



*Permanent Education and Knowledge on  
Information Technology Project*



## **CERTIFICAZIONI INFORMATICHE**

*Aut. Ministero dell'Istruzione,  
Università e Ricerca prot.  
A00DGPERS 6235 del 25/06/2010*





# ***Sommario***

<b>Fase 1 - REGOLE GENERALI DI PROTEZIONE DEI DATI.....</b>	<b>3</b>
<b>Fase 2 - RESPONSABILITA' .....</b>	<b>8</b>
<b>Fase 3 - TECNICHE PER GARANTIRE IL RISPETTO DEL REGOLAMENTO DI PROTEZIONE DI DATI .....</b>	<b>14</b>

# Fase 1 - REGOLE GENERALI DI PROTEZIONE DEI DATI

## **1.1. Contesto normativo**

- 1.1.1. Cenni al concetto di privacy e protezione dei dati in Europa.
  - 1.1.1.1. Protezione dei dati in Italia.
- 1.1.2. Standard e buone pratiche.

## **1.2. La normativa italiana/europea (Reg. EU. 679/2016) sulla protezione dei dati: fondamenti.**

- 1.2.1. Ambito di applicazione
  - 1.2.1.1. Soggettivo
  - 1.2.1.2. Oggettivo
  - 1.2.1.3. Esclusioni
- 1.2.2. Definizioni.
- 1.2.3. Soggetti obbligati.
- 1.2.4. Soggetti non obbligati

## **1.3. La normativa italiana/europea (Reg. EU. 679/2016) sulla protezione dei dati: principi**

- 1.3.1. Il binomio diritto / dovere nella protezione di dati.
- 1.3.2. Legittimità del trattamento
- 1.3.3. Lealtà e trasparenza
- 1.3.4. Limitazione delle finalità
- 1.3.5. Minimizzazione di dati
- 1.3.6. Esattezza dei dati

## **1.4. La normativa italiana/europea (Reg. EU. 679/2016) sulla protezione dei dati: legittimazione**

- 1.4.1. Raccolta dei dati
  - 1.4.1.1. Presso interessato
  - 1.4.1.2. Non presso interessato
- 1.4.2. Informativa
  - 1.4.2.1. Contenuto

- 1.4.3. Consenso
  - 1.4.3.1. Forma del consenso
    - 1.4.3.1.1. Concessione
    - 1.4.3.1.2. Revoca.
  - 1.4.3.2. Consenso dei minori.
- 1.4.4. Consenso informato:
  - 1.4.4.1. Scopo
  - 1.4.4.2. Trasparenza
  - 1.4.4.3. Conservazione
  - 1.4.4.4. Informazione
  - 1.4.4.5. obbligo di comunicazione agli interessati.
- 1.4.5. Categorie speciali di dati.
  - 1.4.5.1. Dati relativi a infrazioni e condanne penali.
  - 1.4.5.2. Dati "medici"
    - 1.4.5.2.1. Dati genetici
    - 1.4.5.2.2. Dati biometrici
    - 1.4.5.2.3. Dati relativi alla salute
  - 1.4.5.3. Trattamento che non richiede identificazione.
  - 1.4.5.4. Basi legali diverse dal consenso.

### **1.5. Diritti degli interessati.**

- 1.5.1. Trasparenza e informazione
- 1.5.2. Accesso, rettifica, cancellazione.
- 1.5.3. Opposizione
- 1.5.4. Limitazioni del trattamento.
- 1.5.5. Decisioni individuali automatizzate.
- 1.5.6. Profilazione
- 1.5.7. Portabilità.
- 1.5.8. Eccezioni ai diritti.

### **1.6. La normativa italiana/europea (Reg. EU. 679/2016) sulla protezione dei dati: misure di conformità.**

- 1.6.1. Le politiche di protezione dei dati.
- 1.6.2. Posizione legale degli intervenienti.
  - 1.6.2.1. Titolare
  - 1.6.2.2. Co-titolare
  - 1.6.2.3. Responsabile
  - 1.6.2.4. Co-responsabile
  - 1.6.2.5. Incaricato del trattamento e suoi rappresentanti.
    - 1.6.2.5.1. Rapporti tra i soggetti e formalizzazione.
    - 1.6.2.5.2. La matrice poteri / doveri dell'incaricato del trattamento
      - 1.6.2.5.2.1. Corrispondenza tra poteri su:

- 1.6.2.5.2.1.1. Documenti cartacei
- 1.6.2.5.2.1.2. Documenti informatici
- 1.6.3. Il registro delle attività di trattamento:
  - 1.6.3.1. identificazione dei trattamenti dei dati.
  - 1.6.3.2. classificazione dei trattamenti dei dati.

### **1.7. La normativa italiana/europea (Reg. EU. 679/2016) sulla protezione dei dati: responsabilità proattiva**

- 1.7.1. Privacy by design e impostazioni predefinite.
- 1.7.2. Valutazione dell'impatto riguardante la protezione dei dati
  - 1.7.2.1. la consultazione preventiva.
  - 1.7.2.2. Trattamenti ad alto rischio.
- 1.7.3. Sicurezza dei dati personali.
  - 1.7.3.1. Sicurezza tecnica
  - 1.7.3.2. Sicurezza organizzativa.
  - 1.7.3.3. Sicurezza fisica
- 1.7.4. Le violazioni della sicurezza.
  - 1.7.4.1. Notifica di violazioni all'autorità.
  - 1.7.4.2. Notifica di violazioni all'interessato
- 1.7.5. Il responsabile della protezione dei dati (RPD/DPO). Contesto normativo.
- 1.7.6. Codici di condotta e certificazioni. Cenni

### **1.8. Il regolamento europeo sulla protezione dei dati. Responsabile Protezione Dati (RPD, DPO o Data Protection Officer).**

- 1.8.1. Designazione.
  - 1.8.1.1. Processo decisionale.
  - 1.8.1.2. Analisi del possibile conflitto di interesse.
  - 1.8.1.3. Formalità nella scelta, rinnovo e cessazione.
- 1.8.2. Competenza professionale.
  - 1.8.2.1. Negoziazione.
  - 1.8.2.2. Comunicazione.
  - 1.8.2.3. Il budget.
  - 1.8.2.4. Formazione.
  - 1.8.2.5. Capacità personali, lavoro di squadra, leadership, gestione delle attrezzature.
- 1.8.3. Obblighi e responsabilità.
  - 1.8.3.1. Indipendenza.
  - 1.8.3.2. Identificazione.
    - 1.8.3.2.1. Collaborazione
    - 1.8.3.2.2. Autorizzazioni preventive
    - 1.8.3.2.3. Rapporti con le parti interessate
    - 1.8.3.2.4. Gestione dei reclami.
    - 1.8.3.2.5. Comunicazione con l'autorità di protezione dei dati.

1.8.3.3. Procedure.

**1.9. La normativa italiana/europea (Reg. EU. 679/2016) sulla protezione dei dati e l'aggiornamento della Privacy. Trasferimenti internazionali di dati**

- 1.9.1. Il sistema decisionale di adeguatezza.
- 1.9.2. Trasferimenti tramite garanzie appropriate.
- 1.9.3. Regole aziendali
  - 1.9.3.1. Eccezioni.
- 1.9.4. Clausole contrattuali
- 1.9.5. Norme d'impresa
  - 1.9.5.1. Binding Corporate Rules
- 1.9.6. Autorizzazione dell'autorità di controllo.
- 1.9.7. Sospensione temporanea

**1.10. La normativa italiana/europea (Reg. EU. 679/2016) sulla protezione dei dati: le autorità di controllo.**

- 1.10.1. Autorità di Controllo (italiana).
  - 1.10.1.1. Dignità.
  - 1.10.1.2. Sanzioni.
- 1.10.2. Comitato europeo per la protezione di Dati.
- 1.10.3. La tutela dell'interessato
  - 1.10.4. Procedure di competenza del garante.
  - 1.10.5. La tutela giurisdizionale.
  - 1.10.6. Il diritto di indennizzo.

**1.11. Linee guida per l'interpretazione del Regolamento Generale sulla Protezione dei Dati (RGPD).**

- 1.11.1. Articolo 29 dell'EU RGPD.
  - 1.11.1.1. Pareri del Comitato europeo per la protezione di dati
- 1.11.2. Criteri degli organi di giurisdizione.
- 1.11.3. Valore giuridico dei pareri espressi

**1.12. Alcuni soggetti e settori produttivi interessati dalle procedure di protezione dati.**

- 1.12.1. Sanitario, Farmaceutico, Investigativo.
- 1.12.2. Protezione dei minori
- 1.12.3. Solvibilità patrimoniale
- 1.12.4. Telecomunicazioni
- 1.12.5. Videosorveglianza
- 1.12.6. Assicurazione
- 1.12.7. Pubblicità, ecc.
- 1.12.8. Altro....

**1.13. Legislazione italiana sulla privacy con implicazioni sulla la protezione di dati.**

1.13.1. Codice per la protezione dei dati – Decreto legislativo n. 196 del 30/06/2003

**1.14. Regolamento europeo con implicazioni sulla la protezione di dati.**

1.14.1. Direttiva E-Privacy: Direttiva 2002/58 / CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva sulla privacy e comunicazioni elettroniche) o Regolamento e-Privacy quando approvato.

1.14.2. Direttiva 2009/136 / CE del Parlamento europeo e del Consiglio, del 25 novembre 2009, che modifica la direttiva 2002/22 / CE relativa al servizio universale e ai diritti degli utenti in relazione a reti e servizi delle comunicazioni elettroniche, la direttiva 2002/58 / CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e il regolamento (CE) n. 2006/2004 sulla cooperazione nel settore delle comunicazioni elettroniche il consumatori.

1.14.3. Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, l'accertamento o il perseguimento di reati o l'esecuzione di sanzioni penali e la libera circolazione di tali dati e che abroga la decisione quadro 2008/977 / GAI del Consiglio.

# Fase 2 - RESPONSABILITA'

## **2.1. Analisi e gestione dei rischi legati al trattamento dei dati personali.**

- 2.1.1. Introduzione.
  - 2.1.1.1. Quadro generale per la valutazione e la gestione del rischio.
  - 2.1.1.2. Concetti generali.
- 2.1.2. Valutazione del rischio.
  - 2.1.2.1. Inventario e valutazione delle attività.
  - 2.1.2.2. Inventario e valutazione delle minacce.
  - 2.1.2.3. Tutele esistenti
  - 2.1.2.4. Valutazione della loro protezione.
  - 2.1.2.5. Rischio risultante.
- 2.1.3. Gestione del rischio.
  - 2.1.3.1. Concetti.
  - 2.1.3.2. Attuazione.
  - 2.1.3.3. Selezione e assegnazione di salvaguardie alle minacce.
  - 2.1.3.4. Valutazione della protezione.
  - 2.1.3.5. Rischio residuo
    - 2.1.3.5.1. Rischio accettabile
    - 2.1.3.5.2. Rischio non assumibile.

## **2.2. Metodologie per l'analisi e la gestione dei rischi.**

### **2.2.1. Applicazione schema Iso 29151**

- 2.2.1.1. 29151-A.3.1 Consenso (raccolta)
- 2.2.1.2. 29151-A.3.2 Scelta e diritto di opposizione
- 2.2.1.3. 29151-A.3.2-ADD Consenso (gestione)
- 2.2.1.4. 29151-A.4.1 Legittimità delle finalità
- 2.2.1.5. 29151-A.4.2 Specifica delle finalità
- 2.2.1.6. 29151-A.5 Limitazione della raccolta dei dati
- 2.2.1.7. 29151-A.6 Minimizzazione dei dati
- 2.2.1.8. 29151-A.7.1 Limitazione dell'uso, conservazione (oblio) e divulgazione
- 2.2.1.9. 29151-A.7.2 Cancellazione sicura
- 2.2.1.10. 29151-A.7.3 Notifica della divulgazione e delle violazioni (data breach)
- 2.2.1.11. 29151-A.7.4 Registrazione della divulgazione
- 2.2.1.12. 29151-A.7.5 Registrazione dei fornitori
- 2.2.1.13. 29151-A.8 Accuratezza e qualità
- 2.2.1.14. 29151-A.9.1 Informativa



- 2.2.1.15. 29151-A.9.2 Apertura e trasparenza
- 2.2.1.16. 29151-A.10.1 Accesso ai dati da parte dell'interessato
- 2.2.1.17. 29151-A.10.2 Diritto di rettifica
- 2.2.1.18. 29151-A.10.3 Gestione dei reclaim
- 2.2.1.19. 29151-A.11.1 Governo (e DPO)
- 2.2.1.20. 29151-A.11.2 Privacy impact assessment
- 2.2.1.21. 29151-A.11.3-ADD Rapporti con i clienti (titolari e super-fornitori)
- 2.2.1.22. 29151-A.11.3 Requisiti per i fornitori
- 2.2.1.23. 29151-A.11.4 Monitoraggio e audit
- 2.2.1.24. 29151-A.11.5 Sensibilizzazione e formazione
- 2.2.1.25. 29151-A.11.6 Reporting
- 2.2.1.26. 29151-A.12 Sicurezza e autorizzazioni
- 2.2.1.27. 29151-A.13.1 Conformità
- 2.2.1.28. 29151-A.13.2 Trasferimenti extra-UE

## **2.2.2. Applicazione schema Iso 27001**

- 2.2.2.1. 27001 - A.05.01.01 Politiche per la sicurezza delle informazioni
- 2.2.2.2. 27001 - A.05.01.02 Riesame delle politiche per la sicurezza delle informazioni
- 2.2.2.3. 27001 - A.06.01.01 Ruoli e responsabilità per la sicurezza delle informazioni
- 2.2.2.4. 27001 - A.06.01.02 Separazione dei compiti
- 2.2.2.5. 27001 - A.06.01.03 Contatti con le autorità
- 2.2.2.6. 27001 - A.06.01.04 Contatti con gruppi specialistici
- 2.2.2.7. 27001 - A.06.01.05 Sicurezza delle informazioni nella gestione dei progetti
- 2.2.2.8. 27001 - A.06.02.01 Politica per i dispositivi portatili
- 2.2.2.9. 27001 - A.06.02.02 Telelavoro
- 2.2.2.10. 27001 - A.07.01.01 Screening
- 2.2.2.11. 27001 - A.07.01.02 Termini e condizioni di impiego
- 2.2.2.12. 27001 - A.07.02.01 Responsabilità della direzione
- 2.2.2.13. 27001 - A.07.02.02 Consapevolezza, istruzione, formazione e addestramento sulla sicurezza delle informazioni
- 2.2.2.14. 27001 - A.07.02.03 Processo disciplinare
- 2.2.2.15. 27001 - A.07.03.01 Cessazione o variazione delle responsabilità durante il rapporto di lavoro
- 2.2.2.16. 27001 - A.08.01.01 Inventario degli asset
- 2.2.2.17. 27001 - A.08.01.02 Responsabilità degli asset
- 2.2.2.18. 27001 - A.08.01.03 Utilizzo accettabile degli asset
- 2.2.2.19. 27001 - A.08.01.04 Restituzione degli asset
- 2.2.2.20. 27001 - A.08.02.01 Classificazione delle informazioni
- 2.2.2.21. 27001 - A.08.02.02 Etichettatura delle informazioni
- 2.2.2.22. 27001 - A.08.02.03 Trattamento degli asset
- 2.2.2.23. 27001 - A.08.03.01 Gestione dei supporti rimovibili

- 2.2.2.24. 27001 - A.08.03.02 Dismissione dei supporti
- 2.2.2.25. 27001 - A.08.03.03 Trasporto dei supporti fisici
- 2.2.2.26. 27001 - A.09.01.01 Politica di controllo degli accessi
- 2.2.2.27. 27001 - A.09.01.02 Accesso alle reti e ai servizi di rete
- 2.2.2.28. 27001 - A.09.02.01 Registrazione e de-registrazione degli utenti
- 2.2.2.29. 27001 - A.09.02.02 Provisioning degli accessi degli utenti
- 2.2.2.30. 27001 - A.09.02.03 Gestione dei diritti di accesso privilegiato
- 2.2.2.31. 27001 - A.09.02.04 Gestione delle informazioni segrete di autenticazione degli utenti
- 2.2.2.32. 27001 - A.09.02.05 Riesame dei diritti di accesso degli utenti
- 2.2.2.33. 27001 - A.09.02.6 Rimozione o adattamento dei diritti di accesso
- 2.2.2.34. 27001 - A.09.03.01 Utilizzo delle informazioni segrete di autenticazione
- 2.2.2.35. 27001 - A.09.04.01 Limitazione dell'accesso alle informazioni
- 2.2.2.36. 27001 - A.09.04.02 Procedure di log-on sicure
- 2.2.2.37. 27001 - A.09.04.03 Sistema di gestione delle password
- 2.2.2.38. 27001 - A.09.04.04 Uso di programmi di utilità privilegiati
- 2.2.2.39. 27001 - A.09.04.05 Controllo degli accessi al codice sorgente dei programmi
- 2.2.2.40. 27001 - A.10.01.01 Politica sull'uso dei controlli crittografici
- 2.2.2.41. 27001 - A.10.01.02 Gestione delle chiavi
- 2.2.2.42. 27001 - A.11.01.01 Perimetro di sicurezza fisica
- 2.2.2.43. 27001 - A.11.01.02 Controlli di accesso fisico
- 2.2.2.44. 27001 - A.11.01.03 Rendere sicuri uffici, locali e strutture
- 2.2.2.45. 27001 - A.11.01.04 Protezione contro minacce esterne ed ambientali
- 2.2.2.46. 27001 - A.11.01.05 Lavoro in aree sicure
- 2.2.2.47. 27001 - A.11.01.6 Aree di carico e scarico
- 2.2.2.48. 27001 - A.11.02.01 Disposizione delle apparecchiature e loro protezione
- 2.2.2.49. 27001 - A.11.02.02 Infrastrutture di support
- 2.2.2.50. 27001 - A.11.02.03 Sicurezza dei cablaggi
- 2.2.2.51. 27001 - A.11.02.04 Manutenzione delle apparecchiature
- 2.2.2.52. 27001 - A.11.02.05 Trasferimento degli asset
- 2.2.2.53. 27001 - A.11.02.06 Sicurezza delle apparecchiature e degli asset all'esterno delle sedi
- 2.2.2.54. 27001 - A.11.02.07 Dismissione sicura o riutilizzo delle apparecchiature
- 2.2.2.55. 27001 - A.11.02.08 Apparecchiature incustodite degli utenti
- 2.2.2.56. 27001 - A.11.02.09 Politica di schermo e scrivania puliti
- 2.2.2.57. 27001 - A.12.01.01 Procedure operative documentate
- 2.2.2.58. 27001 - A.12.01.02 Gestione dei cambiamenti (sistemistici)
- 2.2.2.59. 27001 - A.12.01.03 Gestione della capacità
- 2.2.2.60. 27001 - A.12.01.04 Separazione degli ambienti di sviluppo, test e produzione
- 2.2.2.61. 27001 - A.12.02.01 Controlli contro il malware
- 2.2.2.62. 27001 - A.12.03.01 Backup delle informazioni
- 2.2.2.63. 27001 - A.12.04.01 Raccolta di lg degli eventi (e monitoraggio)

- 2.2.2.64. 27001 - A.12.04.02 Protezione delle informazioni di log
- 2.2.2.65. 27001 - A.12.04.03 Log di amministratori e operatori
- 2.2.2.66. 27001 - A.12.04.04 Sincronizzazione degli orologi
- 2.2.2.67. 27001 - A.12.05.01 Installazione del software sui sistemi di produzione
- 2.2.2.68. 27001 - A.12.06.01 Gestione delle vulnerabilità tecniche
- 2.2.2.69. 27001 - A.12.06.02 Limitazioni all'installazione del software
- 2.2.2.70. 27001 - A.12.07.01 Controlli per l'audit dei sistemi informative
- 2.2.2.71. 27001 - A.13.01.01 Controlli di rete
- 2.2.2.72. 27001 - A.13.01.02 Sicurezza dei servizi di rete
- 2.2.2.73. 27001 - A.13.01.03 Segregazione nelle reti
- 2.2.2.74. 27001 - A.13.02.01 Politiche e procedure per il trasferimento delle informazioni
- 2.2.2.75. 27001 - A.13.02.02 Accordi per il trasferimento delle informazioni
- 2.2.2.76. 27001 - A.13.02.03 Messaggistica elettronica
- 2.2.2.77. 27001 - A.13.02.04 Accordi di riservatezza o di non divulgazione
- 2.2.2.78. 27001 - A.14.01.01 Analisi e specifica dei requisiti per la sicurezza delle informazioni
- 2.2.2.79. 27001 - A.14.01.02 Sicurezza dei servizi applicativi su reti pubbliche
- 2.2.2.80. 27001 - A.14.01.03 Protezione delle transazioni dei servizi applicative
- 2.2.2.81. 27001 - A.14.02.01 Politica per lo sviluppo sicuro
- 2.2.2.82. 27001 - A.14.02.02 Procedure per il controllo dei cambiamenti di Sistema
- 2.2.2.83. 27001 - A.14.02.03 Riesame tecnico delle applicazioni in seguito a cambiamenti nelle piattaforme operative
- 2.2.2.84. 27001 - A.14.02.04 Limitazioni ai cambiamenti dei pacchetti software
- 2.2.2.85. 27001 - A.14.02.05 Principi per l'ingegnerizzazione sicura dei sistemi
- 2.2.2.86. 27001 - A.14.02.06 Ambiente di sviluppo sicuro
- 2.2.2.87. 27001 - A.14.02.07 Sviluppo affidato all'esterno
- 2.2.2.88. 27001 - A.14.02.08 Test di sicurezza dei sistemi
- 2.2.2.89. 27001 - A.14.02.09 Test di accettazione dei sistemi
- 2.2.2.90. 27001 - A.14.03.01 Protezione dei dati di test
- 2.2.2.91. 27001 - A.15.01.01 Politica per la sicurezza delle informazioni nei rapporti con i fornitori
- 2.2.2.92. 27001 - A.15.01.02 Indirizzare la sicurezza all'interno degli accordi con i fornitori
- 2.2.2.93. 27001 - A.15.01.03 Filiera di fornitura per l'ICT (Information and communication technology)
- 2.2.2.94. 27001 - A.15.02.01 Monitoraggio e riesame dei servizi dei fornitori
- 2.2.2.95. 27001 - A.15.02.02 Gestione dei cambiamenti ai servizi dei fornitori
- 2.2.2.96. 27001 - A.16.01.01 Gestione degli incidenti: Responsabilità e procedure
- 2.2.2.97. 27001 - A.16.01.02 Segnalazione degli eventi relativi alla sicurezza delle informazioni

- 2.2.2.98. 27001 - A.16.01.03 Segnalazione dei punti di debolezza relativi alla sicurezza delle informazioni
- 2.2.2.99. 27001 - A.16.01.04 Valutazione e decisione sugli eventi relativi alla sicurezza delle informazioni
- 2.2.2.100. 27001 - A.16.01.05 Risposta agli incidenti relativi alla sicurezza delle informazioni
- 2.2.2.101. 27001 - A.16.01.6 Apprendimento dagli incidenti relativi alla sicurezza delle informazioni

### **2.3. Programma di conformità per la protezione dei dati e per la sicurezza nelle organizzazioni.**

- 2.3.1. Il programma di protezione dei dati nel contesto dell'organizzazione.
  - 2.3.1.1. La progettazione
  - 2.3.1.2. l'attuazione
- 2.3.2. Obiettivi del programma di conformità.
- 2.3.3. Il principio di accountability (responsabilizzazione).
  - 2.3.3.1. Culpa in eligendo
  - 2.3.3.2. Culpa in vigilando
    - 2.3.3.2.1. Necessità di poter dimostrare a posteriori di avere correttamente scelto collaboratori
    - 2.3.3.2.2. Necessità di poter dimostrare a posteriori di avere correttamente determinate soluzioni
    - 2.3.3.2.3. Necessità di poter dimostrare a posteriori di avere correttamente scelto fornitori
    - 2.3.3.2.4. Necessità di poter dimostrare a posteriori di avere correttamente impartito idonee istruzioni
    - 2.3.3.2.5. Necessità di poter dimostrare a posteriori di avere correttamente impartito monitorato l'effettiva esecuzione delle istruzioni

### **2.4. Sicurezza delle informazioni.**

- 2.4.1. Quadro normativo.
- 2.4.2. Attuazione della sicurezza delle informazioni.
  - 2.4.2.1. Security by design e per impostazione predefinita.
  - 2.4.2.2. Il ciclo di vita dei sistemi informativi.
  - 2.4.2.3. Integrazione della sicurezza e della privacy nel ciclo di vita.
  - 2.4.2.4. Il controllo di qualità della IS.

### **2.5. Valutazione dell'impatto della protezione dei dati "Data Protection Impact Assessment - DPIA".**

- 2.5.1. Introduzione e fondamenti dell'DPIA: origine, concetto e caratteristiche dell'DPIA.
  - 2.5.1.1. Portata e necessità.
  - 2.5.1.2. Standard.

2.5.2. Esecuzione di una valutazione d'impatto.

2.5.2.1. Aspetti preparatori e organizzativi

2.5.2.2. Analisi della necessità di effettuare la valutazione e le consultazioni precedente.

# Fase 3 - TECNICHE PER GARANTIRE IL RISPETTO DEL REGOLAMENTO DI PROTEZIONE DI DATI

## **3.1. Il controllo della protezione dei dati.**

- 3.1.1. Il processo di audit.
  - 3.1.1.1. Domande generali e approccio alla verifica.
  - 3.1.1.2. Caratteristiche di base dell'Audit.
- 3.1.2. Preparazione del rapporto di audit.
  - 3.1.2.1. Granularità del rapporto di audit
- 3.1.3. Aspetti di base e importanza del rapporto di audit.
  - 3.1.3.1. Esecuzione audit
    - 3.1.3.1.1. follow-up
    - 3.1.3.1.2. azioni correttive.

## **3.2. Audit dei sistemi Informativi.**

- 3.2.1. Il ruolo dell'auditing nei sistemi informativi.
  - 3.2.1.1. Concetti di base.
  - 3.2.1.2. Standard e linee guida di audit IS.
- 3.2.2. Controllo interno e miglioramento continuo.
- 3.2.3. Buone pratiche.
- 3.2.4. Integrazione dell'audit di protezione dei dati nella revisione di IS.
- 3.2.5. Pianificazione
- 3.2.6. Esecuzione
  - 3.2.6.1.1. Follow-up
  - 3.2.6.1.2. azioni correttive.

## **3.3. La gestione della sicurezza dei trattamenti.**

- 3.3.1. Sistema di sicurezza nazionale, ISO / IEC 27001: 2013 (UNE ISO / IEC 27001: 2014: [Iso 29151](#), requisiti per i sistemi di gestione della sicurezza delle informazioni, ISMS).
- 3.3.2. Gestione della sicurezza delle attività.
  - 3.3.2.1. Sicurezza logica
  - 3.3.2.2. Sicurezza procedurale.

- 3.3.2.3. Sicurezza fisica
- 3.3.2.4. Sicurezza applicata a IT
- 3.3.2.5. Documentazione.
- 3.3.3. Disaster Recovery
- 3.3.4. Business Continuity.
- 3.3.5. Pianificazione e gestione del recupero dei disastri.
- 3.3.6. Protezione dei beni tecnici
- 3.3.7. Protezione dei beni documentari.

### **3.4. Altre nozioni.**

- 3.4.1. Il cloud computing.
- 3.4.2. Gli Smartphone.
- 3.4.3. Social network
- 3.4.4. Big data ed elaborazione dei profili.
- 3.4.5. Internet delle cose (IoT).
- 3.4.6. Tecnologie di monitoraggio utente
- 3.4.7. Blockchain e sviluppi tecnologici