ARCHITETTURE DI SISTEMI DOCUMENTALI

21 Marzo 2017

Emanuele Tonelli

L’architettura dell’Unione Reno Galliera e il piano della sicurezza

Emanuele Tonelli

Presentazione

- Responsabile Sistemi Informativi Unione Reno Galliera
- Reno Galliera
  - 8 comuni nel territorio metropolitano di Bologna
  - 73 mila abitanti
  - Servizi in Unione:
    - Personale, Informatica
    - SUAP, Urbanistica, CUC
    - PM, Protezione Civile
    - Servizi alla persona (6 comuni)

Emanuele Tonelli

UNIONE
RENO GALLIERA

Agenda

- L’architettura del sistema documentale dell’Unione Reno Galliera
- La piattaforma DOC-ER e le integrazioni
- Il piano della sicurezza
- Il tema sicurezza come approccio organizzativo
- Rischi attuali e scenari futuri (il Regolamento Europeo)

Emanuele Tonelli

Il contesto in cui operiamo

- Omogeneizzazione degli strumenti applicativi (2011-2012)
- Nuove competenze archivistiche (orientate al digitale da acquisire)
- La scelta doc-er
- La revisione del Manuale di Gestione del Protocollo (2015)

Emanuele Tonelli

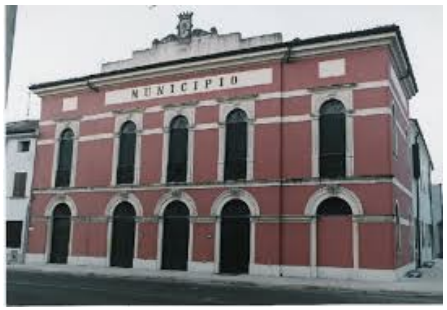
Il mondo DOC-ER

SUAP / SUE

DEMOGRAFICI

TRIBUTI

ATTI AMM.



Emanuele Tonelli

ISTANZE

SIEDER

DOC-ER

PARER

Sistema Documentale

Sistema di PROTOCOLLO

La scelta DOC-ER

- Una maggiore correttezza archivistica
- La relazione tra il protocollo e altri sistemi
- Un occhio alla sicurezza e alla riservatezza dei dati
  - Prima del 2013 avevamo livello di accesso meno controllati
  - I livelli di accesso definiti nel protocollo sono gli stessi che si hanno con le applicazioni terze (pianta organica condivisa)

Emanuele Tonelli

Il piano della sicurezza

- Occasione: il gruppo di lavoro dedicato al rifacimento del Manuale
- Opportunità oltre che obbligo
- Piano della sicurezza Sistema di Conservazione
- Piano di sicurezza del sistema di gestione informatica dei documenti
- Piano della Sicurezza Generale
- Piano della sicurezza è obbligo del responsabile del Protocollo (Gestione documentale), art. 4 co. 1 lett. C Regole Tecniche

DPCM 3 dic. 2013 Regole tecniche, art. 7 Requisiti minimi di sicurezza dei sistemi di protocollo informatico

- 1. Il sistema di protocollo informatico assicura:
  - a) l'univoca identificazione ed autenticazione degli utenti;
  - b) la protezione delle informazioni relative a ciascun utente nei confronti degli altri;
  - c)la garanzia di accesso alle risorse esclusivamente agli utenti abilitati;
  - d) la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantirne l'identificazione.
- 2. Il sistema di protocollo informatico deve consentire il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppo di utenti.
- 3. Il sistema di protocollo informatico deve consentire il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore.
- 4. Le registrazioni di cui ai commi 1, lettera d), e 3 devono essere protette da modifiche non autorizzate.
- 5. Il registro giornaliero di protocollo è trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto.
- 6. Il sistema di protocollo rispetta le misure di sicurezza previste dagli articoli da 31 a 36 e dal disciplinare tecnico di cui all'allegato B del Codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196.

La Struttura del piano

- Redazione di un piano di sicurezza, non solo limitato al protocollo e al sistema documentale
- Piano di sicurezza del sistema di conservazione → PARER
- Le risorse da difendere:
  - Corretta individuazione delle banche dati
- L'analisi dei rischi
- Le misure di sicurezza da attivare
- Privilegiare l'aspetto organizzativo

L’analisi dei rischi

- **Disponibilità**: Le risorse computazionali devono essere sempre disponibili
  - Guasto hardware; Eventi calamitosi
  - Virus, ransomware o altri codici maligni
  - Attacchi mirati; Errori degli operatori
- **Riservatezza**: Le informazioni devono essere accessibili solo alle entità autorizzate
- **Integrità**: Le risorse e le informazioni devono poter essere sempre considerate autentiche

Emanuele Tonelli

Uno scenario preoccupante

- A partire dal 2014, si sono diffusi i ransomware quali cryptolocker
  - (crittografano i dati per ottenere un riscatto)
- Gli attacchi sono ora rivolti anche alla Pubblica Amministrazione
  - Agenzia USA per il controllo degli impiegati governativi (4 milioni di dipendenti)
  - Dipartimento Funzione Pubblica (2016)
  - Equitalia (2016)

Emanuele Tonelli

Cosa può accadere

- Furto di un portatile con dati troppo aperti
  - Abbiamo crittografato i nostri dati?
- Il vostro Telefono mobile sotto controllo
  - Abbiamo un antivirus per i dispositivi mobili
- Il classico cryptolocker
  - Il ransomware più famoso, ma non l'unico
  - Il rischio PEC

Emanuele Tonelli

Non solo tecnologie…

- Ottenere un indirizzo politico per la sicurezza
- Definire un budget specifico
- Rinforzare il concetto di identità digitale
- Catalogare i dati e classificarli
- Verificare periodicamente le procedure ed effettuare dei test di ripristino
- Formare in modo opportuno gli utenti

Emanuele Tonelli

Alcuni consigli pratici

- Attenzione alle mail
  - Non eseguire gli allegati o i link nelle mail sospette, nel dubbio non agire
- Difendere la propria identità digitale
  - Non cedere la password
  - Disattivare gli utenti che cambiano mansioni o lavoro
  - Definire chi può accedere a che cosa (responsabili del trattamento)
  - Concedere solo gli accessi strettamente necessari per lavorare

Emanuele Tonelli

Le domande da fare

- Chi è il responsabile della sicurezza?
- Avete ricevuto formazione adeguata?
- Qual è il perimetro dei dati che sono protetti?
- Sono stati classificati i dati?
- Quando è stato fatto l'ultimo test di restore?
- Il protocollo di emergenza

Uno sguardo in avanti

- Da maggio 2016 è stato approvato il Regolamento Generale Protezione dei Dati GDPR (Regolamento UE 2016/679)
- 2 anni per adeguarsi
- Privacy by design
- Superato il concetto di misure minime, maggiore responsabilizzazione “Accountability” (il titolare decide quali misure adottare)
- Nomina del Data Protection Officer (obbligatoria per la PA)

Riferimenti

- www.renogalliera.it
- E.tonelli@renogalliera.it
- Twitter: @emanueletonelli
- www.emanueletonelli.it

Emanuele Tonelli