

Sicurezza Documentale

a.a. 2017/2018

DOCENTI: DOTT.SSA VALERIA FIONDA

DOTT. GIUSEPPE PIRRÒ



Organizzazione del corso e modalità d'esame

Calendario Didattico

- I corsi iniziano il 02.10.2017 e terminano il 22.12.2017.
- La sessione invernale di esami va dal 08.01.2018 al 03.03.2018.

Orario delle lezioni

- Martedì 11.00 – 13.00, aula F, cubo 20B, Il piano.
- Venerdì 11.00-13.00, aula F, cubo 20B, Il piano.

- Modulo 1
 - Lezione 0: 03/10/2017
 - Lezione 1: 06/10/2017
 - Lezione 2: 10/10/2017
 - Lezione 3: 13/10/2017
 - Lezione 4: 17/10/2017
 - Lezione 5: 20/10/2017
 - Lezione 6: 31/10/2017
 - Lezione 7: 03/11/2017
 - Lezione 8: 07/11/2017
 - Lezione 9: 10/11/2017
 - Lezione 10: 22/12/2017

Orario delle lezioni

- Modulo 2
 - Lezione 11: 14/11/2017
 - Lezione 12: 17/11/2017
 - Lezione 13: 21/11/2017
 - Lezione 14: 24/11/2017
 - Lezione 15: 28/11/2017
 - Lezione 16: 01/12/2017
 - Lezione 17: 05/12/2017
 - Lezione 18: 12/12/2017
 - Lezione 19: 15/12/2017
 - Lezione 20: 19/12/2017

Informazioni generali


- Ricevimento: ogni lunedì dalle 15 alle 16
- Pagina del corso: www.mat.unical.it/fionda → teaching → Sicurezza Documentale
- Email docenti: fionda@mat.unical.it / valeria.fionda@unical.it
pirro@icar.cnr.it

Programma del corso

Parte Teorica

- Dematerializzazione delle informazioni e sicurezza informatica.
- Tipi di attacchi informatici, misure e sistemi di sicurezza.
- Normativa e Piani di sicurezza
- Formati digitali

Parte Pratica

- Robustezza dei formati dei dati
 - Sistemi di accesso controllato alle informazioni
 - Sicurezza e tutela dei dati
- 

Materiale

- Slides fornite dal docente
- Collegamenti a fonti esterne sotto forma di link

Modalità d'esame

- L'esame consta di:
 1. Esoneri svolti durante le esercitazioni: Esercizi da svolgere durante le lezioni e/o a casa e da consegnare via email;
 2. Un test a risposta multipla sugli argomenti di teoria alla fine del corso.

*Dematerializzazione
delle informazioni e
sicurezza informatica*

La dematerializzazione delle informazioni



La dematerializzazione delle informazioni



La dematerializzazione delle informazioni



La dematerializzazione delle informazioni

De materializzazione



interfacce



leggittimazione



I vantaggi della dematerializzazione

- Risparmio di carta, energia e spazio
- Velocizzazione e semplificazione dell'accesso ai documenti
- Accesso ai documenti svincolato dal luogo fisico
- Forte riduzione dei costi legati al ciclo della stampa
- Semplificazione della gestione e tracciabilità in tempo reale dei documenti
- Riduzione degli errori legati ad una gestione manuale dei processi

Digitalizzazione e dematerializzazione

- Digitalizzazione: IMPATTO TECNOLOGICO
- Dematerializzazione: IMPATTO ORGANIZZATIVO

Il documento Informatico

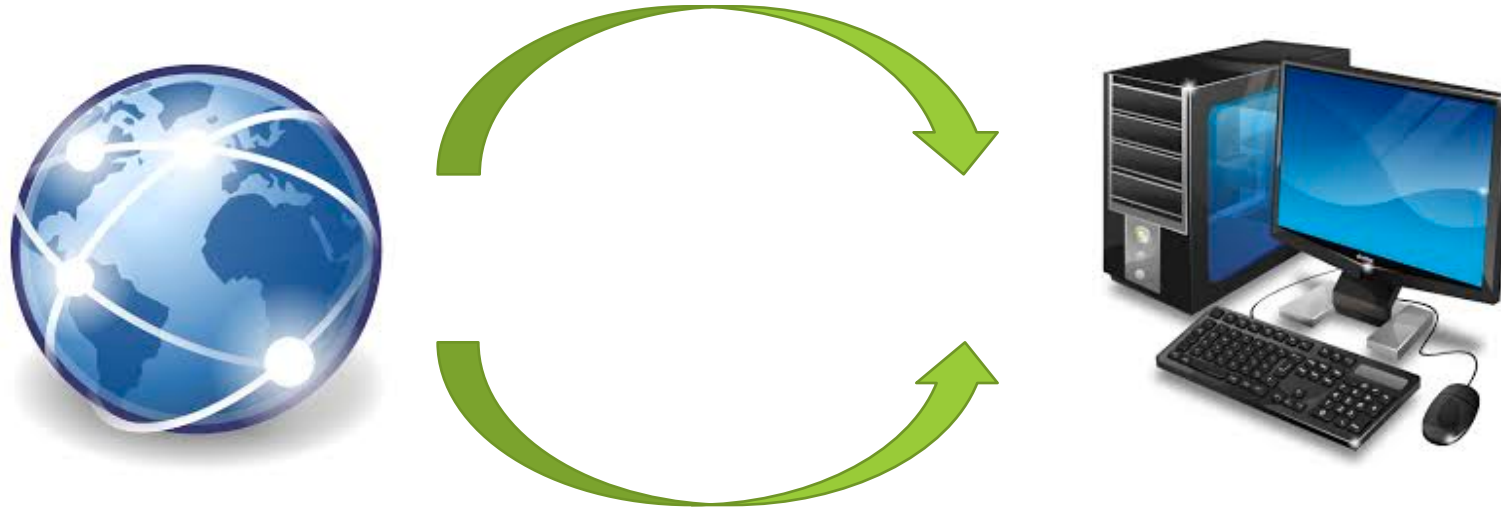
- Il documento ANALOGICO è la rappresentazione NON “digitale”, ovvero NON informatica, degli atti, fatti o dati giuridicamente rilevanti.
- Il documento INFORMATICO è la rappresentazione “digitale”, ovvero informatica, degli atti, fatti o dati giuridicamente rilevanti.

La formazione del documento Informatico

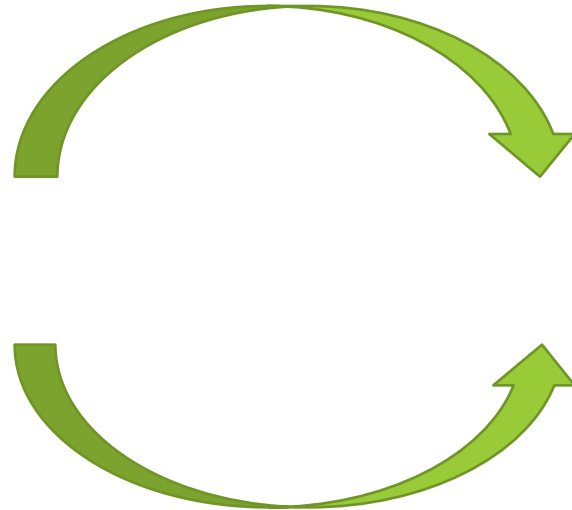
- DOCUMENTI INFORMATICI NATIVI:
Redazione tramite l'utilizzo di appositi strumenti software



Aquisizione di un documento Informatico per via telematica



Aquisizione di un documento Informatico su supporto informatico



Aquisizione di un documento Informatico per copia immagine

- Acquisizione della copia immagine di un documento analogico



Aquisizione di un documento Informatico per registrazione

- Acquisizione da transazioni o processi informatici



Aquisizione di un documento Informatico per registrazione

- Di moduli e formulari compilati dall'utente

PROTEZIONE CIVILE REGIONALE
- Volontariato -
Regione di

Scheda richiesta del Volontario per rilascio tessera di riconoscimento

Organizzazione di Volontariato di appartenenza

Nome _____ Cognome _____

Esige il dato di nascita (gg/mm/aaaa) _____

Indirizzo di residenza (indicare Via, comune, e a.p. e provincia) _____

Numero telefono fisso _____ Numero cellulare _____

Eventuale indirizzo di posta elettronica _____

Codice Fiscale _____ Data di prima iscrizione nell'attuale organizzazione di volontariato _____

Professionista (medico, infermiere ecc. - indicare anche se non occupato o pensionato) _____

Eventuale specializzazione professionale (medico, saldatore ecc.) _____

Nome _____

Modulo da compilare

Nome e Cognome: _____

Indirizzo email: _____

Opzione 1

Domanda

Sì

No

Aquisizione di un documento Informatico per generazione o raggruppamento

- Generazione o raggruppamento, per via automatica, di un insieme di dati provenienti da una o piu basi di dati



Aquisizione di un documento Informatico per generazione o raggruppamento

- Generazione o raggruppamento, per via automatica, di un insieme di dati provenienti da una o piu basi di dati



Cosa significa conservare I documenti informatici



Consentire l'accesso ai dati per fini di ricerca



Proteggere nel tempo gli archivi digitali



Garantire autenticità, integrità, leggibilità e reperibilità dei documenti informatici



Predisporre opportune misure per la qualità e la sicurezza dei sistemi

principio fondamentale

la sicurezza di un sistema informatico è legata

- ... molto al processo con cui un sistema viene gestito
 - pianificazione, analisi dei rischi, gestione dei sistemi, formazione del personale, ecc.
- ... e limitatamente ai prodotti e alle tecnologie utilizzate
 - firewall, antivirus, ecc.

l'importanza degli aspetti tecnologici

la conoscenza della tecnologia è comunque importante per:

- comprendere le vulnerabilità e quindi i rischi
- adottare contromisure che siano...
 - Efficaci
 - Economiche
 - Scalabili
 - Gestibili
 - Usabili

perché curare la sicurezza?

evitare di incorrere in danni economici

- conformità alle leggi (compliance)
 - es. D.Lgs. 196/2003
- il motore principale che muove il mercato della sicurezza è la paura
 - di perdite economiche
 - di non conformità alle leggi vigenti

chi dovrebbe badare alla sicurezza (informatica)?

- Imprese
- pubblica amministrazione ed enti pubblici
- chiunque utilizzi sistemi informatici per scopi economicamente rilevanti
- anche se non a scopo di lucro!
 - l'università (quanto vale il sistema di paghe e stipendi dell'ateneo?)
 - lo studente che scrive la tesi (quanto vale il documento "tesi.doc" il giorno prima della consegna?)

Il manuale di gestione documentale



Piano di sicurezza

- Garantire, monitorare e controllare la sicurezza dei sistemi informativi a supporto del Sistema di Conservazione
- Minimizzare i rischi
- Soddisfare i requisiti relativi alla privacy e alla protezione dei dati personali trattati dall'organizzazione

Piano sicurezza

- Il tema della sicurezza informatica della PA riveste un'importanza fondamentale perché necessaria per garantire la disponibilità, l'integrità e la riservatezza delle informazioni del Sistema informativo della Pubblica amministrazione.
- Essa è inoltre direttamente collegata ai principi di privacy previsti dall'ordinamento giuridico.

Schema piano sicurezza - Agid

Personale responsabile della sicurezza

- Nel manuale è necessario definire quale personale sia dedicato alla sicurezza informatica della conservazione, con le relative responsabilità
 - Responsabile della Sicurezza
 - Responsabile della sicurezza dei sistemi per la conservazione

Procedure di produzione, diffusione e gestione della documentazione di sicurezza

- Le procedure di gestione della documentazione di sicurezza, riguardano le attività legate all'acquisizione, produzione, archiviazione e diffusione del materiale relativo alla Certificazione della Sicurezza delle Informazioni.
- La Gestione Documentale della Sicurezza deve prevedere la produzione di documenti che debbono essere elaborati e pubblicati, in seguito alla fase di analisi dei rischi, dal Responsabile della Conservazione come strumento di condivisione delle procedure di sicurezza al personale.

Procedure per la dismissione o alienazione

- Regolamentazione delle procedure di dismissione o alienazione
 - procedura di cancellazione delle informazioni;
 - procedura di distruzione dei supporti non riscrivibili utilizzati per la memorizzazione delle informazioni;
 - procedura di cancellazione sicura dai supporti riscrivibili utilizzati per la memorizzazione delle informazioni
 - procedura di triturazione di supporti (quali quelli cartacei e analoghi).

Procedure per la continuità operativa

- Descrizione delle misure adottate a garantire la continuità operativa quali ad esempio il disaster recovery, il back up delle informazioni, gli apparati ridondati.
- Rappresentazione del grado di affidabilità mediante indicatori specifici (MTBF - tempo medio fra i guasti, MTTR - Tempo medio di ripristino).

Politiche di Sicurezza

- Procedure per il controllo degli accessi fisici e logici;
- Politica di gestione delle postazioni di lavoro (regole per l'installazione del software sulle postazioni di lavoro, regole per la limitazione della connettività a supporti esterni come ad esempio Pen Drive);
- Politica di gestione dei canali di comunicazione (e.g., quali e-mail, sistemi di instant messaging, VoIP, internet, accessi wireless)

Gestione degli incidenti

- Si definisce “incidente di sicurezza” qualsiasi evento che comprometta o minacci di compromettere il corretto funzionamento dei sistemi e/o delle reti dell’organizzazione o l’integrità e/o la riservatezza delle informazioni in esse memorizzate od in transito, o che violi le politiche di sicurezza definite o le leggi in vigore
- Il processo di gestione degli incidenti è articolato nelle seguenti fasi:
 - rilevazione/identificazione/classificazione
 - contenimento
 - eliminazione
 - ripristino
 - follow-up
- norme ISO/IEC 27001:2013, ISO/IEC 27007 e TR 101 533-02.

Riferimenti Normativi

Codice Civile, articolo 2215 bis - Documentazione informatica

- I libri, i repertori, le scritture e la documentazione la cui tenuta è obbligatoria per disposizione di legge o di regolamento o che sono richiesti dalla natura o dalle dimensioni dell'impresa possono essere formati e tenuti con strumenti informatici.
- I libri, i repertori e le scritture tenuti con strumenti informatici [...] hanno l'efficacia probatoria di cui agli articoli 2709 e 2710 del codice civile.

Riferimenti Normativi

Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 -
Testo Unico delle disposizioni legislative e regolamentari in materia
di documentazione amministrativa

b) DOCUMENTO INFORMATICO la rappresentazione informatica di
atti, fatti o dati giuridicamente rilevanti;

r) SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI l'insieme
delle risorse di calcolo, degli apparati, delle reti di comunicazione e
delle procedure informatiche utilizzati dalle amministrazioni per la
gestione dei documenti;

Riferimenti Normativi

Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 -
Articolo 8

- Il documento informatico da chiunque formato, la registrazione su supporto informatico e la trasmissione con strumenti telematici, sono validi e rilevanti a tutti gli effetti di legge, se conformi alle disposizioni del presente testo unico.
- Le regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici sono definite con decreto del Presidente del Consiglio dei Ministri sentiti l'Autorità per l'informatica nella pubblica amministrazione e il **garante per la protezione dei dati personali**. Esse sono adeguate alle esigenze dettate dall'evoluzione delle conoscenze scientifiche e tecnologiche, con cadenza almeno biennale.
- Con il medesimo decreto del Presidente del Consiglio dei Ministri sono definite le **misure tecniche, organizzative e gestionali volte a garantire l'integrità, la disponibilità e la riservatezza delle informazioni** contenute nel documento informatico

Riferimenti Normativi

Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 -
Articolo 51

- Le pubbliche amministrazioni provvedono a realizzare o revisionare sistemi informativi finalizzati alla totale automazione delle fasi di produzione, gestione, diffusione ed utilizzazione dei propri dati, documenti, procedimenti ed atti in conformità alle disposizioni del presente testo unico ed alle **disposizioni di legge sulla tutela della riservatezza dei dati personali.**

Riferimenti Normativi

Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 -
Articolo 52

- Il sistema di gestione informatica dei documenti, in forma abbreviata "sistema" deve:
 - a) **garantire la sicurezza e l'integrità del sistema;**
 - e) consentire, in **condizioni di sicurezza**, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali;

Riferimenti Normativi

Decreto Legislativo 30 giugno 2003, n. 196

- Codice in materia di protezione dei dati personali (non viene mai usata la parola privacy)
- 186 articoli più 3 allegati e 3 codici di deontologia (77 pagine)
- Disciplinare tecnico in materia di misure minime di sicurezza (password, antivirus, disabilitazione utenti, disaster recovery ...)
- Diritto alla protezione dei dati personali
- Principio di semplificazione (“niente di più di quello che serve ...”)
- Principio di necessità (“... e solo se è proprio necessario”)
- Trattamento dei dati (non necessariamente elettronico)
- “Dato personale” vs “Dato anonimo”
- Dato giudiziario (Art 4 comma 1 lettera e richiama altri 5 DPR ...)
- Dato sensibile (“idoneo a rivelare razza, politica, sindacato ...”)

Riferimenti Normativi

Decreto Legislativo 30 giugno 2003, n. 196

Articolo 1

- Chiunque ha diritto alla **protezione** dei dati personali che lo riguardano.

Articolo 3

- I sistemi informativi e i programmi informatici sono configurati **riducendo al minimo l'utilizzazione di dati personali e di dati identificativi**, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità

Riferimenti Normativi

Decreto Legislativo 30 giugno 2003, n. 196

Articolo 31

- I dati personali oggetto di trattamento sono **custoditi e controllati**, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, **in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.**

Articolo 34

- Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate [...] le seguenti **misure minime**:
 - a) autenticazione informatica;
 - b) adozione di procedure di gestione delle credenziali di autenticazione;
 - c) utilizzazione di un sistema di autorizzazione;
 - d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
 - e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
 - f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
 - g) [soppressa] (1);
 - h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

Riferimenti Normativi

Decreto Legislativo 7 marzo 2005 n. 82

Articolo 14-bis

- L'Agenzia per l'Italia Digitale (AgID) è preposta alla realizzazione degli obiettivi dell'Agenda Digitale Italiana, in coerenza con gli indirizzi dettati dal Presidente del Consiglio dei ministri o dal Ministro delegato, e con l'Agenda digitale europea. AgID, in particolare, promuove l'innovazione digitale nel Paese e l'utilizzo delle tecnologie digitali nell'organizzazione della pubblica amministrazione e nel rapporto tra questa, i cittadini e le imprese, nel rispetto dei principi di legalità, imparzialità e trasparenza e secondo criteri di efficienza, economicità ed efficacia. Essa presta la propria collaborazione alle istituzioni dell'Unione europea e svolge i compiti necessari per l'adempimento degli obblighi internazionali assunti dallo Stato nelle materie di competenza.
- AgID svolge le funzioni di:
 - a) emanazione di regole, standard e guide tecniche, nonché di vigilanza e controllo sul rispetto delle norme di cui al presente Codice, anche attraverso l'adozione di atti amministrativi generali, in materia di agenda digitale, digitalizzazione della pubblica amministrazione, **sicurezza informatica**, interoperabilità e cooperazione applicativa tra sistemi informatici pubblici e quelli dell'Unione europea;

[...]

Riferimenti Normativi

Decreto Legislativo 7 marzo 2005 n. 82

Articolo 44

- Il sistema di gestione informatica e conservazione dei documenti informatici della pubblica amministrazione assicura.
 - a) **l'identificazione** certa del soggetto che ha formato il documento e dell'amministrazione o dell'area organizzativa omogenea di riferimento di cui all'articolo 50, comma 4, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445;
 - b) la **sicurezza e l'integrità** del sistema e dei dati e documenti presenti;
 - f) **l'accesso, in condizioni di sicurezza**, alle informazioni del sistema, nel rispetto delle disposizioni in materia di **tutela dei dati personali**;
 - i) l'accesso remoto, in **condizioni di sicurezza**, ai documenti e alle relative informazioni di registrazione **tramite un identificativo univoco**;

Riferimenti Normativi

Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 -
Regole tecniche in materia di sistema di conservazione ai sensi del
Decreto Legislativo n. 82 del 2005;

Art 7

- 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.
- Il sistema di protocollo informatico deve consentire il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppo di utenti.
- Il sistema di protocollo informatico deve consentire il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore.

obiettivi della sicurezza

- confidenzialità o riservatezza o segretezza
 - dati letti solo da chi è “autorizzato”
- Integrità
 - dei dati: i dati non sono stati modificati in maniera incontrollata
 - dell'origine: l'origine dei dati è certa
 - dei sistemi: non compromissione
- Disponibilità
 - dati o servizi sono disponibili per accesso/uso