CYBER
SICURO

Repubblica e Cantone Ticino

La nuova legge federale sulla protezione dei dati (LPD)

Genesi, sfide e opportunità

Lugano, 14 ottobre 2021

Repubblica e Cantone Ticino

CYBER SICURO

Repubblica e Cantone Ticino

Introduzione

Dr. Alessandro Trivilini

Responsabile del Servizio informatica forense del Dipartimento tecnologie innovative, SUPSI
Membro Gruppo «Cyber sicuro»

Repubblica e Cantone Ticino

Norman Gobbi

Consigliere di Stato e Direttore del Dipartimento delle istituzioni

Dipartimento delle istituzioni

Cyber sicuro: breve introduzione

Campagna di prevenzione presentata il 21 febbraio 2020

Punto di riferimento e di contatto cantonale per il Consiglio di Stato, gli enti pubblici, le aziende, la popolazione, le associazioni di categoria e i media per tutte le questioni concernenti la sicurezza informatica

Tra i suoi obiettivi:

1. **Informare sui rischi legati all'uso di strumenti e dispositivi informatici**
2. **Attività di alfabetizzazione digitale**
3. **Promuovere la conoscenza e la consapevolezza della dimensione «cyber»**

I dati personali: definizione

Cosa è un dato personale?

La nuova Legge federale sulla protezione dei dati personali (nLPD) stabilisce che i dati personali sono quelle informazioni che **identificano direttamente o indirettamente una persona fisica**, anche combinate tra loro.

I dati personali: un bene individuale da tutelare

- Nella popolazione è riscontrabile una certa **sfiducia** riguardo all'uso che aziende, organizzazioni ed enti pubblici potrebbero fare dei dati personali

- **Ai cittadini vanno date le garanzie necessarie affinché possano usare le tecnologie digitali in totale fiducia e serenità**

- Momenti come quello odierno sono essenziali per migliorare la conoscenza delle tecnologie che usiamo quotidianamente e delle tutele legali

- **La nLPD possiede tutti gli elementi per costituire una rinnovata fiducia tra gli utenti**

La nLPD: cosa significa per i cittadini?

- La nLPD, analogamente al GPDR europeo, rappresenta la più **grande tutela legale per il cittadino nell'ambito della protezione dei dati**

- **Chi «cede» i dati ha dei diritti, chi li «raccoglie» ha dei doveri**

  - **Coloro che chiederanno i nostri dati personali dovranno garantire sicurezza, trasparenza, proporzionalità e finalità riguardo ai dati raccolti, rispettivamente la modalità di conservazione e di trattamento**

- **Le regole della nLPD valgono per tutti**: aziende, enti pubblici, ecc.

Obiettivi della conferenza

- Permettere a tutti di apprendere i **principi fondamentali della nLPD**
- Informare e sensibilizzare sull'**importanza dei dati personali e il loro corretto trattamento**, guardando anche al principio del «consenso» personale
- Incrementare la consapevolezza sulla **centralità della sicurezza informatica**
- Fornire gli spunti utili a una prima valutazione su cosa occorre fare per **non farsi trovare impreparati al momento dell'entrata in vigore della legge**

Repubblica e Cantone Ticino

Christian Vitta

Consigliere di Stato e Direttore del Dipartimento delle finanze e dell’economia

Dipartimento delle finanze e dell’economia

Intervento (video) del Consigliere di Stato Christian Vitta

Repubblica e Cantone Ticino

Dr. Daniel Dzamko-Locher

Responsabile dell'Ambito direzionale Protezione dei dati presso l'Incaricato federale della protezione dei dati e per la trasparenza (IFPDT)

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

L'Incaricato federale della protezione dei dati e della trasparenza (IFPDT)

La nuova legge federale sulla protezione dei dati

Panoramica dal punto di vista dell'IFPDT

Daniel Dzamko-Locher

Capo della unità di direzione della protezione dei dati, IFPDT

Lugano, Giovedì 14 ottobre 2021

Saluto e presentazione dell’IFPDT

- Saluto dell’Incaricato
- Presentazione dell’IFPDT alla luce della pandemia di Corona
  - Attività dell’IFPDT
  - Le preoccupazioni principali dell’IFPDT
  - Esempio pratico
- Ulteriori informazioni sull’IFPDT
  - Soprattutto nell'attuale 28. rapporto di attività 2020/21

La nuova LPD dal punto di vista dell'IFPDT (1/7)

- Solo dati di persone fisiche
  - Dati delle persone giuridiche non sono più coperti della nuova LPD
- Dati personali degni di particolare protezione
  - Dati genetici
  - Dati biometrici (parzialmente)
- Consulenti per la protezione dei dati
  - Obbligo per organi federali
  - Nominazione volontaria per imprese private

La nuova LPD dal punto di vista dell'IFPDT (2/7)

- Valutazioni d'impatto sulla protezione dei dati
  - Rischio elevato
  - Eccezioni
  - Contenuto
  - Obbligo di consultazione
- Codici di condotta
  - Asscociazioni professionali, settoriali e commerciali
  - Parere dell’IFPDT
  - Presunzione

La nuova LPD dal punto di vista dell'IFPDT (3/7)

- Certificazione
  - Importanza attuale
  - Nessun cambiamento fondamentale
  - Campo ampliato: certificazione dei servizi
  - Nuovo incentivo: esenzioni dall’obbligo DPIA
- Registro delle attività di trattamento
  - Eccezione per aziende con < 250 collaboratori e rischio basso

La nuova LPD dal punto di vista dell'IFPDT (4/7)

- Comunicazione di dati personali all’estero
  - Manutenzione del concetto attuale con modificazioni
  - Excursus: SCC dopo «Schrems II»
- Obblighi di informazione estesi
  - Limitazione nel campo privato abolita
  - Informazioni sullo stato ricevente e le eventuali garanzie
  - Decisioni individuali automatizzate

La nuova LPD dal punto di vista dell'IFPDT (5/7)

- Diritto d’accesso della persona interessata
  - Ampliato, in particolare elenco esteso delle informazioni minime
- Sicurezza dei dati e la sua violazione
  - Continuità
  - Approccio basato sul rischio
  - Violazioni della sicurezza dei dati
  - Delimitazioni
  - Notifica di violazione dei dati (titolare → IFPDT; responsabile → titolare)

La nuova LPD dal punto di vista dell'IFPDT (6/7)

- Inchiesta per tutta violazione delle disposizioni sulla protezione dei dati
  - Soglia di intervento nel campo dei privati abolita
  - Eccezione per violazioni di poca importanza
- Decisioni
  - Procedura regolata dalla LPA
  - IFPDT può emettere decisioni

La nuova LPD dal punto di vista dell'IFPDT (7/7)

- Emolumenti
  - Codice di condotta
  - Valutazione d’impatto
  - Clausole tipo (SCC) e norme interne d’impresa vincolanti (BCR)
  - Servizi di consulenza generale ai privati
- Sanzioni
  - Multe fino a CHF 250’000 per i privati
  - Ruolo dell’IFPDT non cambia (nessuna competenza penale)

Excursus: le autorità e la Cloud

- Sfida per la Confederazione e i Cantoni
- Protezione dei dati e sicurezza delle informazioni
- Segreto d’ufficio
- Problemi speciali con la Cloud all'estero

Repubblica e Cantone Ticino

Dr. Giorgio Rastrelli

Co-Direttore, Centro di Calcolo Elettronico SA

Centro di calcolo elettronico
Dott. Ing. G. Lombardi SA

Protezione dei dati e sicurezza del sistema informativo – La situazione nei Comuni

Dott. Giorgio Rastrelli

Lugano, 14 Ottobre 2021

Centro di calcolo elettronico
Dott. Ing. G. Lombardi SA

Chi è CCE SA

- CCE si «stacca» dalla LOMBARDI SA e diventa una società autonoma focalizzata nella progettazione e realizzazione di soluzioni e servizi per le Amministrazioni Comunali

- Opera nel Canton Ticino e nei Grigioni di lingua italiana

- I suoi clienti sono Comuni, Patriziati, Enti e il Cantone

- Le soluzioni offerte sono:
  - Ge.Co.Ti. Web: soluzione per la gestione dei processi del Comune (38 moduli quali ad esempio Controllo Abitanti, Gestione Stabili, Tasse, Gestione Morosi, Naturalizzazioni, ecc.)
  - eGov.Ti.: soluzione di eGovernment composta da diversi moduli (eMunicipio, eCittadino, ePolizia, ecc.)

oltre a fornire servizi di consulenza , formazione e outsourcing sistemistico

Centro di calcolo elettronico
Dott. Ing. G. Lombardi SA

Chi è CCE SA

- 81 Comuni clienti comprese le città
- 32 Patriziati e Enti
- Oltre l’80% della popolazione gestito con la soluzione Ge.Co.Ti. Web

Centro di calcolo elettronico
Dott. Ing. G. Lombardi SA

La protezione dei dati per i Comuni

Come noto in termine di protezione dei dati:

- I Comuni sono assoggettati alla LPDP
- Attualmente la LPDP è sottoposta a «*….revisione totale, in recepimento del diritto internazionale superiore. Stato della revisione: Progetto legislativo e rapporto al vaglio del Consiglio di Stato*.» Fonte: sito ufficiale del Cantone-Sezione Protezione Dati
- Attualmente non sono noti i tempi di entrata in vigore della nLPDP

Ciò non toglie che ci si debba attivare per non farsi trovare impreparati

Centro di calcolo elettronico
Dott. Ing. G. Lombardi SA

Sicurezza informatica e protezione dei dati. La situazione nei Comuni dal nostro osservatorio

Sulla base delle informazioni raccolte, e delle evidenze osservate quotidianamente, possiamo affermare che:

- Non c'è sufficiente conoscenza dei cambiamenti legislativi che stanno arrivando in merito alla protezione dei dati e degli effetti che questi hanno sull'organizzazione e sui processi del Comune

- Non c'è sufficiente consapevolezza della necessità di proteggere il patrimonio di dati sensibili gestiti dai Comuni. Si tende a pensare che sia un problema dei fornitori

- Non c'è sufficiente cultura in merito alla stretta connessione tra sicurezza del sistema informativo e protezione dei dati, dove per sistema informativo si intende tutto l'insieme delle componenti e risorse che rilevano e gestiscono dati. Oggi tutti i sistemi sono interconnessi (allarmi, video sorveglianza, controllo accessi etc..) di conseguenza, l'effetto «domino» negli attacchi è devastante

Centro di calcolo elettronico
Dott. Ing. G. Lombardi SA

Sicurezza informatica e protezione dei dati. La situazione nei Comuni dal nostro osservatorio

ma qualcosa sa sta cambiando ….

- Fino a poco tempo fa, nonostante il CCE stesse sensibilizzando da diverso tempo i propri clienti con mail ed eventi in merito al tema della protezione dei dati connesso alla sicurezza informatica, non venivano intraprese azioni in tal senso dai Comuni

- I recenti eventi di attacchi informatici ai Comuni (ad esempio Rolle) ha indotto una maggiore attenzione alla problematica delle protezione dei dati legata alla sicurezza del sistema informatico. Quello che non poté la ragione poté la paura

- La pubblicazione da parte della Confederazione del tool di valutazione della gestione sicurezza (si trova il link anche sulla pagina https://www4.ti.ch/di/cybersicuro/home) ha fornito un utile strumento di autovalutazione che ha permesso di meglio comprendere l'ampiezza della problematica e la necessità di promuovere azioni atte a rispondere ai requisiti richiesti

Centro di calcolo elettronico
Dott. Ing. G. Lombardi SA

Sicurezza informatica e protezione dei dati. La situazione nei Comuni dal nostro osservatorio

- Molti clienti stanno passando dall'utilizzo delle soluzioni dalla modalità On Premise alla modalità SaaS che, grazie anche a garanzie e certificazioni ISO da parte di Datacenter qualificati, possono garantirsi livelli di sicurezza maggiori

- Ad oggi solo il 10% dei Comuni nostri clienti ha intrapreso azioni atte a migliorare la protezione dei dati anche dagli attacchi informatici aumentando la sicurezza dei propri sistemi

- Le recenti iniziative come quella odierna e le recenti vicende successi in altri Comuni, hanno fatto si che in meno di un mese un ulteriore 10% dei Comuni nostri clienti si è attivato per la valutare le azioni da intraprendere

Centro di calcolo elettronico
Dott. Ing. G. Lombardi SA

Prepararsi all'introduzione della nLPDP. Cosa si può fare da subito

- Pur non essendo ancora ufficializzata la nuova versione della nLPDP si sa già che recepirà quanto recepito nella nLPD seppur contestualizzato
- I cambiamenti introdotti dalla nLPDP toccheranno diversi aspetti quali ad esempio:
  - l'organizzazione per la richiesta della presenza di procedure idonee alla corretta gestione e salvaguardia dei dati e di precisi ruoli e responsabilità
  - la formazione del personale sulle procedure e sull'utilizzo corretto degli strumenti a disposizione
  - la conformità del sistema informativo agli standard di sicurezza necessari per garantire la corretta protezione dei dati

Centro di calcolo elettronico
Dott. Ing. G. Lombardi SA

Prepararsi all'introduzione della nLPDP. Cosa si può fare da subito

Si possono adottare una serie di soluzioni e servizi per aiutare i Comuni a prepararsi al rispetto di alcuni aspetti che saranno sicuramente presenti nella nLPDP.

- **Disponibilità di soluzioni in modalità SaaS** per garantire ai comuni un livello di protezione dei dati elevata. Alcune caratteristiche delle soluzioni da adottare:
  - Autenticazione delle soluzioni a due fattori
  - Architettura dei collegamenti di rete progettata e realizzata per soddisfare pienamente i criteri di sicurezza per i servizi ad alta affidabilità (es. connessioni tramite VPN in modalità end to end crittografata, monitoraggio continuo 7X7 24X24 e servizi di Advanced threat Protection tra cui servizi di Intrusion Detection, ecc.)
  - Utilizzo di Data Center Svizzero certificato almeno con standard ISO 27001 a garanzia di rispetto delle normative in ambito di sicurezza dell'informazione.
  - Politica di backup applicata per soddisfare al meglio un eventuale recupero dei dati nel caso necessitasse.
  - …..

Centro di calcolo elettronico
Dott. Ing. G. Lombardi SA

Prepararsi all'introduzione della nLPDP. Cosa si può fare da subito

- **Servizi di Cybersecurity**

  Sono servizi che, tra l'altro, rispondono e soddisfano diversi requisiti richiesti nel tool di valutazione della Confederazione. Alcune caratteristiche :

  - Inventario aggiornato della dotazione informatica
  - Stato di aggiornamento del software di middleware utilizzato (S.O., Browser, ecc.) e possibili minacce legate al mancato aggiornamento
  - Monitoraggio costante della rete 7X7 24x24 e di tutti i dispositivi connessi con identificazione e documentazione delle minacce esterne
  - Identificazione dei software dannosi (ransomware, trojan, malware, ecc.) e segnalazione
  - Registrazione dei log di accesso
  - Elaborazione degli eventi di sicurezza tramite apposite dashboard

Centro di calcolo elettronico
Dott. Ing. G. Lombardi SA

Prepararsi all'introduzione della nLPDP. Cosa si può fare da subito

- Innesco situazioni di allarme su soglie impostate
- Monitoraggio del dark web
- Presa in carico delle segnalazioni derivanti dal sistema di monitoraggio e adozioni azioni corrette in funzione del tipo di segnalazione
- Pianificazione delle contromisure
- .....

Centro di calcolo elettronico
Dott. Ing. G. Lombardi SA

Prepararsi all'introduzione della nLPDP. Cosa si può fare da subito

- **Servizi di consulenza** per il supporto alla compliance del Comune alla nLPDP . Alcuni esempi:

  - Check di valutazione sulla situazione del Comune
  - Supporto nella definizione di ruoli e responsabilità rispetto a quanto richiesto dalla nLPDP
  - Supporto nella definizione delle procedure necessarie per l'attuazione e la verifica di quanto previsto dalla nLPDP
  - Supporto nell'identificazione delle misure necessarie nell'ambito del sistema informatico del Comune
  - …

Centro di calcolo elettronico
Dott. Ing. G. Lombardi SA

Conclusioni

- I Comuni dovrebbero incrementare la loro conoscenza in merito alle novità normative. Convegni come questo aiutano a diffondere la conoscenza e la consapevolezza

- I Comuni dovrebbero comprendere che le nuove normative hanno un impatto importante sulla situazione attuale della loro organizzazione e che quindi dovranno supportare una gestione del cambiamento (change management)

- I Comuni dovrebbero fare propria la stretta correlazione che intercorre tra protezione dei dati e sicurezza del sistema informativo, adottando soluzioni e strumenti idonei a garantire il Comune e i suoi cittadini in merito alla corretta gestione e protezione dei dati

- I Comuni dovrebbero attivarsi da subito affidandosi a fornitori di comprovata esperienza che li supportino nell'implementazione di quanto necessario per la compliance con nLPDP. Alcuni interventi si possono e si devono fare da subito

… c'è molto da fare… ma ce la faremo

Repubblica e Cantone Ticino

Avv. Rocco Talleri

Avvocato e titolare dello studio legale Talleri Law

LPD – DA DOVE COMINCIARE?

SPUNTI PRATICI

SOMMARIO

1. Identificare , conoscere e monitorare i PROCESSI
2. Esame di IMPATTO
3. «GAP analysys»
4. La gestione del RISCHIO

CONOSCERE L'ATTIVITÀ

(STUDIO E COMPRENSIONE DEL FLUSSO DEI DATI)

1. PROCESSI

- La nuova LPD, che si applica al trattamento da parte di privati e organi federali*(art. 2), ha lo scopo di *«proteggere la personalità e i diritti fondamentali delle persone fisiche i cui dati personali sono oggetto di trattamento» (art. 1).* La Legge definisce i dati personali (art. 5 a) e distingue *i dati personali degni di particolare protezione (art. 5 c)* e le attività di trattamento, comunicazione e profilazione e profilazione a rischio elevato (art. 5 d-g), così come pure i diversi ruoli nel trattamento (art. 5 j e k).
- La LPD sancisce i principi del trattamento (art. 6), in particolare quelli della liceità, della buona fede, della proporzionalità, dello scopo (definito, limitato e riconoscibile), della conservazione limitata dallo scopo o dalle norme, dell'esattezza dei dati e dei diritti dell'interessato qualora non sia il caso, dell'adeguatezza delle misure di sicurezza (commisurate al RISCHIO) la presenza se necessario (art. 6 cpv. 7) del consenso.
- La LPD introduce il principio della protezione dei dati personali sin dalla progettazione e per impostazione predefinita (art. 7, privacy by design e by default)
- La LPD impone al titolare e al responsabile di garantire la sicurezza dei dati (art. 8)
- La LPD prevede il *«registro delle attività di trattamento» (art. 12)*

CONOSCERE L'ATTIVITÀ

(STUDIO E COMPRENSIONE DEL FLUSSO DEI DATI)

1. PROCESSI

- Il ROPA (Record Of Processing Activities) come strumento di lavoro. L'aiuto arriva dalla nLPD, che fornisce gli elementi che devo identificare e conoscere. Questa operazione, che può essere gestita anche attraverso dei tools, implica una profonda conoscenza delle attività e permette anche di riordinare e ottimizzare i processi aziendali.
- L'art. 12 recita:

  1 I titolari e i responsabili del trattamento tengono ognuno un registro delle rispettive attività di trattamento.

  2 Il registro del titolare del trattamento contiene almeno:

  a. ***l'identità del titolare del trattamento****;*
  b. lo ***scopo del trattamento****;*
  c. una ***descrizione delle categorie di persone interessate e delle categorie di dati personali trattati****;*
  d. le ***categorie di destinatari****;*
  e. se possibile, ***la durata di conservazione*** *dei dati personali o* ***i criteri per determinare tale durata****;*
  f. se possibile, una ***descrizione generale dei provvedimenti tesi a garantire la sicurezza dei dati personali*** *secondo l'articolo 8;*
  g. se i dati personali sono comunicati all'estero, le indicazioni relative allo Stato destinatario e le garanzie di cui all'articolo 16 capoverso 2.

L'IMPATTO
(SULLE PERSONE INTERESSATE)

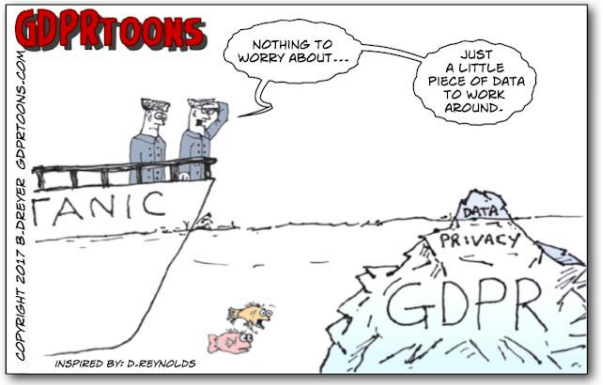
2. IMPATTO

- La nuova LPD, prevede (art. 22, cpv. 1) che «*il titolare del trattamento effettua previamente* ***una valutazione d'impatto*** *sulla protezione dei dati quando il trattamento dei dati personali può comportare* ***un RISCHIO elevato per la personalità o i diritti fondamentali della persona interessata***. *Se prevede più operazioni di trattamento simili può procedere a una valutazione d'impatto comune*»;
- Per il legislatore (art. 22 cpv. 2), «*Il rischio elevato, in particolare in caso di utilizzazione di nuove tecnologie, risulta dal tipo, dall'entità, dalle circostanze e dallo scopo del trattamento. Sussiste segnatamente nel caso di:*
  a. *trattamento su grande scala di dati personali degni di particolare protezione;*
  b. *sorveglianza sistematica di ampi spazi pubblici.*
- La valutazione deve contenere almeno (art. 22 cpv. 3), «*una* ***descrizione del trattamento previsto****, una* ***valutazione dei rischi per la personalità*** *o per i diritti fondamentali della persona interessata nonché i provvedimenti a loro tutela*»

L'IMPATTO
(SULLE PERSONE INTERESSATE)

2. IMPATTO

- La valutazione dell'IMPATTO impone di conoscere nel dettaglio i processi di trattamento e di identificare i RISCHI. Occorre quindi valutare quali processi sono più adatti per raggiungere gli scopi dell'attività, valutando eventualmente opzioni alternative.
- La valutazione impone di identificare la base giuridica del trattamento, la qualità e la quantitià dei dati raccolti, le modalità di gestione, le misure organizzative interne (ed esterne), le misure per garantire l'esecizio dei diritti degli interessati, le norme a cui devono sottostare i partner (responabili del trattamento).
- Tale analisi deve essere documentata e non è un processo statico ma si evolve con l'attività dell'azienda.

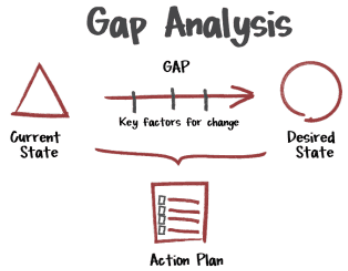


GAP ANALYSIS

(OVVERO LA RICERCA DELLE NON CONFORMITÀ)

3. GAP

- Fra la **situazione di fatto** e **quella conforme alle disposizioni appli**cabili vi è sempre **un divario:**
  - generalmente non vi è chiarezza sulla base legale del trattamento, spesso legato al consenso e quindi potenzialmente problematico;
  - i partner e i fornitori lavorano spesso su basi consuetudinali e non su contratti che definiscono i principi legati alla protezione dei dati (e non solo quelli…);
  - ruoli e responsabilità non definiti e non corrispondenti all'organizzazione e all'organigramma;
  - documentazione obsoleta, incompleta e non corretta;
  - archivi «pieni» di vecchi dati del tutto inutili.
- Occorre quindi prevedere le misure necessarie per correggere le situazioni non conformi, stabilendo chiare responsabilità e definendo gli obiettivi, avendo sempre cura di documentare tutto nel dettaglio e di adeguare tale attività al quadro normativo di riferimento che può mutare.

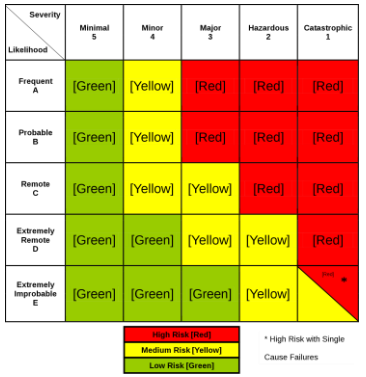


LA GESTIONE DEL RISCHIO

(E DELLE MISURE DI MITIGAZIONE)

4. RISCHIO

- La gestione del RISCHIO è un processo estramente complesso e deve partire ed essere gestito dai vertici dell'azienda (CdA).
- La cosidetta Risk Governance esprime la consapevolezza dei vertici in relazione al RISCHIO e alla sua gestione. Deve tenere conto della predisposizione o «appetito» (risk appetite) dell'azienda,. L
- La gestione del RISCHIO passa attraverso la definizione di processi strategici, operativi e organizzativi, laddove i sistemi di mitigazione del RISCHIO devono essere integrati nei processi in maniera efficace e dinamica. Occorre una supervisione costante e una capicità di intercettare le situazioni ad alto RISCHIO e possibilimente di anticiparle. In questo ambito l'aspetto tecnologico deve essere integrato e servire da supporto attivo alla altre misure
- Ci sono diversi approcci (vedi esempi sotto, fonte wikipedia), che hanno in cumune da un lato l'analisi del RISCHIO e dall'altro la «misura» dell'efficacia delle soluzioni e dei sistemi di mitigazione e, in ultima analisi costituiscono un importante base per le decisioni del management.



GRAZIE PER L'ATTENZIONE

Rocco Talleri
Avvocato – CAS DPO-HSG

Studio legale
Talleri Law
Via Cattedrale 4
P. O. Box 6544
CH-6901 Lugano
tel. ++ 41 91 921 45 47
rocco@talleri.ch
www.talleri.law

talleri | law

Repubblica e Cantone Ticino

Conclusioni

Dr. Alessandro Trivilini

Responsabile del Servizio informatica forense del Dipartimento tecnologie innovative, SUPSI
Membro Gruppo «Cyber sicuro»

Domande

CYBER
SICURO