gli enti locali

La dematerializzazione dei processi comporta inevitabilmente il trattamento di un maggior numero di informazioni da parte delle Pubbliche Amministrazioni e degli Enti Pubblici.

In aggiunta alle disposizioni ad hoc già presenti nel D.lgs. n. 196/2003 “Codice in materia di protezione dei dati personali” con riferimento ai soggetti pubblici e ai trattamenti in ambito pubblico, l'Autorità Garante della Privacy è intervenuta con una serie di provvedimenti mirati volti a definire linee guida per lo svolgimento sicuro dei processi in cui vengono trattati dati personali nel settore pubblico e ad identificare un set di misure minime di sicurezza che necessariamente devono essere adottate.

La normativa privacy e la focalizzazione sulle tematiche riguardanti gli enti locali



La normativa privacy e la focalizzazione sulle tematiche riguardanti gli enti locali

Principali definizioni

TRATTAMENTO

qualunque operazione, effettuata anche senza l'ausilio di strumenti elettronici, concernente la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati.

DATO PERSONALE

qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

DATI SENSIBILI

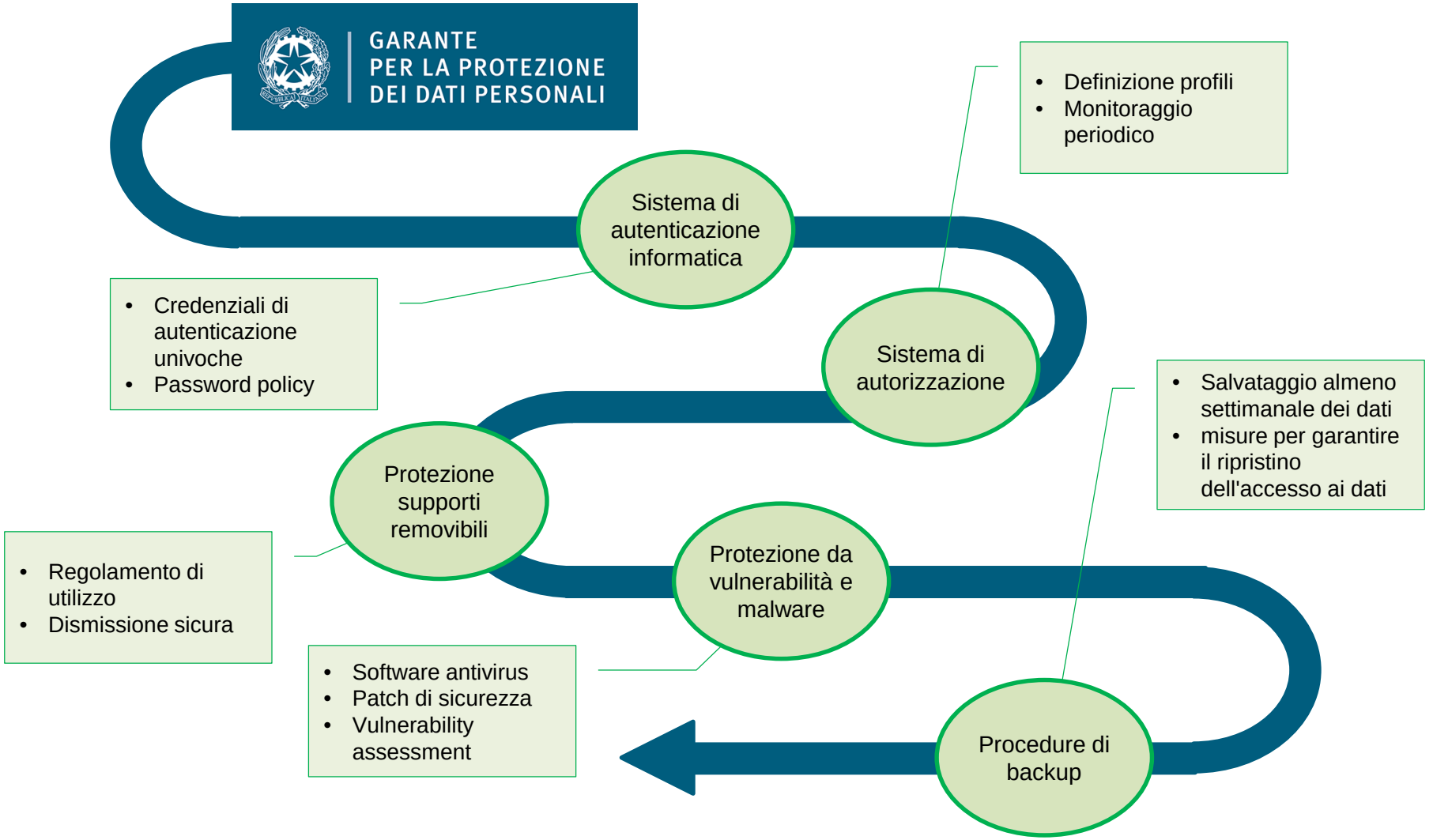
dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

DATI GIUDIZIARI

dati personali idonei a rivelare provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale

La normativa privacy e la focalizzazione sulle tematiche riguardanti gli enti locali

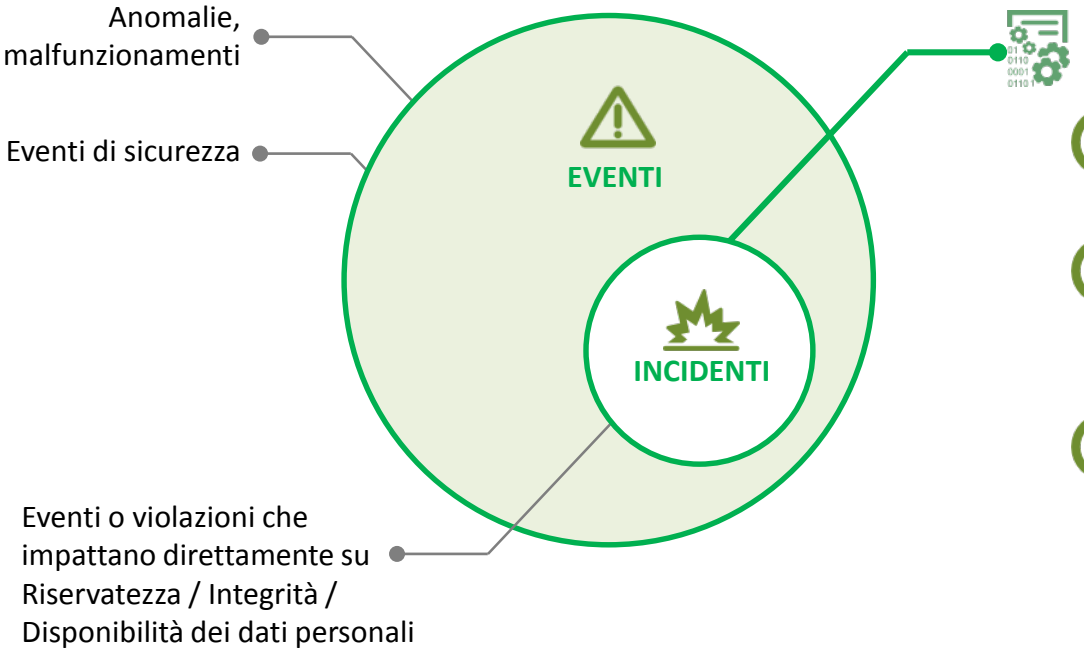
Misure minime di sicurezza



La normativa privacy e la focalizzazione sulle tematiche riguardanti gli enti locali

Comunicazione delle violazioni

Per via delle peculiari caratteristiche delle banche dati delle Amministrazioni Pubbliche, contraddistinte dall'ingente mole di dati trattati, dalla delicatezza delle informazioni ivi contenute e dalla molteplicità di soggetti autorizzati ad accedervi, eventuali violazioni dei dati o incidenti informatici (accessi abusivi, azione di malware) che, pur non avendo un impatto diretto su di essi, possano comunque esporli a rischi di violazione devono essere comunicate tempestivamente al Garante Privacy.



Incident Management

- Indirizzare il trattamento degli incidenti
- Garantire il tempestivo riconoscimento e gestione degli incidenti
- Comunicare entro 48h dalla conoscenza del fatto, tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali

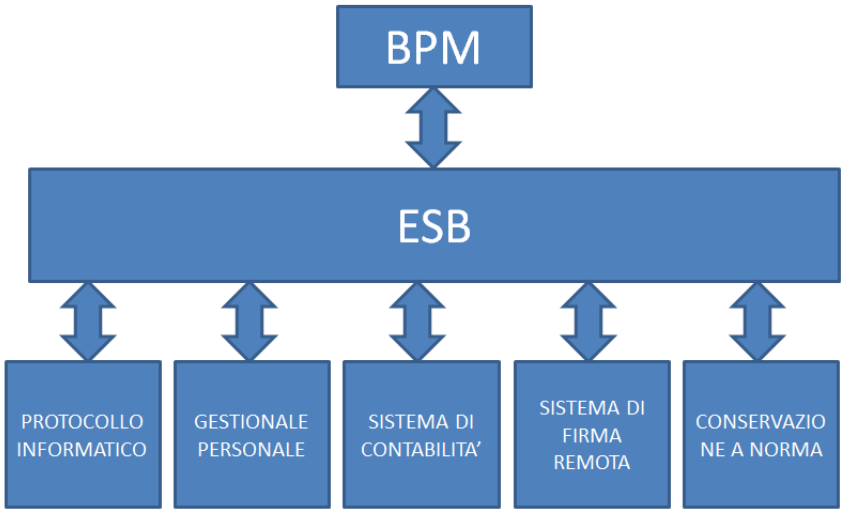
Casi di studio

Saranno presentati a cura di Digicamere una serie di Screenshot con riferimento alla digitalizzazione di alcuni processi di gestione documentale progettati e realizzati per le camere di commercio quali ad esempio:

- la gestione e la conservazione del registro di protocollo informatico
- la gestione e la conservazione delle fatture elettroniche PA
- Le funzioni di sicurezza e segregazioni di funzioni attivate

Casi di studio – Il modello DigiCamere

Infrastruttura del sistema



Holding camerale : 18 mesi di utilizzo, 700+ utilizzatori suddivisi in 100+ uffici, 51.000+ documenti firmati digitalmente

Flussi ciclo passivo conclusi:

- 3.000+ determine
- 2.500+ Richieste di Acquisto e Ordini
- 12.000+ Fatture passive
- 12.000+ Mandati di Pagamento

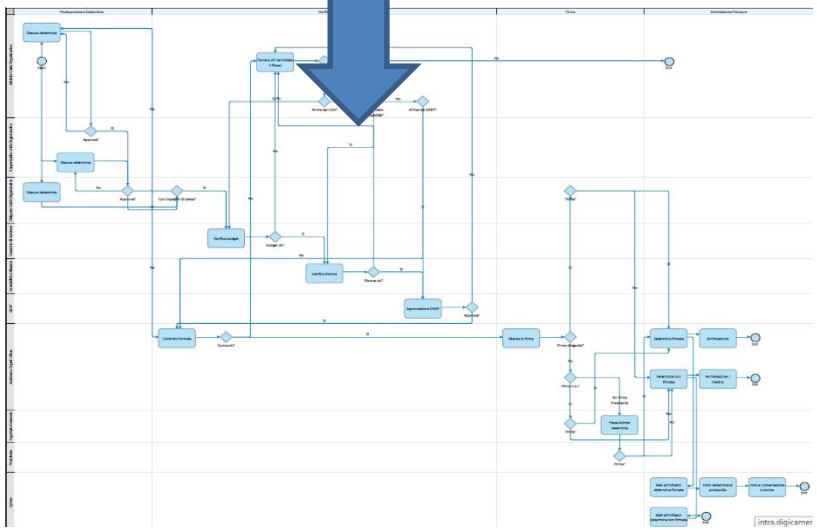
- Disegno e Digitalizzazione dei processi dell'intero Ciclo Passivo :
  - Determine
  - Acquisti (Richiesta d'acquisto, Ordinativo e Contratti)
  - Fatturazione Elettronica Passiva
  - Pagamento elettronico dei Mandati
- Disegno e Digitalizzazione di parte dei processi del Ciclo Attivo
  - Fatturazione Elettronica Attiva
  - Riscossione elettronica delle Reversali
- Disegno e Digitalizzazione altri processi verticali

Casi di studio - I processi del ciclo passivo e la gestione dei ruoli

Creazione Richiesta d'Acquisto → Selezione del fornitore → Approvazione Richiesta → Generazione Ordine → Doppia firma Ordine → Invio Ordine al fornitore

Creazione Mandato di Pagamento ← Approvazione Pagamento ← Valutazione Fattura ← Registrazione Fattura in contabilità ← Ricezione Fattura Elettronica

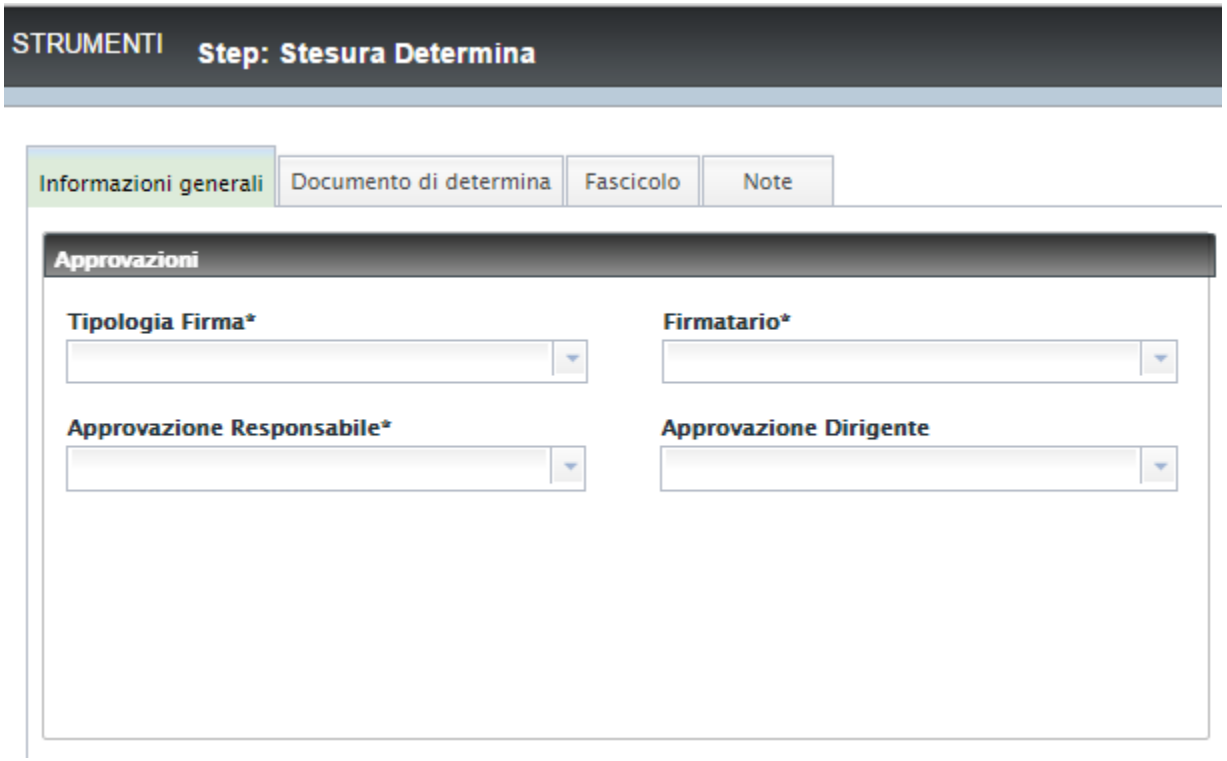
Generazione del tracciato informatico del pagamento → Doppia firma del Mandato → Invio del Mandato al Tesoriere → Elaborazione risposte Tesoriere → Archiviazione a norma del Mandato



Casi di studio – La gestione degli aspetti di sicurezza…

… Sicurezza nella Profilazione

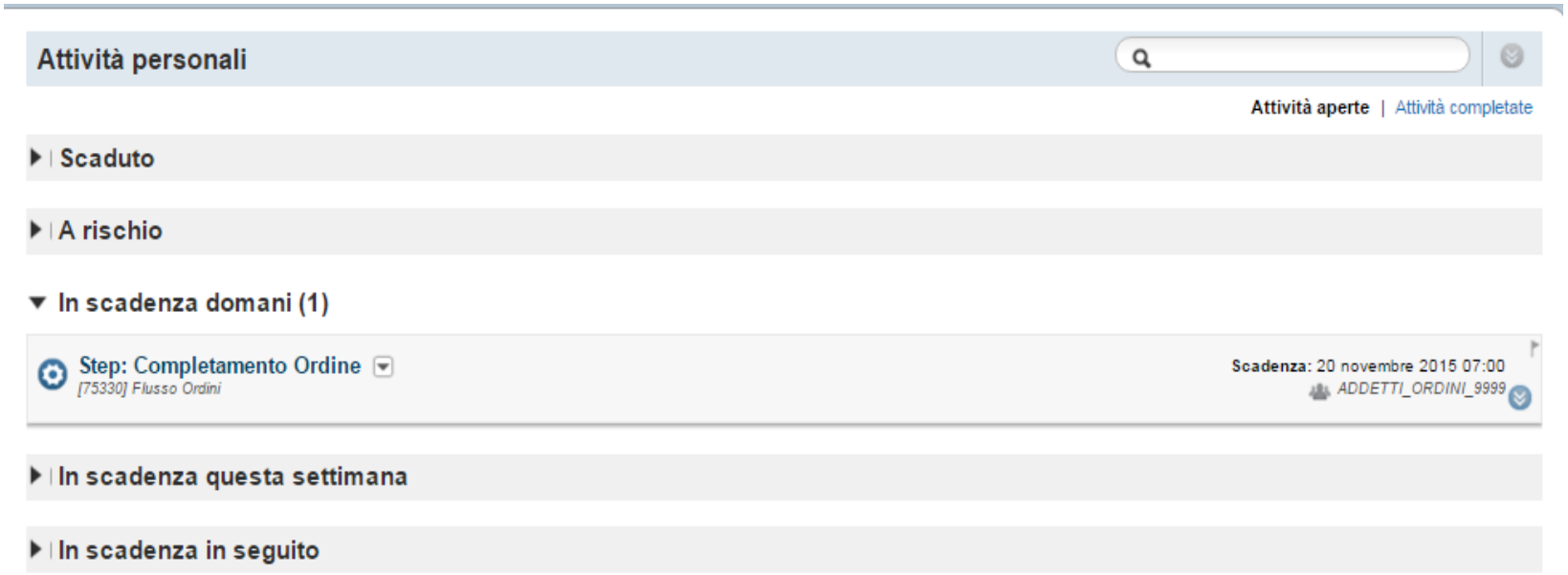
Il sistema è direttamente collegato alla gestione del Personale al fine di gestire in automatico le diverse funzioni aziendali (es: nominativi degli approvatori e dei firmatari, determina del Presidente piuttosto che del Dirigente) con evidenza dei diversi attori che intervengono nella gestione e nell'approvazione dell'intero flusso.



Casi di studio – La gestione degli aspetti di sicurezza…

… gestione delle eventuali interruzioni dei flussi operativi del processo

A tutti gli attori del processo viene presentata la lista delle attività in attesa con una classificazione in funzione delle scadenze e dei diversi rouli nell'Ente. La **gestione delle scadenze riduce i rischi di errore e di interruzione dei processi.** E' disponibile un **sistema di notifiche** (mail) e eventuali **alert** (pop up).



Casi di studio – La gestione degli aspetti di sicurezza…

… monitoraggio delle attività

In qualunque momento ciascun attore del flusso può **visionare chi ha agito** sugli step del processo nel quale è coinvolto e conoscere le date di ingresso e uscita da ciascuno step.

Ci sono utenti abilitati alla supervisione di tutti i flussi e il sistema garantisce il controllo sulla versione dei documenti .

Risultato Audit

Descrizione Step	User	Stato Attività	Entrata il	Chiusa il
Stesura RdA	Operatore 1	Chiusa	2014-04-17	2014-04-17
Approvazione Responsabile Rda	Operatore 2	Chiusa	2014-04-17	2014-04-17
Approvazione Dirigente Rda	Operatore 3	Chiusa	2014-04-17	2014-04-17
Istruttoria RdA	Operatore 4	Chiusa	2014-04-17	2014-04-18
Analisi RdA respinta	Operatore 1	Chiusa	2014-04-18	2014-04-29
Istruttoria RdA	Operatore 4	Chiusa	2014-04-29	2014-05-06
Verifica budget Acquisti	Operatore 5	Chiusa	2014-05-06	2014-05-06
Verifica RdA globale	Operatore 6	Chiusa	2014-05-06	2014-05-06
Istruttoria RdA	Operatore 4	Chiusa	2014-05-06	2014-05-06
Verifica RdA globale	Operatore 6	Chiusa	2014-05-06	2014-05-06

Casi di studio – La gestione degli aspetti di sicurezza…

… firma dei documenti

I documenti sono firmati con un **sistema di firma forte** utilizzando un sistema di firma remoto. Operativamente significa inserire un PIN collegato al proprio certificato di firma