Risk Management Q&A

Edoardo Ottavianelli & Matteo Piermartini

Asaro:

1. Leggi omeostatiche

La società umana, in questa fase primitiva si trova in una condizione di alta entropia, siccome non è regolata da specifiche norme, la struttura va in crash. L'entropia è distruttiva perché significa collasso delle regole che consentono alla struttura di sopravvivere. Ma le strutture umane si proteggono, hanno un meccanismo chiamato omeostasi che ristabilisce gli equilibri. Quindi queste azioni regolatrici prodotte dal feedback è un effetto dell'omeostasi.
Possiamo definire la legge come un fattore di termoregolazione delle tensioni sociali. Da qui discende che la legge è un fattore di protezione per i membri della comunità ed è anche un fattore di sviluppo della società = quindi la legge è un fattore omeostatico.

Ci sono 3 assunzioni e una conclusione:
1. La legge regola i conflitti sociali;
2. La legge proteggi i membri di una comunità;
3. La legge è un fattore di sviluppo della società.
Ma questi sono compiti tipici dell'omeostasi allora dobbiamo arrivare alla conclusione che: la legge è un fattore omeostatico.

2. Tipi di distruzione del dato

Esistono diverse tecniche di cancellazione a seconda del grado di importanza e segretezza delle informazioni da cancellare.
Lo standard NIST 800-88 definisce i seguenti tipi di eliminazione dei dati (sanificazione):
• smaltimento, cioè il semplice smaltimento del supporto come rifiuto, così come noi facciamo con gli ordinari rifiuti di casa;
• clearing, che impedisce il recupero dei dati sovrascrivendo i supporti;
• purging, ovvero l'eliminazione dei dati dal supporto magnetico e l'inoperabilità della memoria (risultato ottenuto mediante l'utilizzo di un 'smagnetizzatore', ovvero un processo di smagnetizzazione che cancella hard disk e drive rendendoli inutilizzabili);
• la distruzione, ovvero la distruzione fisica del supporto.

Secondo lo standard 800-88, la distruzione deve essere fatta in casi estremi. Le azioni suggerite per la distruzione sono, a seconda del tipo di memoria: triturazione, polverizzazione, fusione, incenerimento. Questo sistema è adottato dalla NSA (National Security Agency degli Stati Uniti, organismo che, insieme alla CIA e all'FBI, si occupa della sicurezza nazionale americana) per tutte le procedure riguardanti le forze militari e le informazioni 'top secret' in possesso delle agenzie di intelligence.

3. Tipi di dato

Esistono due tipi di dato:
1. Dato tecnico:
- Dato Booleano;
- Puntatori;
- Array: è una matrice di variabili tutte dello stesso tipo, costituita da caselle chiamate celle o elementi.
- Record: sono contenitori di tipi di dati strutturati. Il dato immesso in un campo del record ne rappresenta il valore ed è detto "attributo".
- Variabile: è un contenitore di un solo valore che può cambiare.
- Costante: è un valore che non può essere modificato nel corso dell'esecuzione del programma.
- Tipi Numerici: Abbiamo tre tipi: Numeri interi, Numeri a virgola mobile e Punto fisso.
- Chiave Primaria: in una tabella identifica in modo univoco una riga. Serve per evitare l'equivocità del dato.
- Template: Sono costruttori di ulteriori tipi definiti dal programmatore.
- Abstract data type (ADT): è un modello matematico per i tipi di dati. Le operazioni sui dati vengono compiute dall'utente sulla base della semantica delle sue operazioni. L' utente non agisce sul processore, manipola i dati in base alla risposta operativa alle sue operazioni.

2. Dato semantico: Dal punto di vista del dato, i dati verranno classificati in ragione del loro significato.
Il dato semantico viene classificato in relazione al:
- campo di conoscenza a cui appartiene (es.: medicina);
- allo specifico settore (es.: cardiologia);
- alle eventuali sottoclassi (es.: cardiologia vascolare);
I tipi di dati semantici sono per esempio: dati meteorologici, dati monetari, dati linguistici, dati epidemiologici, dati giuridici, dati personali.
Ai dati semantici bisogna applicare dei controlli di Legalità e di Consistenza:

- Legacy control: Il controllo di legalità ha ad oggetto la corrispondenza del dato alle regole che ne disciplinano la produzione e l'uso. Queste regole possono essere di tipo giuridico (provvedimento emesso dall'ente) o stabilite dal produttore del dato (attraverso un contratto), o da entrambi.
- Consistency control: Il controllo di coerenza del dato differisce dal controllo di legalità. Qui entra in campo la semantica, cioè l'analisi del contenuto di conoscenza denotato dal dato, la sua localizzazione nell'universo del discorso (ambito di conoscenza e di operatività) rappresentato nel sistema, la sua compatibilità con esso.
Il controllo di coerenza ha, in particolare, ad oggetto:
• la compatibilità del dato con le specifiche e gli scopi del sistema;
• la riferibilità concettuale del dato alla sua classe di dati (ad. es. il dato "piovosità" non sarebbe compatibile con un catalogo di invertebrati);
• l'osservanza della gerarchia dei dati (ad es., "dirigente", in una classificazione del personale, non può essere rappresentato ad un livello inferiore a "impiegato");
• l'unicità e l'univocità del dato rispetto al contenuto rappresentato.

4. Struttura norma penale

Innanzitutto possiamo fare una distinzione tra due tipi di norme penali:
1. Norma penale di Comportamento (detta anche "Norma di diritto penale Sostanziale");
2. Norma penale di Procedura (detta anche "Norma di diritto penale Processuale").
La Norma Penale in generale è formata da due tipi di regole:
1. Regole di Qualificazione: per esempio, la norma che qualifica determinati soggetti come pubblici ufficiali, in relazione alle funzioni svolte.
2. Regole Procedurali: regole del processo penale, per esempio, come si fanno le investigazioni.
Possiamo dire che il Reato è una norma di diritto Penale Sostanziale, la quale è composta da due elementi base:
1. Condotta tipica;
2. Pena;

5. Funzionamento Procedimento Penale

L'accertamento delle responsabilità penale avviene attraverso il procedimento penale. Esso passa attraverso le seguenti fasi:
• le indagini preliminari, dirette dal pubblico ministero;
• il processo, diretto dal giudice.

Da notare: le indagini preliminari fanno parte del procedimento penale, ma non del processo penale perché non sono dirette dal giudice.
Le indagini preliminari prendono avvio dalla notizia di reato trasmessa da un organo di polizia giudiziaria (PG) al Pubblico Ministero (PM). Ma questi può acquisire la notizia di reato anche direttamente . La notizia di reato può altresì provenire dalla querela della persona offesa o dalla denuncia di un privato. La querela è una istanza con cui la persona offesa dal reato chiede la punizione del colpevole. Viene presentata alla polizia giudiziaria o al pubblico ministero, a pena di decadenza, entro novanta giorni dal fatto o dalla conoscenza di esso. La denuncia è la segnalazione che chiunque può fare al PM o alla PG che un reato è stato commesso, con l'indicazione dell'autore, se conosciuto.
Durante le indagini preliminari diversi atti, contenenti dati penali, vengono compiuti dal pubblico ministero, dalla polizia giudiziaria, dal difensore dell'indagato. Non tutti questi dati entrano nel processo. Uno sbarramento preliminare, costituito da norme procedurali, funge da filtro.
Conclusasi la fase delle indagini preliminari, l'indagato, se portato a processo, prende il nome di imputato. Il processo penale e il procedimento penale non sono la stessa cosa, il procedimento penale è l'insieme degli atti che vanno da quando io commetto/si presume il reato e qualcuno inizia ad indagare, quindi va da quando si inizia ad indagare sino alla sentenza finale. Il processo penale è quella parte che compete al giudice, quando il pm ha effettuato le indagini preliminari e le consegna al giudice.
Onere della prova e Gradi di giudizio vedi sotto.

6. Gradi di giudizio

Il processo penale in Italia si articola in più gradi:
• Processo di primo grado;
• Giudizio di appello;
• Giudizio di Cassazione.
Il passaggio al grado successivo è determinato da un atto di impugnazione che può essere proposto sia dall'imputato (o dal suo difensore), sia al pubblico ministero. In difetto di impugnazione o quando è esaurito l'ultimo grado, la sentenza del giudice passa in giudicato, cioè diventa definitiva e deve essere eseguita.

7. La prova

Nel corso delle indagini preliminari il Pubblico Ministero, avvalendosi della collaborazione della Polizia Giudiziaria, raccoglie elementi atti a individuare il

responsabile, a ricostruire le modalità e circostanze del fatto criminoso, ad assicurare le fonti di prova.
Gli atti di evidence compiuti dal PM e dalla PG delegata possono dunque essere classificati in relazione alla fonte, in quanto diretti ad acquisire rispettivamente:

1. Prova personale: la prova che si ottiene attraverso l'esame di persone. Abbiamo diverse fonti di prova personale che si ottengono da dichiarazioni:
- interrogatorio del sospettato: La persona indagata può rendere dichiarazioni al pubblico ministero o all'ufficiale di polizia giudiziaria delegato sotto forma di interrogatorio. Questo atto è compiuto con la presenza necessaria del difensore. L'indagato ha il dovere di presentarsi al PM. Prima di interrogarlo il PM fa presente all'indagato che ogni sua affermazione potrà essere usata contro di lui. L'indagato ha la facoltà di rifiutarsi di rispondere, o di rispondere solo in parte, o anche di mentire per ciò che attiene al merito dell'accusa. La persona sottoposta alle indagini ha, invece, il dovere di rispondere e di dire la verità in relazione alle domande sulla sua identità e sulle sue condizioni personali. Prima di procedere all' interrogatorio, il pubblico ministero rende noto all'indagato il reato per cui sta procedendo e gli elementi acquisiti contro di lui. Il PM può tacere sulle fonti di questi elementi, se può derivare un pregiudizio per l'indagine.
- dichiarazioni dell'indagato alla Polizia Giudiziaria: È vietato alla polizia giudiziaria (PG) assumere informazioni dalla persona sottoposta ad indagini in assenza del suo difensore. Può eccezionalmente farlo soltanto nel luogo e nell'immediatezza del fatto, ma in questo le dichiarazioni rese dall'indagato non possono essere documentate, né utilizzate contro di lui. Possono invece essere usate a fini investigativi.
La persona indagata può rendere spontaneamente alla polizia giudiziaria dichiarazioni anche in assenza del suo difensore, ma queste dichiarazioni non possono essere utilizzate come prova, né essere trascritte in documenti. Anche qui l'unico uso possibile è di tipo investigativo.
L'ufficiale di polizia giudiziaria può interrogare l'indagato solo su delega del pubblico ministero.
- persona informata sui fatti
- il consulente tecnico del P.M. o dell'indagato o della persona offesa
- la polizia giudiziaria
- l'interprete

2. Prova reale: Chiamiamo prova reale quella che si ottiene attraverso l'esame di cose.

In particolare, costituiscono prova reale tutte quelle cose che per la loro esistenza, o presenza in un certo tempo o luogo, o per la loro conformazione, o per le tracce su di loro impresse, o per la loro condizione o qualità, sono atte a lumeggiare il fatto criminoso o le sue circostanze, o il suo movente, o a evidenziare le caratteristiche personali o di ambiente della vittima o del colpevole, o di soggetti comunque coinvolti nel procedimento.

3. Prova documentale: Chiamiamo prova documentale quella che si ottiene attraverso l'acquisizione e l'esame di documenti. Questi possono essere cartacei, o in formato elettronico e possono avere qualsiasi contenuto: testo, diagrammi, software, immagini, ecc.. Costituiscono prova documentale, fra gli altri:
• la relazione tecnica: I consulenti tecnici eventualmente nominati dalle parti private hanno diritto di assistere sia alla consulenza tecnica che alla perizia. A conclusione dell'incarico ricevuto, il consulente tecnico o il perito depositano una relazione nella quale illustrano i risultati raggiunti e il procedimento seguito. Questa relazione è una prova documentale. Il consulente tecnico o il perito possono essere chiamati a dare delle delucidazioni orali sul contenuto della relazione. In tal caso siamo in presenza di una prova personale.
• i rilievi topografici, fotografici, aerofotogrammetrici
• gli atti di altro procedimento di cui la legge consenta l'acquisizione
• ogni altro documento acquisito al fascicolo del pubblico ministero o prodotto dalla difesa.

8. Responsabilità civili e penali nel Pen Test

Nell'esecuzione del pentest è possibile che l'operatore commetta uno o più reati previsti dalle norme penali elencate di seguito:
- Accesso non autorizzato a un computer o a un sistema di telecomunicazione
- Possesso e distribuzione non autorizzati dei codici di accesso ai sistemi informatici o di telecomunicazione
- Distribuzione di apparecchiature, dispositivi o programmi informatici finalizzati a danneggiare o interrompere un sistema informatico o telematico
- Chiunque fraudolentemente intercetta comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi(2), ovvero le impedisce o le interrompe(3), è punito con la reclusione da sei mesi a quattro anni
- Chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito [...]
- Danni a informazioni, dati e programmi informatici utilizzati dallo Stato o da altri pubblici o in ogni caso di pubblica utilità

- Danni ai sistemi informatici o telematici
- Danni ai sistemi informatici o telematici di pubblica utilità

È possibile che sia l'operatore che il gestore del sistema inseguano di responsabilità civile a causa di un fatto illecito che ha danneggiato l'altra parte, o per aver violato le regole del contratto di prova di penetrazione. Di seguito sono riportate alcune regole del codice civile che possono essere prese in considerazione:
- Il debitore e il creditore devono comportarsi secondo le regole della correttezza
- Nell'adempiere l'obbligazione il debitore deve usare la diligenza del buon padre di famiglia
- Il debitore che non esegue esattamente la prestazione dovuta è tenuto al risarcimento del danno [...]
- Il risarcimento del danno per l'inadempimento o per il ritardo deve comprendere così la perdita subita dal creditore come il mancato guadagno
- È nullo qualsiasi patto che esclude o limita preventivamente la responsabilità del debitore per dolo o per colpa grave
- Il contratto deve essere eseguito secondo buona fede
- Qualunque fatto doloso o colposo, che cagiona ad altri un danno ingiusto, obbliga colui che ha commesso il fatto a risarcire il danno

9. Le condizioni generali del contratto e cause di invalidità delle clausole

Le condizioni generali di contratto predisposte da uno dei contraenti sono efficaci nei confronti dell'altro, se al momento della conclusione del contratto questi le ha conosciute o avrebbe dovuto conoscerle usando l'ordinaria diligenza. In ogni caso non hanno effetto, se non sono specificamente approvate per iscritto, le condizioni che stabiliscono, a favore di colui che le ha predisposte, limitazioni di responsabilità , facoltà di recedere dal contratto o di sospenderne l'esecuzione, ovvero sanciscono a carico dell'altro contraente decadenze, limitazioni alla facoltà di opporre eccezioni, restrizioni alla libertà contrattuale nei rapporti coi terzi, tacita proroga o rinnovazione del contratto, clausole compromissorie o deroghe alla competenza dell'autorità giudiziaria.

10. Il dato

Il dato non è isolato ma vive in un universo di informazioni. Vediamo quali sono i componenti del dato:
- Contenuto
- Formato

- Contesto
- Funzione
- Scopo
- Conoscibilità
- Produttore
- Tipologia
- Link
- Metadata

1. Contenuto: Il contenuto di un dato è l'unità elementare di conoscenza in esso contenuta. Questo contenuto richiede di essere interpretato, sia che si tratti di una figura o di un'immagine o di parole. Mentre le figure e le immagini richiamano direttamente nella nostra mente la rappresentazione della cosa (quando vedo una rosa disegnata la paragono alle rose che sono cadute sotto la mia esperienza), se vedo la parola "rosa" scritta devo interpretarla. E lo faccio non sulla base di un'esperienza, ma sulla base di una conoscenza, proprio sulla base della conoscenza condivisa della mia comunità linguistica che usa un codice condiviso (le parole) per indicare tutto ciò che è oggetto della nostra conoscenza.
Inoltre è importante che la forma del dato sia univoca e unica. La differenza sta che se dico sedia deve significare sedia (univoca), per dire la stessa cosa non devo poter dire seggia, sedia, seggio, questo diventa un elemento di confusione nella fase di computazione.

2. Formato: Il formato è l'involucro esterno del dato, l'elemento materiale in cui esso è contenuto. Esiste quindi una chiara distinzione tra il contenuto informativo dei dati e il supporto materiale in cui sono incorporati.
L'informazione è una porzione di conoscenza. Appartiene quindi alla classe dei significati. La forma in cui quella informazione è espressa è qualcosa che la richiama, che la denota. È dunque un significante.

3. Contesto: Ci sono dati il cui significato è interamente denotato dalla forma (significante) che lo esprime. Ma il più delle volte questo non accade. Il dato acquista significato nel contesto comunicativo che lo contiene. In termini di rischio, il contesto assume particolare rilevanza, in quanto la separazione arbitraria dei dati dal loro contesto pregiudica l'esatta interpretazione e può causare gravi danni. Nella gestione del rischio, la preservazione del contesto è un profilo dell'integrità dei dati.

4. Funzione: La funzione realizza lo scopo pratico del dato, ciò a cui esso serve. Non è dissimile dalla funzione degli oggetti: la penna serve per scrivere, qualsiasi cosa io scriva; la funzione del log è quella di registrare gli accessi e le operazioni effettuate dall'utente, indipendentemente dall'uso che potrà essere fatto di quelle registrazioni. Possiamo dunque definire la funzione di un dato come il suo scopo immanente, inerente alla sua struttura o tipologia.

5. Scopo (Finalità): Funzione del dato è ciò per cui il dato è stato creato, mentre la finalità è un requisito esterno, ciò che possiamo fare con questo dato. Possiamo distinguere la finalità in due modi:
- Finalità operativa: come il dato mi lavora nel sistema informatico insieme ad altri dati.
- Finalità strategica: che risultati mi può dare questo dato? Come il dato migliora il risultato che io mi propongo di ottenere?

6. Conoscibilità: è il rapporto tra il contenuto di un dato e i soggetti che sono autorizzati a prendere conoscenza del dato. Dal punto di vista della sicurezza informatica, l'attributo della conoscibilità si chiama confidenzialità.

7. Produttore: Il produttore dei dati non è l'operatore incaricato di inserirli in un database, ma colui che dà forma ad un'unità elementare di conoscenza trasformandola in un dato. A questo punto il dato può essere tout court inserito in un insieme di dati o, come più frequentemente accade, classificato in una tassonomia.

8. Tipologia: è suddivisione che riguarda la tipologia che possono riguardare dati personali e dati di altro tipo.

9. Link: Come avviene che il dato si colleghi ad un altro, abbiamo 3 possibilità:
- lo presuppone (un web feed presuppone lo scambio tra applicazioni o piattaforme);
- lo menzione espressamente (un vaccino antinfluenzale menziona specificamente l'influenza);
- è necessariamente legato ad esso (la quantità di gin in un cocktail è esplicitamente legata agli altri ingredienti).

10. Metadata: guardare domanda 33

11. Differenza tra obbligo e onere

Chi ha un onere deve osservare l'adempimento richiestogli se egli vuole ottenere un determinato risultato per lui vantaggioso. Ad esempio, se voglio ottenere la patente di guida devo fare l'esame di guida. Nessuno mi obbliga a fare questo esame, ma sono tenuto a farlo se voglio, e solo se voglio, ottenere la patente di guida. Invece, chi ha un obbligo deve osservarlo, senza se e senza ma. L'obbligo vincola indipendentemente dalla convenienza il soggetto ne abbia. Ad esempio, il pagamento delle tasse è un obbligo.
Il pubblico ministero non ha l'obbligo della prova ma ha l'onere della prova. L'onere è l'adempimento obbligato da chi voglia un risultato a lui favorevole.

12. La discrezione amministrativa

I dati sono di natura amministrativa quando vengono prodotti o comunque riguardano una pubblica amministrazione nell'esercizio dei suoi poteri. L'attività amministrativa può essere:
• vincolata (se l'ente pubblico è tenuto per legge ad emettere il provvedimento);
• discrezionale (se la legge lascia all'ente pubblico la scelta se emettere il provvedimento o meno).
La discrezionalità della pubblica amministrazione è "normativamente orientata". Ciò significa che l'ente, esaminati gli atti e ogni relativa circostanza:
• deve valutare se sia necessario o opportuno emettere un provvedimento, e quale;
• se la risposta è affermativa, ha l'obbligo di emetterlo.

13. Il processo amministrativo e l'atto impugnato (il profilo della legittimità)

Nel processo amministrativo la contesa giudiziaria si instaura fra un soggetto privato e un provvedimento della pubblica amministrazione. Diversamente dal procedimento penale e da quello civile, non abbiamo due soggetti contrapposti fra loro (Il pubblico ministero e l'imputato nel processo penale; attore e convenuto nel processo civile). Il procedimento amministrativo è attivato da un atto di impugnazione del soggetto privato. Qual è l'evento trigger che scatena il processo amministrativo? È l'atto d'impugnazione alla corte. I soggetti del rapporto amministrativo sono il cittadino e l'ente pubblico. Ma l'analogia con il diritto penale finisce qui. Nel diritto penale l'antagonista è lo Stato, rappresentato dal Pubblico Ministero; nel diritto amministrativo l'antagonista non è necessariamente lo Stato, può essere qualsiasi ente pubblico (Prefetto, Provincia, Capitano di Porto, ecc.). Inoltre, l'illecito penale è un reato, per il quale è prevista una pena; la violazione di un provvedimento amministrativo è

una violazione amministrativa, per la quale è prevista una sanzione amministrativa (di tipo pecuniario o consistente in obblighi o divieti).
Quando un provvedimento è impugnato, il Tribunale accerta se esso è immune da vizi di legittimità. Essi sono:
• Incompetenza, se l'atto è emesso da un soggetto o un ente non competente, cioè non autorizzato dalla legge ad emetterlo; (come un giudice civile chiude una causa penale, come se il pm decide per una causa penale)
• Violazione di legge, se l'atto è contrario ad una legge dello Stato;
• Eccesso di potere, se vi è stata disparità di trattamento, motivazione illogica, manifesta ingiustizia o altra deviazione da un uso corretto del potere. Quando si fa un uso non corretto del potere;

14. Il processo civile

Il diritto civile è costituito dall'insieme delle regole che regolano i rapporti privati tra le persone, sia economici che personali.
Di solito è un soggetto, detto attore, che si rivolge al giudice perché emetta una decisione nei confronti del suo antagonista, detto convenuto.
Il convenuto respinge la pretesa dell'attore, sostenendo le proprie ragioni (eccezioni), o avanzando a sua volta una pretesa contro l'attore (riconvenzione). Ma possono pure essere entrambe le parti a rivolgersi congiuntamente al giudice.
Nel processo civile l'onere della prova spetta all'attore, non al convenuto. Questo onere spetta al convenuto limitatamente alle eccezioni e alle pretese avanzate contro l'attore in via riconvenzionale.
Il diritto civile è regolato dal principio di disponibilità.
A differenza di quanto avviene in campo penale, dove il giudice interviene d'autorità quando la legge viene violata, in campo civile è il soggetto leso nel suo diritto a decidere se citare in giudizio il responsabile (disponibilità dell'azione). Le prove sono offerte dalle parti e il giudice, salvo casi particolari, non può cercarle o indicarle d'ufficio (disponibilità della prova).Se io non la dimostro il giudice non può sostituirmi come nel processo penale, che il giudice può disporre di ulteriore prove.
I dati relativi al diritto civile sono numerosi, perché hanno a che fare con la vita degli uomini.
Appartengono al diritto civile: la regolamentazione delle locazioni, dei diritti reali, della famiglia, del commercio e dei contratti, e così via.

15. Impresa privata vs Ente Pubblico

Le aziende pubbliche hanno un soggetto giuridico pubblico. Le aziende pubbliche, a differenza di quelle private, non hanno come scopo il

conseguimento di un profitto bensì il raggiungimento di un interesse pubblico. Ad esse si applicano le norme di diritto amministrativo.
Le aziende private hanno un soggetto giuridico privato. Rientrano in questa categoria alcune società dette società di capitali, le associazioni, le fondazioni. Esempio: sono aziende private la Pirelli & C. Spa, la Fininvest Spa, le associazioni sportive, ecc..
Rientrano tra gli enti pubblici:
- territoriali: Essi operano nell'ambito di un certo territorio ed hanno obiettivi istituzionali. Esempio: Stato, Regioni, Province, Comuni;
- istituzionali: Sono enti che, a differenza dei precedenti, non operano nell'ambito di un certo territorio. Essi hanno come scopo il soddisfacimento dei bisogni di particolari gruppi di individui o della collettività. Esempio: INPS, INAIL, Camere di Commercio, enti ospedalieri autonomi, università ecc..
- economici: Sono enti che esercitano un'impresa. In passato questa categoria di enti pubblici era piuttosto numerosa. Ad essa appartenevano ad essa l'IRI, l'ENI, la Cassa deposito e prestiti, ma successivamente sono stati successivamente trasformati in S.p.A. Esempio: un esempio di ente pubblico economico, attualmente, è dato dall'Istituto per il Credito Sportivo.
Per quanto riguarda il punto di vista legale, le imprese private possono far parte del processo penale, civile e amministrativo.
Mentre per l'ente pubblico può subire solamente un processo amministrativo.
Vedi altre domande riguardo il punto di vista legale.

16. Legal Data

Il dato giuridico è un elemento molecolare del complesso normativo che possiamo definire ordinamento giuridico. È una regola di:
• comportamento oppure
• di procedura oppure
• di qualificazione oppure
• un dato accessorio ad una o più delle predette regole
A seconda dei casi, il dato giuridico può essere di tipo penale, civile o amministrativo. Ci imbattiamo spesso in termini come illiceità (detta anche illecito), illegittimità, illegalità. Non sono equivalenti. L'illiceità ha ad oggetto un fatto commesso in violazione della legge penale (il reato) per cui è prevista una pena; o in violazione di un diritto del privato (l'illecito civile) per cui è previsto il risarcimento del danno. L'illegittimità ha ad oggetto un atto emesso in violazione della legge. L'illegalità esprime in modo generico la contrarietà di un fatto o di un atto alla legge o ad altre norme. Comprende dunque l'illiceità e l'illegittimità.
Criminal data:

Il dato criminale appartiene al settore dell'ordinamento definito criminale (in italiano penale). Deriva dalla "pena", ovvero la punizione inflitta a chi viola una norma penale. Ma quando è una norma criminale? Si tratta di quando sono previste una o più delle seguenti sanzioni per l'autore del reato: arresto, ammenda, carcere o ergastolo, multa.
I reati puniti con l'arresto e/o una ammenda sono definiti contravvenzioni. Quelli puniti con l'incarcerazione, l'ergastolo, la multa sono chiamati delitti. Tutti i reati, siano essi contravvenzioni o crimini, sono considerati reati. Nel settore penale gli antagonisti sono lo Stato, rappresentato dal pubblico ministero che formula l'accusa, e l'imputato, assistito dal suo avvocato. Il giudice, terzo ed imparziale rispetto ai due antagonisti, deciderà se accettare o meno la richiesta di punizione avanzata dal pubblico ministero nei confronti dell'imputato.
I dati penali:
Oltre alle sanzioni previste per coloro che commettono reati, definiamo penali tutti quei dati attraverso i quali viene accertata la responsabilità penale (dati investigativi) e provata davanti al giudice (dati probatori), si compiono gli atti del processo (dati procedurali), si eseguono le disposizioni del giudice (dati esecutivi). Sono anche dati penali quelli relativi alle persone indagate e alle vittime del reato, ai mezzi e alle circostanze del reato, al loro contesto sociale, ai mezzi giudiziari e tecnici di rilevazione e valutazione (sempre più raffinati nel campo delle prove digitali), ai criteri di validità degli atti del processo e alla loro usabilità. L'accertamento della responsabilità penale passa attraverso una serie di passaggi, corrispondenti alle fasi del processo:
• Indagini preliminari, condotte dal pubblico ministero
• processo, condotto dal giudice. Il giudice verifica la conformità degli atti procedurali alle norme. Puo' dichiarare:

- decadenza (a causa della scadenza del termine iniziale fissato dalla legge)
- l'inutilita (dovuta alla scadenza del termine finale stabilito dalla legge)
- la nullità (per violazione delle norme previste dalla legge come causa di nullità)

I dati civili:
Il settore civile è costituito dall'insieme di regole che regolano le relazioni private tra le persone, sia economiche che personali. Quando sorgono questioni in proposito, non esiste antagonismo tra lo Stato e una o più persone, come avviene nel settore criminale. L'antagonismo nasce tra soggetti privati, che possono anche essere enti pubblici quando agiscono a tutela di interessi privati. La decisione spetta al giudice, come sempre terzo tra le parti. Il processo civile è regolato dal principio di disponibilità. A differenza di quanto avviene in campo penale, dove il giudice interviene per autorità in caso di

violazione della legge, in campo civile è il soggetto leso nel suo diritto di decidere se citare in giudizio il responsabile. Le prove sono offerte dalle parti e il giudice, salvo eccezioni, non può cercarle o indicarle d'ufficio. Data la varietà delle materie che compongono il settore civile, i provvedimenti giudiziari civili sono di vario tipo. Il giudice può ordinare la restaurazione di un manufatto, la nullità di un contratto, la cessazione degli effetti civili del matrimonio e, più in generale, la cessazione di un rapporto giuridico, e così via. Nel settore
degli obblighi derivanti da
• un atto illecito (responsabilità extracontrattuale, ad esempio un incidente stradale)
• violazione del contratto (responsabilità contrattuale, ad es. errata esecuzione di un test di penetrazione)
Se il giudice accetta la richiesta della persona danneggiata, condanna il responsabile al risarcimento del danno.
I dati amministrativi:
Il dato è di tipo amministrativo quando è emesso o comunque riguarda una pubblica amministrazione nell'esercizio dei suoi poteri. Questa attività può essere:
• vincolata (se l'ente è tenuto per legge ad emettere il provvedimento)
• discrezionale (se la legge lascia all'ente la scelta se emettere o no il provvedimento).
Di solito la discrezionalità è normativamente orientata. La scelta se emettere o no il provvedimento non è rimessa al mero arbitrio dell'ente: esso valuta la situazione, e se questa lo richiede, deve emettere il provvedimento. Si può sintetizzare ciò con l'espressione: "L'ente deve, se è il caso". Nei procedimenti amministrativi, a differenza dei procedimenti penali e civili, l'oggetto della decisione non è il comportamento di un uomo o di un ente, ma una misura della pubblica amministrazione. Il giudice amministrativo non valuta se la misura è illegale ai sensi del diritto civile o penale, ma se è legale. Ciò significa che egli verifica se il provvedimento è stato emanato dall'organismo abilitato ad emetterlo e in conformità con i suoi poteri (controllo di legittimità), nonché nell'interesse pubblico (controllo di merito). A seguito di tale riesame, il tribunale amministrativo può confermare o annullare l'atto contestato. Essa può anche sospendere i suoi effetti in attesa della sua decisione.

17. Differenza dato/processo penale e civile, cos'è il reato

Differenza processo penale/civile: guarda 5 e 15.
Il reato è composto da due elementi base: la condotta tipica e la pena. Le pene previste dalla legge per le violazioni penali, dette pure reati, sono:
- Contravvenzioni: l'ammenda e l'arresto

- Delitti: la multa, la reclusione, civile, l'ergastolo
La pena prevista per ciascun reato ha un'importanza che va oltre la specificazione delle conseguenze penali a cui va incontro il trasgressore. Serve anche a classificare il reato. Se noi immaginiamo il reato come una classe, secondo la metodologia UML, ci accorgiamo che è una classe di collegamento fra 3 classi che sono: il soggetto, la norma penale e il fatto. Se noi diciamo "il luogo del reato", "il tempo" sono attributi del fatto, invece la punizione è un attributo della norma.

18. PDND

La Piattaforma Nazionale Dati Digitali (PDND) ha lo scopo di estendere alla Pubblica Amministrazione i vantaggi offerti dalle moderne piattaforme per la gestione e l'analisi dei big data.
In particolare, si propone di:
• sviluppare e semplificare lo scambio dei dati pubblici tra le pubbliche amministrazioni;
• promuovere la diffusione del riutilizzo dei dati;
• ottimizzare i processi di analisi dei dati e di generazione della conoscenza.

Il PDND si basa su una piattaforma per big data, composta da:
• un data lake (archiviazione delle banche dati istituzionali della PA e dei dati generati dai sistemi informativi delle pubbliche amministrazioni sotto forma di log);
• un insieme di motori di dati (per armonizzare ed elaborare i dati grezzi memorizzati nel data lake e per implementare modelli di apprendimento automatico);
• strumenti per la comunicazione dei dati (per facilitare l'utilizzo dei dati elaborati da parte degli stakeholder).

19. Vocabolari controllati

Si tratta di vocabolari normalizzati i cui elementi in modo univoco denotano contenuti concettuali specifici per evitare sovrapposizioni equivoche e facilitare la ricerca. Questi elementi si riferiscono anche ai metadati che vengono elaborati dal modello dei dati.
Ad esempio vediamo tre modelli di dati semplificati ed estensibili:
1. Location Vocabulary: include le caratteristiche fondamentali di un luogo, rappresentato come indirizzo, nome geografico o rappresentazione geometrica;
2. Person vocabulary: include le caratteristiche fondamentali di una persona, ad esempio il nome, il sesso, la data di nascita, ecc;

3. Business vocabulary: include le caratteristiche fondamentali di una persona giuridica, ad esempio la denominazione legale, l'attività, l'indirizzo, il manager/direttore, il tipo di azienda e le sue attività.

20. LCA (in particolare eliminazione nel caso di documenti importanti)

LCA è l'acronimo di Life Cycle Assessment (valutazione del ciclo di vita). La norma ISO 14040: 2018 mira a definire i principi e il quadro di riferimento per il Life Cycle Assessment. Essa considera, tra le altre cose, le seguenti fasi:
• definizione dell'obiettivo e dell'ambito di applicazione della LCA;
• analisi dell'inventario del ciclo di vita (LCI) - fornisce informazioni su tutti gli input e gli output sotto forma di flusso elementare da e verso l'ambiente da tutti i processi unitari coinvolti nello studio;
• interpretazione del ciclo di vita - tecnica per identificare, quantificare, controllare e valutare le informazioni provenienti dai risultati dell'inventario del ciclo di vita e/o della valutazione dell'impatto del ciclo di vita (da quello che abbiamo valutato quali conclusioni possiamo trarre? identificare, quantificare, controllare, valutare, che cosa? Le informazioni che sono il risultato dell'inventario dopo aver valutato l'impatto interrogando le informazioni che provengono dall'inventario e valutate - la valutazione è il giudice del dato);
• reporting e revisione critica della LCA - processo per verificare se una LCA ha soddisfatto i requisiti per la metodologia, i dati, l'interpretazione e il reporting e se è coerente con i principi (devo verificare se la valutazione del ciclo di vita ha soddisfatto i requisiti di metodologia, la revisione è il giudice della valutazione).
Eliminazione di un documento importante non pervenuta.

21. Che cosa sono gli interessi legittimi

Rispetto ad un provvedimento amministrativo che lo danneggi, il cittadino può far valere in giudizio un interesse legittimo. Qui dobbiamo capire bene la differenza tra l'interesse legittimo e l'essere titolari di un diritto. Ma attenzione: essere titolari di un interesse legittimo non significa essere titolari di un diritto. Qual'è la differenza? Il diritto è una situazione giuridica che il soggetto può far valere nei confronti di chicchessia, ivi compresa la pubblica amministrazione. L'interesse legittimo ha ad oggetto un provvedimento della pubblica amministrazione che danneggia il cittadino, senza ledere tuttavia un suo diritto. Prendiamo ad esempio l'espropriazione. Se lo Stato espropria il mio frutteto io subisco una doppia lesione giuridica. Come proprietario ho diritto ad un indennizzo corrispondente al valore del mio frutteto. Non ho però il diritto di impedire l'espropriazione, rientrando essa nei poteri dello Stato. Rispetto all'espropriazione posso far valere solo un interesse legittimo. Ma che significa ciò in concreto? Cosa posso fare in quanto titolare di un interesse legittimo?

Il titolare dell'interesse legittimo può impugnare il provvedimento davanti al Tribunale Amministrativo Regionale e chiederne l'annullamento, sostenendo di avere interesse a impugnare perché quel provvedimento gli ha causato un danno. Ma ciò non basta. L'interesse a impugnare è il primo di tre requisiti. Vediamo gli altri due:
• il provvedimento deve essere illegittimo;
• il provvedimento deve essere contrario all'interesse pubblico.

22. Eccesso di potere

L'eccesso di potere è un vizio di legittimità dell'atto amministrativo che si manifesta nel cattivo uso del potere da parte della Pubblica amministrazione o nella deviazione del potere da quei principi generali stabiliti dal legislatore, come la correttezza, la buona fede o la diligenza.

23. Norma giuridica

Sono leggi che tendono a regolare i rapporti fra i soggetti di un'organizzazione sociale, definiscono i confini dei rispettivi interessi, individuano e tutelano i beni e valori ad essi comuni. Il mancato adempimento alla regola prevede una sanzione di tipo amministrativo, civile o penale.
Le norme non giuridiche pongono solo doveri moralmente corretti, che rientrano nei buoni usi e costumi sociali.
Esempio parcheggio in divieto di sosta -> multa. Sull'autobus ci stanno i posti per gli handicappati ma non lo faccio sedere -> non multa, ma sei un maleducato.

24. Querela

La querela è una istanza con cui la persona offesa dal reato chiede la punizione del colpevole. Viene presentata alla polizia giudiziaria o al pubblico ministero, a pena di decadenza, entro novanta giorni dal fatto o dalla conoscenza di esso.

25. Risk management planning

RMP: 1 - Identificazione dei rischi
L'identificazione del rischio comprende le seguenti fasi:
• Registro dei rischi (l'elenco dettagliato dei rischi più importanti e probabili in relazione alla natura del progetto)
• Struttura di suddivisione dei rischi (suddivisione dei rischi in categorie per una migliore organizzazione degli interventi)
• Analisi dei rischi (le sue fasi sono: identificazione dei rischi, analisi della loro probabilità e del loro impatto).

RMP: 2 - Assegnazione di priorità ai rischi
In questa fase si elaborano i risultati della fase precedente e si procede a classificare i rischi, in base alla loro gravità. Ciò consente la creazione di matrici di rischio. Se vengono identificati rischi di pari gravità si ricorre a metodi suppletivi di classificazione o, in ultima analisi, al senso comune. E' in questo campo che si misurano le capacità del manager. Egli infatti tiene conto di parametri non facilmente misurabili, quali il rischio di immagine per l'azienda, le prospettive di mercato, i buoni rapporti commerciali, e via dicendo.

RMP: 3 - Misure in caso di rischio
Le misure da adottare nel caso il cui l'evento di danno che è oggetto del rischio si verifica possono essere schematicamente indicate come segue:
• Evitare - Eliminare la minaccia eliminando la parte o la funzionalità del progetto che è stata attaccata.
• Trasferire - Trasferire gli effetti dannosi del rischio su terzi, come ad esempio stipulare un contratto assicurativo o emettere un performance bond;
• Mitigare - Ridurre la gravità dell'evento di rischio, attenuando le sue conseguenze con misure adeguate a tal fine.
• Accettare - Accettare la verificazione dell'evento di danno quando la perdita stimata non è sufficiente a giustificare la spesa da sostenere per evitarlo. Nota pure come "risk retention".

RMP: 4 - The Performance Bond
Il Performance Bond è la garanzia del committente contro il rischio di inadempimento totale o parziale dell'appaltatore nell'esecuzione dei lavori. È emesso da un istituto di credito. In caso di inadempimento dell'Appaltatore, il Committente potrà richiedere alla banca garante il pagamento della somma di denaro da lui indicata a titolo di pagamento per lavori non eseguiti.
Ciò costituisce una fonte di rischio per l'appaltatore, che può essere soggetto a pagamento anche in caso di malafede da parte del cliente, il quale, per ottenere il denaro in garanzia, non deve provare l'effettivo inadempimento. Il Performance Bond può anche essere emesso non da una banca ma da una società appartenente al gruppo dell'appaltatore. In questo caso si può stabilire che il garante, invece di pagare una somma di denaro, esegue i lavori non ultimati dall'appaltatore.

26. Incidente probatorio e in generale indagini preliminari

Il procedimento penale, oltre al processo, comprende anche una fase che precede l'avvio del processo, detta fase delle indagini preliminari. Queste sono

condotte dal Pubblico Ministero (PM). Le indagini preliminari e il processo, unitariamente considerati, costituiscono il procedimento penale.
Le indagini preliminari prendono avvio dalla notizia di reato trasmessa da un organo di polizia giudiziaria (PG) al Pubblico Ministero (PM). Ma questi può acquisire la notizia di reato anche direttamente . La notizia di reato può altresì provenire dalla querela della persona offesa o dalla denuncia di un privato.
Nel corso delle indagini preliminari il Pubblico Ministero, avvalendosi della collaborazione della Polizia Giudiziaria, raccoglie elementi atti a individuare il responsabile, a ricostruire le modalità e circostanze del fatto criminoso, ad assicurare le fonti di prova
Gli Atti di anticipazione del processo sono quegli atti che, per ragioni di urgenza, vengono compiuti nel corso delle indagini preliminari con le garanzie tipiche del dibattimento, sotto la direzione del Giudice per le Indagini Preliminari (GIP). Essi sono:
• L'Incidente probatorio: Se è noto in anticipo che l'atto è irripetibile, si attiva una speciale procedura, detta incidente probatorio (art. 392 c.p.p.) davanti al GIP, che procede all'esame della prova con l'osservanza delle stesse garanzie di difesa previste dalla legge per il dibattimento.
• L'accertamento tecnico non ripetibile: Gli atti di indagine compiuti dal P.M. non sono prove utilizzabili a carico dell'imputato, bensì elementi la cui sussistenza e fondatezza dovranno essere dimostrate davanti al giudice del dibattimento. Ciò vale anche per le indagini difensive compiute dal difensore. Fanno eccezione a questa regola gli atti irripetibili compiuti dal pubblico ministero, che entrano nel processo in quanto prove. Sono atti irripetibili ad esempio, gli accertamenti su fonti di prova deperibili, come gli alimenti, o quelli divenuti irripetibili per sopravvenuta impossibilità di ripetizione (dichiarazioni di persona successivamente deceduta).
Qual'è la differenza? L'accertamento tecnico non ripetibile è disposto in via esclusiva dal pubblico ministero invece l'incidente probatorio può essere richiesto sia dal p.m. che dall'indagato oltre che dalla parti lese ed è disposto dal gip. In realtà nonostante il contraddittorio si svolga esplicitamente nell'udienza dell'incidente probatorio, anche nell'accertamento irripetibile non vengono comunque negate le garanzie in quanto l'indagato può nominare un perito di fiducia per il confronto.

27. Qualità dei dati: Requisito sintattico, Requisito semantico, Requisito pragmatico (x2)

ISO 8000 è un'importante standard internazionale per la misurazione delle informazioni relative alla qualità dei dati: qualità sintattica, qualità semantica e qualità pragmatica.

Qualità sintattica:
La qualità sintattica richiede che i dati siano conformi alla sintassi di riferimento, cioè all'insieme di regole che i dati devono osservare per confrontarsi al proprio modello. Queste regole sono strutturate attraverso i requisiti indicati dai metadati. Questi includono:
• valori legali, solitamente definiti in un lessico di riferimento denominato "profilo"; (per un valore del profilo è scritto da 1 a 7 ed io metto 8 quello è un dato/valore illegale);
• integrità referenziale dei dati: tale requisito che richiede che le relazioni tra tabelle debbano essere sempre coerenti. In altre parole, qualsiasi campo chiave esterno deve concordare con la chiave primaria a cui fa riferimento la chiave esterna;
• vocabolario aziendale: insieme di definizione utilizzate per descrivere entità, relazioni, processi all'interno dell'azienda;
• qualsiasi altra regola definita nel contesto del sistema.;

Qualità semantica:
L'espressione qualità semantica indica la corrispondenza di significato tra il dato e la realtà che rappresenta. Un dato ha una qualità semantica ottimale quando questa corrispondenza è piena. Si pensi a una tavola dei colori in cui l'etichetta "rossa" corrisponde a un rosso pallido, accanto al rosa. In questo caso siamo in presenza di una cattiva qualità semantica di quel dato.
In ascensore capita spesso che si prema il pulsante due e si va al piano terra, ma spesso ci si trova d'innanzi in cui il piano terra viene indicato con la T, o con 0 o con 1, e questo crea disordine incidendo negativamente alla qualità del dato.

Qualità Pragmatica:
La misurazione della qualità pragmatica consente di accertare se i dati trattati dal sistema sono:
• idonei, cioè idonei al raggiungimento degli obiettivi del sistema, in corrispondenza del business plan;
• utili, cioè se sono considerati tali nella percezione degli utenti del servizio.
Prendo una linea di cioccolatini ma in questi cioccolatini metto una faccia di una persona triste, che intristisce colui che dovrebbe compare, oppure uno scarafaggio che sarebbe orribile a vedersi da chi si accinge a mangiare il cioccolato. Allora a questo punto il dato in questo caso non sarebbe idoneo al raggiungimento degli obiettivi di sistema. Un dato non è idoneo quando non ha presa, non riesce a modificare la situazione.

28. Dati Personali: Cosa sono i dati identificativi, Dati sensibili (x5)

All'interno della tipologia possiamo trovare una distinzione importante tra dati personali (che dall'entrata in vigore del GDPR comprendono anche quelli delle istituzioni e delle persone giuridiche, oltre a quelli delle persone fisiche) e gli altri tipi di dati. In Italia, la protezione giuridica dei dati è regolata dal Decreto Legislativo n. 196 del 2003 (Codice della Privacy) e dal GDPR. Cos'è un dato personale? Secondo il GDPR è qualsiasi informazione relativa a una persona fisica, persona giuridica, entità o associazione, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, compreso un numero di identificazione personale. Tra i dati personali vengono considerati:

• Dati di identificazione (consentono l'identificazione)
• Dati Giudiziari (status dell'indagato o imputato, condanne, sanzioni ecc.)
• Dati Sensibili

Sono considerati dati sensibili:

• l'origine razziale ed etnica
• credenze religiose, filosofiche ecc.
• opinioni politiche, appartenenze a partiti, associazioni ecc.
• stato di salute e vita sessuale

N.B. Il trattamento dei dati sensibili NON può essere applicato per analogia ad altri tipi di dato (i dati sensibili costituiscono un numero chiuso).

Per quanto riguarda il trattamento dei dati sensibili, il Codice Privacy distingue a seconda che il trattamento sia svolto da soggetti privati o da soggetti pubblici. Nel primo caso (soggetti privati) i dati possono essere trattati solo con il consenso scritto dell'interessato e previa autorizzazione del Garante.
Nel caso di soggetti pubblici il trattamento dei dati sensibili è consentito "solo se autorizzato da espressa disposizione di legge".

29. Risk management: quali rischi ci possono essere e come evitarli

I rischi considerati dal GDPR possono essere suddivisi in due grandi categorie:

1. Rischi per la persona:
    a. se il trattamento può comportare discriminazione, furto, danno alla reputazione, perdita della riservatezza o qualsiasi altro danno economico o sociale significativo;
    b. se l'interessato rischia di essere privato dei propri diritti e libertà;
    c. se sono trattati dati personali che rivelino l'origine razziale o etnica;
    d. in caso di valutazione di aspetti personali, riguardanti la prestazione professionale, la situazione economica, la salute;

e. per creare o utilizzare profili personali;
f. se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori;
g. se il trattamento riguarda una quantità significativa di dati personali e un numero elevato di persone.

2. Rischi per il sistema:
   a. Organizzativi: Tali rischi sono strettamente dipendenti dall'organizzazione aziendale, sia per quanto riguarda le dinamiche aziendali sia per quanto riguarda la politica aziendale. Tra le misure suggerite:
      i. Formazione continua dei professionisti del settore;
      ii. Sistemi di autenticazione attraverso credenziali uniche, evitando account condivisi, con procedure di creazione e cancellazione delle password ben definite;
      iii. Un'adeguata gestione degli account utente
   b. Tecnici: Il rischio tecnico è la conseguenza del guasto o malfunzionamento di un sistema, della sua funzionalità o di uno dei suoi componenti, che si discostano dal risultato atteso. La mancata previsione e identificazione o gestione di queste minacce espone il sistema a gravi vulnerabilità. Una corretta gestione deve basarsi su precauzioni proattive, manutenzione costante, diagnosi tempestive e affidabili e riparazioni tempestive

30. Privacy by design e by default

Privacy by design:
Questo principio è stabilito nel primo comma dell'articolo 25 del GDPR e intende tutelare la privacy fin dalla progettazione del sistema che tratterà poi i dati. In quest'ottica, aziende e pubbliche amministrazioni devono proteggere dati con un approccio proattivo anziché reattivo (previeni e non correggere), predisponendo fin dall'inizio misure di sicurezza a tutela della privacy. Questo principio si basa su:
• previeni piuttosto che correggere
• la privacy è integrata nel progetto iniziale
• massima funzionalità (la privacy non è una causa di minore sicurezza)
• sicurezza garantita per tutto il ciclo di vita del servizio
• visibilità e trasparenza del trattamento
• centralità dell'utente
Privacy by default:
Questo principio è definito nel secondo comma dell'articolo 25 del GDPR e limita il trattamento di default di dati personali necessari per le finalità del

progetto. Di fatto la durata della conservazione e la quantità di dati raccolti non può superare lo stretto necessario. Da questo principio ne consegue che:
• la protezione dei dati personali deve essere fissata in modo da rispettare i principi generali della protezione della privacy
• i dati devono essere ridotti al minimo
• le finalità del trattamento fungono da limite oltre il quale non si possono più usare i dati
• i dati possono essere accessibili ai soli utenti dei servizi

31. Open data

La direttiva OPEN DATA è la direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio del 20 giugno 2019 sugli open data e il riutilizzo delle informazioni del settore pubblico. Essa fornisce un quadro giuridico comune per un mercato europeo dei dati detenuti dai governi (informazioni del settore pubblico). Si basa su due pilastri fondamentali del mercato interno: trasparenza e concorrenza leale. L'obiettivo della direttiva Open Data è quello di rendere riutilizzabili i dati del settore pubblico e quelli finanziati con fondi pubblici. A questo scopo la direttiva si concentra sugli aspetti economici (licenze, prezzi, ecc.) del riutilizzo delle informazioni piuttosto che sull'accesso alle informazioni da parte dei cittadini. Essa incoraggia gli Stati membri a rendere disponibile il maggior numero possibile di informazioni da riutilizzare. Ciò evidenzia ancora una volta la tendenza a trattare i dati come beni e a metterli in circolazione per il loro uso economico.
Perché questi dati sono chiamati "aperti"?
- sono disponibili sulla base di una licenza che ne consente l'uso da parte di chiunque, anche a fini commerciali, in un formato disaggregato;
- sono adatti all'uso automatico da parte di programmi per computer e sono forniti con i loro metadati;
- sono resi disponibili gratuitamente o ai costi marginali sostenuti per la loro riproduzione e divulgazione, salvo casi eccezionali.
In due parole: il riutilizzo dei dati, anche a fini commerciali, da parte degli stakeholder.

32. Inspire

INSPIRE è una direttiva del Parlamento europeo e del Consiglio (2007/2/CE del 14 marzo 2007). Il suo nome è l'acronimo di Infrastruttura per l'informazione territoriale in Europa. L'obiettivo del progetto è quello di creare un quadro giuridico per la costruzione e l'attivazione di un'infrastruttura per l'informazione territoriale in Europa, al fine di formulare, attuare, monitorare e valutare le politiche comunitarie a vari livelli e fornire informazioni ai cittadini. Ciò dovrebbe

rendere disponibili un maggior numero di dati e di qualità superiore per lo sviluppo delle politiche comunitarie e la loro attuazione negli Stati membri. La direttiva si concentra in particolare sulla politica ambientale, ma è prevista la sua applicazione ad altri settori come l'agricoltura, i trasporti e l'energia. L'infrastruttura INSPIRE, a livello europeo, comprende le infrastrutture dei dati territoriali nazionali dei paesi dell'Unione, che a loro volta coordinano quelle del livello subnazionale. Tutte le infrastrutture del sistema sono organizzate secondo le regole della direttiva INSPIRE. Esse riguardano, in particolare, l'armonizzazione dei dati, i servizi di accesso ai dati, i modelli di interoperabilità, gli obblighi e le modalità di condivisione dei dati tra le pubbliche amministrazioni.
Ciascuna delle infrastrutture di dati territoriali nazionali costituirà un "nodo" dell'infrastruttura europea e
dovrà essere resa disponibile:
• dati
• metadati
• servizi
In due parole: la condivisione dei dati tra le pubbliche amministrazioni a titolo gratuito, per i loro scopi istituzionali.

33. Metadati

I metadati si distinguono dai dati per il fatto che sono "dati sui dati", cioè informazioni sui requisiti strutturali di un gruppo omogeneo di dati, che nella gerarchia delle informazioni sono posti a un livello superiore. Poiché contengono informazioni generali sui dati sottostanti, consentono l'indicizzazione e la ricerca. Ad esempio, sono metadati quelli riguardanti le caratteristiche generali dei sistemi dell'organismo umano (respiratorio, cardiovascolare, ecc.). In ambito IT possiamo distinguere i seguenti tipi di metadati:
1. metadati descrittivi: descrivono il contenuto del documento. Sono utilizzati per l'identificazione e il recupero di oggetti digitali. Sono esterni all'archivio digitale, al quale sono collegati tramite appositi link. Normalmente costituiscono le banche dati dei sistemi di recupero delle informazioni;
2. metadati di gestione: riguardano le modalità di conservazione e manutenzione degli oggetti digitali nel sistema di gestione degli archivi digitali. Possono contenere informazioni sui diritti d'accesso, su modalità e data della eliminazione, del responsabile dei file.
3. metadati strutturati: descrivono la struttura interna dei documenti e gestiscono la relazione interna tra i loro componenti. Inoltre, forniscono i dati di identificazione e localizzazione del documento, come il codice identificativo,

l'indirizzo del file sul server, l'archivio digitale a cui appartiene e il suo indirizzo Internet.
Metadata Encoding and Transmission Standards: È un contenitore basato su uno schema XML in cui sono registrati diversi sistemi di codifica dei dati.
Svolge funzioni finalizzate alla conservazione digitale. In particolare:
• Creare istanze di documenti XML che descrivono la struttura gerarchica degli oggetti della libreria digitale;
• Registrare i nomi e le posizioni dei file che includono tali oggetti;
• Registrare i metadati associati.
Libreria digitale, oggetti della libreria digitale, gerarchia tra gli oggetti della libreria digitale, descrizione di questa struttura gerarchica, in che modo? chi opera questa descrizione? Lo fanno istanze di documenti XML.

34. Ciclo di vita del dato

La durata del dato, dal momento della sua produzione a quello della sua eliminazione, rappresenta il suo ciclo di vita:

1. DLC - Data production: Il produttore dei dati non è l'operatore incaricato di inserirli in un database, ma colui che dà forma ad una unità elementare di conoscenza trasformandola in un dato. A questo punto il dato può essere tout court inserito in un insieme di dati o, come più frequentemente accade, classificato in una tassonomia.

2. DLC - Data selection and collection: Includono i seguenti passaggi:
• l'analisi delle finalità dei dati (a cosa i dati mi servono);
• il controllo della qualità dei dati (butto via quello che non mi serve e tengo solo quello che mi serve, quelli di qualità s'intende);
• la selezione dei soli dati necessari per le finalità prestabilite (vedere i singoli passaggi dell'attività aziendale per selezionare i dati che mi servono per quello specifico processo);
• la verifica della liceità della raccolta dei dati;
• l'informativa agli interessati delle finalità e modalità del trattamento, ottenendo il loro consenso quando necessario.

3. DLC - Data storage: I dati devono essere archiviati nella tassonomia di sistema per evitare errori nelle procedure relazioni e con modalità che ne permettano l'immediata identificazione e disponibilità, evitando allo stesso tempo interferenze con dati simili. Una buona pratica per la corretta conservazione dei dati è la loro minimizzazione, da effettuarsi con adeguate misure di sicurezze fisiche, logiche ed organizzative. La legge richiede al

gestore dei dati personali di indicare il periodo della loro conservazione o, se ciò non è possibile, i criteri utilizzati per determinare tale periodo. Questa minimizzazione deve essere accompagnata da misure di sicurezza fisiche (riguardanti l'accesso al macchinario, al server, dove i dati sono immagazzinati) logiche (rapporto tra i dati e quando vengono messi in circolo nel sistema di dati) ed organizzative (tassonomia del sistema a cui i dati si riferiscono, come i dati di vendita devono essere separati dai dati di acquisti).

4. DLC - Data protection: Il dato deve essere protetto da attacchi esterni ma anche dai possibili guasti interni ecco perché abbiamo detto che la qualità del dato è un elemento che ha a che fare direttamente con la sua protezione perché evita dei rischi.
L'oggetto è costituito essenzialmente dagli elementi base della sicurezza informatica: la Confidenzialità, Integrità e l'Availability (disponibilità). Questi devono essere aggiornati e protetti con adeguate misure di sicurezza.
È necessaria inoltre la valutazione dei rischi a cui i dati sono esposti durante la loro gestione.

5. DLC - Data utilization: la prima questione è chi può usare il dato?
- è necessario identificare quali soggetti saranno gli utenti dei dati e accertare chi li utilizza effettivamente;
- è necessario stabilire i diritti di accesso, la loro estinzione, le modalità di esercizio e le relative responsabilità;
- inoltre è necessario comunicare preventivamente agli interessati le modalità di gestione.

6. DLC - Data deletion:
L'eliminazione dei dati dipende essenzialmente da uno dei seguenti fattori:
1. La cessazione dell'utilità dei dati per il raggiungimento dello scopo per il quale i dati sono stati creati o per mancanza di interesse per tale raggiungimento o per impossibilità di realizzarlo;
2. Il dovere legale di cancellazione, soprattutto con riferimento ai dati personali, secondo quanto previsto dal GDPR;

La cancellazione dei dati comporta un'attività di preparazione:
• identificazione di tutti i dati in possesso e della loro ubicazione; (quali sono i dati da distruggere e dove si trovano);
• identificazione dei soggetti che hanno accesso ai dati memorizzati nel sistema; (chi li possiede);

• attivazione di una strategia di distruzione dei dati condivisa che tenga conto dei supporti, dei processi coinvolti, delle aree di competenza e del business; (la strategia non è solo lo scopo è l'insieme dei mezzi che io metto in campo per raggiungere questo scopo, e qui mi trovo i supporti dei dati)
• comunicazione della fase di cancellazione dei dati a tutti i dipendenti e collaboratori;
Esistono due modalità di distruzione dei dati: NIST 800-88 e LCA - ISO 14040.

35. Attributi del dato: granularità del dato (informazione -> dati -> attributi)

La struttura molecolare dei dati produce la granularità della conoscenza. Poniamo che il mio cappotto sia grigio. «Grigio" è un attributo di "cappotto", quindi una delle sue componenti atomiche. Ma il colore grigio in quanto tale è un dato, e quindi un'entità molecolare, che può essere scomposta nelle sue componenti atomiche (per esempio, la gradazione). La gradazione, a sua volta, considerata di per sé, è un'entità molecolare con propri attributi atomici (per esempio, l'intensità). E così via.
Ciò significa che i dati, in quanto entità molecolari, possono essere scomposti in modo granulare e poi ri-aggregati all'interno di reti e di reti di reti, secondo modelli adatti a rappresentare la complessa rete della conoscenza universale (episteme).

36. Giudizio civile vs penale

I gradi di giudizio sono identici.
Giudizio Penale:
Conclusasi la fase delle indagini preliminari, l'indagato, se portato a processo, prende il nome di imputato. Il giudice, dopo avere sentito entrambe le parti, i testimoni, i periti e avere esaminato i mezzi di prova, emette la sua decisione. Essa è:
• una sentenza di condanna, se ritiene l'imputato colpevole;
• una sentenza di assoluzione, se ritiene l'imputato innocente.
Dopo la condanna, l'imputato prende il nome di condannato.
Giudizio civile:
L'antagonismo nasce tra soggetti privati, che si rivolgono al giudice per risolvere la loro vertenza. Di solito è un soggetto, detto attore, che si rivolge al giudice perché emetta una decisione nei confronti del suo antagonista, detto convenuto. Il convenuto respinge la pretesa dell'attore, sostenendo le proprie ragioni (eccezioni), o avanzando a sua volta una pretesa contro l'attore (riconvenzione). Ma possono pure essere entrambe le parti a rivolgersi congiuntamente al giudice. Un ente pubblico può essere l'attore o il convenuto

in un processo civile, quando agisce da privato, ad esempio stipulando un contratto di fornitura o prendendo in locazione un immobile. Nel processo civile l'onere della prova spetta all'attore, non al convenuto. Questo onere spetta al convenuto limitatamente alle eccezioni e alle pretese avanzate contro l'attore in via riconvenzionale.

37. Rischio giuridico di un'impresa (va comunicato entro 72h)

Sebbene il GDPR non faccia espressamente riferimento al penetration test, tale verifica appare oggi indispensabile, tenuto anche conto del fatto che l'articolo 33 di tale regolamento impone agli stessi soggetti l'obbligo di notificare le violazioni subite dal proprio sistema entro 72 ore. I test di vulnerabilità, segnalando il rischio di possibili attacchi, consentono all'azienda di attrezzarsi per prevenirli, evitando danni all'immagine dovuti all'annuncio pubblico di divulgazione delle violazioni. Inoltre, il GDPR prevede pesanti sanzioni per le organizzazioni che subiscono violazioni della sicurezza dei propri sistemi, prevedendo sanzioni fino a 20 milioni di euro, ovvero il 4% del fatturato annuo mondiale, a seconda di quale sia il maggiore.

38. Penetration Test

L'articolo 32 del GDPR impone al titolare e al responsabile del trattamento l'obbligo di testare l'efficacia delle misure tecniche e organizzative atte a garantire la sicurezza del sistema informatico.
Metodi per eseguire il Pentest: scatola nera, bianca e grigia.

Alla fine del test, i risultati vengono analizzati in base a questa sequenza:
• identificazione dell'architettura e dei servizi
• elenco degli errori principali e dei problemi critici
• raccolta di prove che certificano l'esistenza dei problemi individuati
• riepilogo esecutivo, che contiene sia l'analisi dell'impatto sui rischi che la tempistica per la soluzione o la mitigazione dei problemi evidenziati dall'analisi
• relazione tecnica, che contiene un'analisi dettagliata dei risultati e delle soluzioni tecniche proposte per eliminare o mitigare le questioni critiche.

Il test di penetrazione viene effettuato con il consenso della società che gestisce il sistema da testare e comporta la firma di un accordo commerciale con il team incaricato di eseguire il test.
L'accordo è stipulato con un contratto scritto le cui clausole, come vedremo, sono molto importanti perché regolano la responsabilità civile di entrambe le parti in relazione agli obblighi e ai diritti derivanti dal contratto.

Inoltre, il mancato rispetto di alcune clausole può comportare la responsabilità penale dei tecnici che eseguono il Pentest.

39. Modalità Penetration test: (black, grey, white box)

Ci possono essere diversi modi per eseguire il pen test:
• scatola nera: l'esecutore del test non ha ottenuto dall'azienda alcuna informazione preliminare sull'infrastruttura, quindi prima dell'analisi ha bisogno di determinare l'architettura dei servizi del sistema;
• scatola bianca: l'esecutore del test ha ottenuto informazioni dettagliate su infrastruttura, schemi di rete, codice sorgente dell'applicazione, elenchi di indirizzi IP presenti nella rete
• scatola grigia: varianti alle suddette metodologie.
I metodi black and white box possono simulare attacchi sia esterni che interni; il metodo della scatola grigia generalmente simula quello di un dipendente malintenzionato.

40. Diligenza (buon padre di famiglia)

È possibile che sia l'operatore che il gestore del sistema inseguono di responsabilità civile a causa di un fatto illecito che ha danneggiato l'altra parte, o per aver violato le regole del contratto di prova di penetrazione. Di seguito sono riportate alcune regole del codice civile che possono essere prese in considerazione:
Art. 1176 (Diligenza nel rispetto):
Nell'adempiere l'obbligazione il debitore deve usare la diligenza del buon padre di famiglia.
Nell'adempimento delle obbligazioni inerenti all'esercizio di un'attività professionale, la diligenza deve valutarsi con riguardo alla natura dell'attività esercitata.

41. Responsabilità extracontrattuale: (i danni vanno pagati)

11.6.2.3 Art. 1218 l.c.c. Responsabilità del debitore:
Il debitore che non esegue esattamente la prestazione dovuta è tenuto al risarcimento del danno, se non prova che l'inadempimento o il ritardo è stato determinato da impossibilità della prestazione derivante da causa a lui non imputabile
11.6.2.4 Art. 1223 l.c.c. Risarcimento dei danni:
Il risarcimento del danno per l'inadempimento o per il ritardo deve comprendere così la perdita subita dal creditore come il mancato guadagno, in quanto ne siano conseguenza immediata e diretta
11.6.2.5 Art. 1225 l.c.c. Prevedibilità dei danni:

Se l'inadempimento o il ritardo non dipende dal dolo del debitore, il risarcimento è limitato al danno che poteva prevedersi nel tempo in cui è sorta l'obbligazione.

42. Segreti: x2 (Di stato/militare x2, D'ufficio, Epistolare…)

La legge italiana prevede i seguenti tipi di segreto, ognuno dei quali regolato da una norma specifica:

• Segreto di Stato

Con questo nome la legge 801 del 1977 aggrega il segreto politico e il segreto militare e riguarda cose, informazioni (anche contenute in atti di Governo) e documenti che devono essere tenute segrete per la sicurezza o per l'interesse politico dello Stato.

• Segreto d'ufficio

Disciplinato dall'articolo 326 c.p. il quale afferma che il pubblico ufficiale e l'incaricato di un pubblico servizio sono tenuti a non divulgare e a non utilizzare le informazioni del proprio ufficio che devono rimanere segrete. La condotta incriminata dalla legge può essere di due tipi:

– Rivelazione di segreti

– Uso di informazioni segrete per procurare profitto (al pubblico ufficiale o a terzi)

• Segreto professionale

Disciplinato dall'articolo 622 c.p. afferma che chiunque a causa della sua professione venga a conoscenza di un segreto e lo riveli senza giusta causa oppure lo usi per trarne profitto personale (o per terzi) è punito con la reclusione fino ad un anno.

• Segreto industriale

Disciplinato dall'articolo 623 c.p. afferma che chiunque a causa della sua professione venga a conoscenza di un segreto riguardante una scoperta/invenzione scientifica o un'applicazione industriale e lo riveli o lo usi per trarne profitto è punito con la reclusione fino a due anni.

• Segreto del documento

Disciplinato dall'articolo 623 c.p. afferma che chiunque riveli senza giusta causa o impieghi per il proprio profitto o altrui il contenuto di atti o documenti, pubblici o privati, purché non si tratti di corrispondenza postale di cui è venuto a conoscenza, è punito con la reclusione fino a due anni.

• Segreto epistolare

Disciplinato dall'articolo 616 c.p. il quale punisce chiunque prenda atto di una lettera chiusa a lui non indirizzata, o la rubi per farla conoscere ad altri, o la distrugga. Ma è disciplinato anche dall'articolo 618 c.p. che punisce la condotta

di chi, venuto a conoscenza illegalmente del contenuto di una corrispondenza postale che doveva rimanere segreta, la rivela senza giusta causa, se il fatto arreca danno. E infine dall'articolo 620 c.p. che punisce la condotta dell'impiegato del servizio postale che, venuto a conoscenza, in ragione del suo ufficio, del contenuto di una lettera o di un telegramma aperto, lo rivela ad una persona diversa dal destinatario.

43. Dato segreto vs Dato Pubblico vs dato clandestino (intranei, stranieri, informazione, regola di segretezza)

Le interazioni sociali si basano sullo scambio di informazioni e dati che costituisce la conoscenza condivisa dalla comunità. Tuttavia non sempre le informazioni possono essere condivise in un circuito pubblico (il numero di persone che sanno qualcosa è alto → il rischio di divulgazione si alza). Si dice che le informazioni che non si vogliano o non si debbano comunicare siano segrete. Di fatto nessuna informazione è completamente segreta altrimenti si chiamerebbe mistero.
Qualsiasi informazione che non deve essere di pubblico dominio deve avere questi elementi:
• I conoscitori (Connoisseur) → interni
• I soggetti esclusi → esterni
L'obbligo di segretezza consiste nel NON comunicare informazioni possedute dai conoscitori a soggetti esclusi (quindi interno non implica esterno).
Infine ci troviamo in presenza di informazioni clandestine qualora l'informazione stessa e il fatto che sia segreta è un segreto.
Normalmente il segreto non esiste, o meglio, è un concetto relativo a qualcosa, a qualcuno o al contesto in cui nasce. Tuttavia esistono segreti imposti dalla legge che implicano un impedimento legale alla conoscenza. In questo caso avremo:
• Soggetto che è a conoscenza di...
• Soggetto escluso
• Ciò che è conosciuto
• La norma che vieta la conoscenza

44. Three main pillars

Il trend dell'utilizzo del digitale è salito dopo la pandemia del Covid 19.
Sono aumentati gli attacchi informatici sia all'interno e all'esterno dell'Unione Europea.
Da qui nasce la necessità di migliorare la sicurezza informatica e di rendere l'UE tecnologicamente sovrana.

Sono tre i principale pilastri su cui si basa lo sviluppo tecnologico dell'UE per i prossimi anni:

1. Tecnologia al servizio delle persone:
    1. Proteggere le persone dalle minacce informatiche
    2. Sviluppo dell'intelligenza artificiale per aiutare le persone
    3. Diffusione della banda larga ultraveloce ovunque
    4. Trovare soluzioni alternative con il supercalcolo per medicina, trasporti e ambiente
2. Un'economia digitale equale e competitiva:
    1. Finanziamenti per start-up
    2. Leggi sui servizi digitali per migliorare la responsabilità delle piattaforme on-line
    3. Adeguamento della normativa dell'UE all'economia digitale
    4. Miglioramento della protezione dei dati personali e sensibili e dell'accesso ai dati
3. Una società aperta, democratica e sostenibile:
    1. Uso della tecnologia per migliorare l'impatto climatico entro il 2050
    2. Ridurre le emissioni di carbonio del settore digitale
    3. Migliorare tutela e controllo dei dati
    4. Creazione dello "Spazio europeo dei dati sanitari" per promuovere la ricerca
    5. Combattere la disinformazione on-line

45. CSIRT e CVCN

Il CSIRT è un gruppo di intervento per la sicurezza informatica con un contingente di 30 persone. Interviene in caso di incidente e gestisce i rischi secondo una specifica procedura. Gli sono attribuite le funzioni attualmente di competenza del CERT (Computer Emergency Response Team) e del CERT-PA.
Menzioniamo in particolare:
• il monitoraggio degli incidenti a livello nazionale;
• l'emissione di allerte e informazioni alle parti interessate riguardanti rischi e incidenti;
• l'intervento in caso di incidente;
• l'analisi dinamica dei rischi e degli incidenti;

• la cooperazione con il settore privato. A tal fine il CSIRT promuove l'adozione di prassi comuni o standardizzate nel trattamento degli incidenti, dei rischi e di sistemi di classificazione degli stessi.
Il Centro di Valutazione e Certificazione Nazionale (CVCN) ha il compito di effettuare la valutazione di beni, sistemi e servizi ICT destinati a essere impiegati su infrastrutture ICT che supportano la fornitura di servizi essenziali o di funzioni essenziali per lo Stato. I soggetti pubblici e privati che offrono tali servizi o funzioni sono individuati dalle Amministrazioni competenti nei diversi settori strategici sulla base di specifici criteri e quindi inclusi nel perimetro di sicurezza cibernetica. Essi danno comunicazione al CVCN della loro intenzione di acquisire beni, sistemi e servizi ICT da impiegare sui propri asset strategici. Il CVCN può imporre limitazioni e condizioni. A seguito del D.L.14 giugno 2021, n. 82 che ha definito l'architettura nazionale di cybersicurezza, il CVCN è trasferito presso l'Agenzia per la cybersicurezza nazionale, istituita con quest'ultimo D.L.

46. Cosa è la Golden Power

Il Decreto (Perimetro Nazionale della CyberSicurezza) mira ad assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, nonché degli enti e degli operatori nazionali, pubblici e privati, attraverso l'istituzione di un perimetro di sicurezza nazionale cibernetica e la previsione di misure idonee a garantire i necessari standard di sicurezza rivolti a minimizzare i rischi, consentendo, al contempo, la più estesa fruizione dei più avanzati strumenti offerti dalle tecnologie dell'informazione e della comunicazione.
Il decreto sarà attuato in più fasi.

1. Nella prima fase saranno individuati:
    a. i soggetti responsabili di funzioni essenziali dello Stato o di servizi ritenuti fondamentali per la sicurezza dello Stato;
    b. i criteri per predisporre un elenco delle reti, dei sistemi e dei servizi rilevanti.
2. Nella seconda fase i soggetti di cui sopra trasmetteranno l'elenco delle reti, dei sistemi e dei servizi.
3. Nella terza fase saranno definite le procedure per la notifica degli incidenti. Sono previste sanzioni per i trasgressori. Il decreto prevede il CSIRT e il CVCN.

Il decreto attribuisce al Governo poteri speciali di controllo ("golden power") in materia di tutela di infrastrutture o tecnologie critiche allo scopo di esercitare una più efficace tutela dei comparti e delle aziende operanti nel settore. In particolare questi poteri speciali riguardano:

- un penetrante controllo sulle decisioni societarie aventi ad oggetto le infrastrutture e tecnologie critiche;
- la facoltà di vietare decisioni societarie o di imporre sulle stesse condizioni o prescrizioni quando esse riguardano l'affidamento di beni o servizi di ITC da impiegare sulle suddette infrastrutture e tecnologie.

47. The Digital EU

Il programma Digital Europe è un nuovo programma di finanziamento dell'UE per il periodo 2021-2027. Esso si propone il pieno utilizzo della tecnologia digitale da parte di cittadini, imprese e pubbliche amministrazioni. Rendere l'Europa più verde e più digitale sono le due sfide più importanti per la nostra generazione. I loro risultati influiranno in modo determinante sia nelle nostre vite private, sia nelle aziende.
Il programma prevede 5 settori prioritari:
1. Calcolo ad alte prestazioni (HPC - High Performance Computing):
    - Realizzare un'infrastruttura di dati e supercalcolo accessibile su base non commerciale agli utenti pubblici e privati e per finalità di ricerca finanziate con fondi pubblici;
    - Implementare tecnologia derivante da attività di ricerca e innovazione, al fine di creare un ecosistema integrato a livello dell'Unione per il calcolo ad alte prestazioni che comprenda tutti i segmenti della catena del valore scientifica e industriale, inclusi hardware, software, applicazioni, servizi, interconnessioni e competenze digitali;
2. Intelligenza artificiale (IA)
    - Sviluppare e potenziare nell'Unione le capacità di base dell'intelligenza artificiale, ivi compresi gli archivi di algoritmi e le risorse di dati, nel rispetto della normativa in materia di protezione dei dati;
    - rendere queste capacità accessibili a tutte le imprese e a tutte le pubbliche amministrazioni;
3. Cybersicurezza e fiducia
    - Promuovere e sostenere l'acquisizione di attrezzature, infrastrutture di dati e strumenti avanzati per la cybersicurezza, nel rispetto della normativa in materia di protezione dei dati;
    - Sostenere l'impiego ottimale delle conoscenze, delle capacità e delle competenze europee connesse alla cybersicurezza;
    - Garantire un'ampia implementazione delle soluzioni di cybersicurezza più recenti in tutti i settori economici;
    - Rafforzare le capacità negli Stati membri e nel settore privato per aiutarli a ottemperare alla direttiva UE recante misure per un livello

comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

4. Competenze digitali avanzate
    - Sostenere la predisposizione di corsi e attività di formazione a lungo termine per gli studenti, i professionisti informatici e la forza lavoro e a breve termine per gli imprenditori e i responsabili di piccole imprese
    - Sostenere attività di tirocinio e formazione sul posto di lavoro per gli studenti, i giovani imprenditori e i laureati.
    - Realizzare attraverso le predette attività gli obiettivi operativi sopra specificati in relazione all'area prioritaria definita "calcolo ad alte prestazioni".
5. Implementazione, impiego ottimale della capacità digitale e interoperabilità
    - Garantire che il settore pubblico e i settori di interesse pubblico, possano accedere alle tecnologie digitali più avanzate e implementarle, in particolare il calcolo ad alte prestazioni, l'intelligenza artificiale e la cybersicurezza;
    - Implementare, gestire e mantenere infrastrutture di servizi digitali interoperabili a livello transeuropeo, nonché facilitare soluzioni e quadri per l'interoperabilità;
    - Garantire a livello dell'Unione la capacità adattarsi alle nuove tendenze digitali, nonché condividere e integrare le migliori pratiche;
    - Realizzare e potenziare la rete dei poli dell'innovazione digitale.

48. NIS Directive

La direttiva contiene misure mirate ad ottenere un livello elevato di sicurezza della rete e dei sistemi informativi dei paesi membri, in modo da incrementare il livello comune di sicurezza nell'Unione europea. Questa direttiva è stata recepita nell'ordinamento italiano con il decreto legislativo n. 65 del 18 maggio 2018. Tale decreto:
- rappresenta la cornice legislativa delle misure da adottare allo scopo suddetto;
- individua i soggetti competenti per darvi attuazione.

Gli organi istituzionali cui compete dare attuazione alla direttiva NIS sono:

1. Il Presidente del Consiglio dei Ministri:
   Sentito il Comitato interministeriale per la sicurezza della Repubblica (CISR), egli adotta:
    - la strategia nazionale di sicurezza cibernetica per la tutela della sicurezza delle reti e dei sistemi di interesse nazionale
    - le linee di indirizzo per l'attuazione della suddetta strategia
2. Le Autorità competenti NIS:

La qualifica di "autorità competente NIS" è attribuita singoli ministeri (salute, ambiente, sviluppo economico, ecc.) in relazione ai rispettivi settori di competenza (servizi sanitari, acqua potabile, mercati finanziari, ecc.). Tali autorità verificano l'applicazione della direttiva a livello nazionale ed individuano gli operatori di servizi essenziali nell'ambito dei criteri definiti.

3. Il Computer Security Incident Response Team (CSIRT)
4. Il Dipartimento delle informazioni per la sicurezza (DIS):
   Il Dipartimento delle informazioni per la sicurezza (DIS) è l'organo di cui si avvalgono il Presidente del Consiglio dei ministri e l'Autorità delegata per l'esercizio delle loro funzioni. Il D.L. n. 65/2018 ha designato il DIS quale unico organo a livello nazionale incaricato di coordinare le questioni relative alla sicurezza delle reti e dei sistemi informativi, nonché la cooperazione transfrontaliera nell'ambito dell'Unione europea.
5. L'Autorità di contrasto:
   Il decreto legislativo n. 65/2018 individua quale Autorità di contrasto l'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione, organo che in atto gestisce i servizi di protezione informatica delle infrastrutture critiche informatizzate di interesse nazionale. Esso opera mediante collegamenti telematici con i responsabili delle strutture interessate.
6. Gli Operatori di servizi essenziali:
   Si tratta di soggetti pubblici o privati individuati dalle competenti autorità NIS e operanti nei seguenti settori: energia e trasporti, attività bancaria, mercati finanziari, sanità, acqua potabile, infrastrutture digitali. Essi hanno l'obbligo di individuare le misure tecniche e organizzative afferenti alla gestione dei rischi, con specifico riferimento alla prevenzione e minimizzazione degli impatti degli incidenti. Sono, altresì, definite le modalità di notifica degli incidenti che abbiano un impatto rilevante sui servizi interessati.

Come previsto dal decreto legislativo n. 65/2018, l'autorità NIS esercita il controllo sulle attività degli operatori di servizi essenziali e dei fornitori di servizi digitali. In particolare, l'autorità NIS ha poteri di verifica e di ispezione e può applicare sanzioni amministrative per la mancata osservanza degli obblighi posti a carico dei soggetti di cui sopra.

49. CAD

La tutela dei dati informatici è prevista per legge, per quanto riguarda l'Italia, nella "Strategia per la crescita digitale 2014 - 2020", in accordo con l'Agenda Digitale per l'Europa e soprattutto, dal punto di vista giuridico, nel "Codice dell'Amministrazione Digitale", il cui acronimo è CAD. Il CAD stabilisce che le pubbliche amministrazioni devono organizzarsi utilizzando le tecnologie dell'informazione e della comunicazione per rag- giungere gli obiettivi di efficienza, efficacia, economicità, imparzialità, trasparenza, semplificazione e partecipazione, nel rispetto dei principi di uguaglianza e non discriminazione, per l'effettivo riconoscimento dei diritti digitali dei cittadini e delle imprese.

50. Misure minime di sicurezza ICT per la PA

L'Agenzia per l'Italia Digitale (AGID) si occupa, tra l'altro, dell'efficienza dei livelli di sicurezza informatica della P.A. A tal fine emana le misure minime di sicurezza informatica che devono essere osservate dai soggetti e dagli enti della P.A. Tali misure rappresentano un importante riferimento pratico messo a disposizione delle pubbliche amministrazioni per valutare e migliorare il loro livello di sicurezza informatica, al fine di combattere adeguatamente le minacce informatiche più frequenti. Esse consistono in controlli tecnologici, organizzativi e procedurali.
Sono previsti tre livelli di attuazione degli interventi minimi, basati su un criterio di gradualità, in considerazione della complessità del sistema informativo e dell'organizzazione della singola pubblica amministrazione.
• Livello minimo: è costituito dalle misure di sicurezza di base alle quali ogni Pubblica Amministrazione deve conformarsi, indipendentemente dalle dimensioni e dalla struttura organizzativa; (sei ancora censurabile, non va bene);
• Livello standard: rappresenta il modello di riferimento, superiore al livello minimo, proposto ad ogni amministrazione come base di riferimento in termini di sicurezza. Questo livello è osservato dalla maggior parte delle amministrazioni pubbliche italiane.
• Livello avanzato: è il livello a cui devono attenersi le organizzazioni più esposte ai rischi (ad esempio, per la criticità delle informazioni trattate o dei servizi forniti). Rappresenta un obiettivo di miglioramento per tutte le altre organizzazioni.
La cosa importante è che queste misure non sono solo provvedimenti sono anche specifici parametri di misurazione delle performance.
Obiettivi delle misure minime:
• stabiliscono una base comune di misure tecniche ed organizzative irrinunciabili;

• forniscono uno strumento utile a verificare lo stato di protezione contro le minacce informatiche e poter tracciare un percorso di miglioramento;
• responsabilizzano le Amministrazioni sulla necessità di migliorare e mantenere adeguato il proprio livello di protezione cibernetica.

51. Piano ICT PA 20-22

Il nuovo piano triennale indica i seguenti obiettivi strategici:
• Rafforzare le leve per l'innovazione delle PA e coinvolgimento attivo dei territori;
• Rafforzare le competenze digitali per la PA e per il Paese e favorire l'inclusione digitale;
• Migliorare il monitoraggio dei processi di trasformazione digitale e di innovazione della PA.
La realizzazione di questi obiettivi è demandata alle singole amministrazioni che oramai dispongono di adeguati standard per una misurazione omogenea dei risultati. In tale contesto la qualità dei dati assume un rilievo centrale.
Il nuovo piano ICT per la P.A. indica le seguenti linee guida:
• digital & mobile first per i servizi;
• cloud first (cloud come prima opzione), anche al fine di prevenire il rischio di lock-in;
• servizi inclusivi e accessibili e interoperabili by design;
• sicurezza e privacy by design dei servizi digitali;
• servizi user-centric, data driven e agile; (centrati sull'utente, si deve capire che cosa vuole l'utente, perché ha fatto questo accesso)
• once only (non chiedere a cittadini e imprese informazioni già da loro fornite);
• open data (dati pubblici quale bene comune, reso fruibile in forma aperta e interoperabile;
• codice aperto (nel caso software sviluppato dalla PA, rendere disponibile il codice sorgente).
Perché è la mancata consapevolezza che produce risultati, come per il COVID è la mancata consapevolezza di questo rischio che produce comportamenti inappropriati. Niente elimina il rischio, ma il concetto risiede nel mitigarlo.
Il nuovo piano assume come obiettivo centrale la consapevolezza del rischio cyber. Solo da una adeguata consapevolezza dei responsabili e degli operatori possono derivare le azioni organizzative necessarie a mitigare il rischio connesso alle potenziali minacce informatiche. Da qui l'enucleazione dei seguenti obiettivi strategici:
• Aumentare la consapevolezza del rischio cyber nelle PA;
• Aumentare il livello di sicurezza informatica dei portali istituzionali della Pubblica Amministrazione.

52. CyberCrime

Con il termine cybercrime si denota una serie di reati che sono commessi esclusivamente o prevalentemente nel cyberspazio e con l'uso di mezzi informatici. Si distinguono i reati il cui oggetto o la cui condotta tipica sono collegati con un sistema informatico (computer as tool) dai reati in cui è il sistema ad essere oggetto dell'attacco (computer as target).
Appartengono, fra gli altri, al primo gruppo:
• le truffe online;
• la diffamazione a mezzo posta elettronica, o chat, o Internet;
• il riciclaggio;
• le molestie con spamming;
• la pedopornografia;
• il sexting, cioè la diffusione in rete di immagini e video aventi esplicito contenuto sessuale, penalmente rilevante se ha ad oggetto minori (distribuzione di materiale pedopornografico) oppure se compiuta senza il consenso della persona rappresentata nell'immagine o nel video
Appartengono al secondo gruppo i reati introdotti nel nostro ordinamento giuridico con la legge XXX. Quest'ultima ha dato esecuzione alla Convenzione di Budapest 2001.
Le fattispecie di reato più rilevanti sono:
• accesso abusivo ad un sistema informatico o telematico
• detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici
• diffusione di apparecchiature ed altro diretti a danneggiare un sistema informatico o telematico
• danneggiamento di informazioni, dati e programmi informatici
• danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità
• danneggiamento di sistemi informatici o telematici
• danneggiamento di sistemi informatici o telematici di pubblica utilità
• il phishing, realizzato con l'invio di mail ingannevoli, recanti il logo contraffatto di un istituto di credito o di una società di commercio
elettronico con cui si chiede al destinatario di fornire dati riservati, come il numero della propria carta di credito, la password di accesso alla home banking, e così via (reato di truffa e reati minori);
• frode informatica con applicabilità della confisca
• frode informatica del certificatore di firma elettronica

53. Elementi nella gestione del rischio (art 75,76)

L'articolo 25 del GDPR definisce quindi i profili di responsabilità per i trasgressori. La possibilità di incorrere in responsabilità è un fattore di rischio. Ciò è specificato nel considerando del GDPR, ai punti 75 e 76, che trattano il tema del rischio nel trattamento dei dati personali.

Rischi nel trattamento dei dati personali:
Secondo i punti 75 e 76 della premessa al GDPR, nel trattamento dei dati personali devono essere considerati i seguenti elementi di rischio:

- oggetto del rischio
- probabilità del rischio
- severity of risk
- source of the risk: processing of personal data
- consequences of risk: material or immaterial damage
- gravità del rischio
- fonte del rischio: trattamento dei dati personali
- conseguenze del rischio: danno materiale o immateriale

54. Accountability

Il concetto di accountability va oltre quello di responsabilità. Il GDPR lo collega alla conformità e alla dimostrazione. Questo concetto esprime essenzialmente serietà, fiducia, capacità di adempiere ai propri doveri, primo fra tutti quello di osservare le regole e di dimostrare e giustificare tutto ciò attraverso la trasparenza del sistema.
Tra i doveri del titolare del trattamento c'è quello di garantire l'integrità e la riservatezza dei dati. I dati personali sono trattati mediante misure tecniche e organizzative adeguate.

55. Condotta

La condotta è l'azione o l'omissione cosciente e volontaria del soggetto.

Possiamo definire la condotta formata da due elementi:
"T Factor" + "K Factor" = Condotta

1. "T Factor": Possiamo definire l'azione o l'omissione del soggetto come il fattore di transizione, sinteticamente T factor. Rappresenta il livello muscolare della transizione del soggetto nel mondo
2. "K Factor": Il soggetto opera nel mondo sulla base di un impulso psichico. Rappresenta il livello cosciente di attivazione del soggetto. Chiameremo questo impulso il fattore cosciente, sinteticamente K

factor.
Il K Factor, seppur unitario, viene analizzato dalla legge in due fasi distinte:

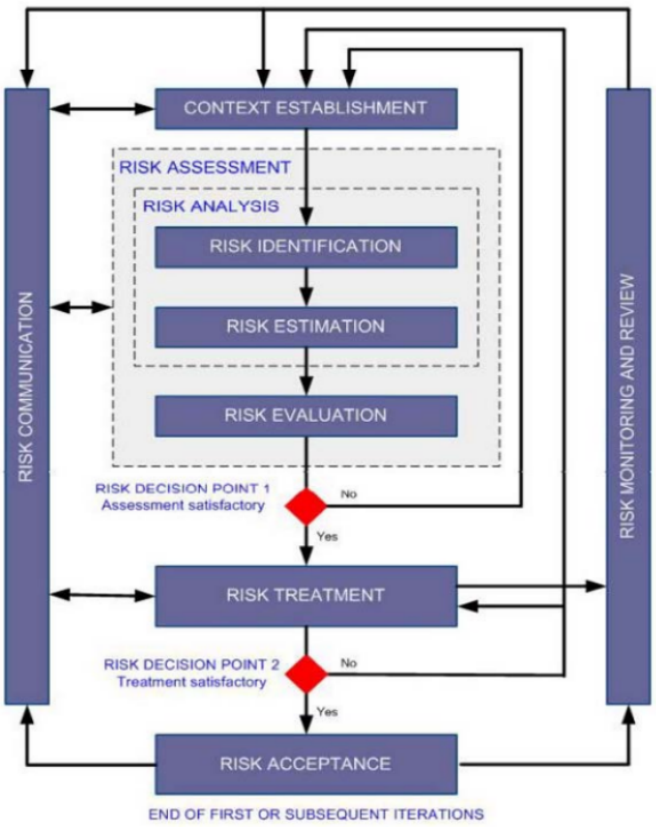
a. La suitas (K1 Factor): Nel sistema penale italiano la suitas è prevista dall'articolo 42, comma 1, del Codice penale che dice letteralmente: "Nessuno può essere punito per un'azione o un'omissione prevista dalla legge come reato se non l'ha commessa con coscienza e volontà".

   Quindi per affermare la responsabilità penale di una persona sono necessari i seguenti elementi:
   • un'azione o un'omissione
   • che tale azione o omissione è qualificata dalla legge come un reato
   • che è stato commesso con coscienza
   • che si è impegnato con volontà

b. L'intenzione (K2 Factor): Il reato è intenzionale o secondo l'intenzione (in italiano "dolo") quando l'evento dannoso o pericoloso che è il risultato dell'azione o dell'omissione e da cui, secondo la legge, dipende dall'esistenza del reato, è previsto e voluto dall'agente a seguito della sua azione o omissione.
   • Il reato è preterintenzionale, o al di là dell'intenzione
   • Il reato è per colpa.

56. Inquadramento civilistico del contratto
57. Norme di diritto privato/civile

Zatti:



The necessary awareness of and commitment to Risk Management at senior management levels throughout the organization is mission critical and should receive close attention by:
• obtaining the active ongoing support of the organization's directors and senior executives for Risk Management and for the development and implementation of the Risk Management policy and plan;
• appointing a senior manager to lead and sponsor the initiatives;
• obtaining the involvement of all senior managers in the execution of the Risk Management plan.

Once a management committee has been created, it must define the scope of the information security management framework so as to focus on the essential. The security perimeter can cover either selected sections of an organization or the entire organization. Keep in mind that the ISMS must be under organizational control. If the organization does not control the ISMS, it will be unable to manage it efficiently.

Context establishment

In order to accurately define your ISMS, you must clearly identify:

- Goal/objective
- Scope: What administrative units and activities will be covered by the information security management framework?
- Boundaries / limits: The limits of the ISMS' scope are defined in accordance to: The specific characteristics of the organization (size, field of endeavor, etc.); Location of the organization; Assets (inventory of all critical data); Technology
- Interfaces: The organization has to take into account interfaces with other systems, other organizations and outside suppliers.

- Dependencies: The ISMS has to respect certain security requirements. These requirements can be of a legal or commercial nature.
- Exclusions and Justification: Any element or domain (part of a network or of an administrative unit) defined by the SGSI, yet not covered by a security policy or security measures, must be identified and its exclusion explained.
- Strategic Context
- Organizational context: The organizational environment enhances the measures implemented to meet specific objectives as set by management.

A correct definition of the scope is fundamental: all the subsequent steps of the methodology rely on an appropriate defined scope. Unfortunately, scope can be wrong in two directions: too narrow or too broad.

Risk Assessment

Identification of assets and their values (Risk Identification)

An inventory of information assets (e.g. IT hardware, software, personnel, data, system documentation, storage media and ICT services) should be maintained. The inventory should record ownership and location of the assets. This list of assets should also comprise their associated values with regards to Confidentiality, Integrity and Availability.

Identification of Threats, Threat Sources and Vulnerabilities (Risk Identification)

Threat: Potential cause of an unwanted incident that damages a system of the organization.

Depending on the inventory compiled in the previous section, we should understand which threats could affect our assets. Look also at ENISA annual report for threats.

E.g.:

- Hardware
  - Web server
    - Hacker attack
    - Disk crash
- Software
  - Web server Apache
    - Software bug
    - Exploit of published vulnerability (before fixing)
- People
  - Network Administrator

        ▪ Defection, Death, Long Term Sick, Mid Term Sick, Short Term Sick, Maternity Leave, Non-deliberate Human Error, Malicious Human Error
- Data
  - Personal Mail
    - Interception, Impersonation, repudiation
    - SPAM
- Physical
  - Power
    - Failure
    - Low voltage

Then we have to enumerate the threat sources. Examples:

- Natural Disasters: fires, floods, earthquakes...
- Non-Human: Flaws, bugs, errors, problems, congestions, overload, overheating, etc.
- Human:
  - Malicious - intentional:
  - Internal: Disgruntled employees, disloyal, spies, etc…
  - External: Hackers, crackers, terrorists, spies, etc…
- Non malicious (non-intentional): Uneducated, uninformed, unaware, employees, human errors, blunders

Vulnerability: A weak point that can be exploited by one or more threats. Examples:

- Hardware
  - Web server
    - Position, Age, disk redundancy (lack of)
- Software
  - Web server Apache
    - Events in the press (mission goal, launch)
    - Software bugs
    - Published vulnerability
- People
  - Network Administrator
    - Health status, Nationality, Hobbies, Sex, Age, Salary
- Data
  - Personal Mail
    - Visibility of staff, size and frequency of messages,
- Physical
  - Power

        - UPS (lack of), status of power grid
    - Air conditioning, heater

Analysis of Risks (Risk Estimation)
Here we can decide two types of Analysis: Qualitative and Quantitative.

Qualitative analysis:
It provides a scale of attributes to describe the extent of the potential consequences (low, medium, high) and the likelihood that they will occur.
PROS: Easy to understand
CONS: The scale is subjectively chosen
When should it be used?
• For the initial screening of a risk that requires a much more detailed analysis
• Where numerical and statistical data are inadequate

Quantitative analysis:
It provides a numerical scale used for both consequences and probabilities. Its quality will be higher the more accurate and truthful the data on which it is processed is and the more reliable the reference models are.
PROS: Use of historical data directly linked to safety objectives
CONS: "less reliable" scale on new data or almost totally unreliable if factual data is not available.

Once this phase is over we have each risk with an associated value for probability and impact (qualitative or quantitative).

Evaluation of Risks (Risk Evaluation)
In this phase we have all (hopefully) the risks associated with their impact and probability value. Now we have to prioritize them… what does this mean? This means that we have to arrange the risks in an appropriate order such that we can understand which ones we have to treat before and after. Under which conditions? It depends on a lot of factors: type of business, etc.
We have then to insert the risks in an acceptance matrix: this means that for the risks having a value (probability * impact) less than X (a certain threshold) we can accept those risks, for all the others having a value higher than X we have to understand how we have to treat them.
If the assessment isn't satisfying we can 'save' the results and restart from the initial step (Context definition).

Risk Treatment

Risk Treatment is the process of selecting and implementing measures to modify risk. Once risks have been identified and calculated, a decision must be made as to the management of these risks.
How risks are to be managed is usually a function of:

- Initial security policy;
- Level of assurance required;
- Risk assessment results;
- Existing business, legislative and regulatory constraints.

There are four risk treatment options:

1. Risk Mitigation / Reduction: The organization implements measures or adopts the means that will reduce risk to an acceptable level.
2. Risk Acceptance: The organization takes a calculated risk and knowingly assumes responsibility for the consequences.
3. Risk Avoidance: Risks can be avoided by moving potentially targeted assets out of the risk area or by completely abandoning the business activities that generate security weaknesses.
4. Risk Transfer: The organization transfers the risk through the purchase of insurance or through outsourcing.

Among the risk treatment options seen so far risk reduction is always the most suitable one.
Risk Reduction is by far and large the option selected, in line with the available resources. Consequently, objectives must be set, and controls implemented. Upon completion of the risk assessment, you must select the implementation of various controls, consistent with the ISO 27001 standard, in each targeted information environment. The afforded protection is adapted to the perceived threat. The Executive management (Risk Owner) retains or rejects the proposed solution before proceeding with the development of the Risk Treatment plan.

Risk Communication

An integral part of the treatment of risks are the Communications on risks which must be carried out on an ongoing basis. What are risk communications about? Collect information, share the results of the ISRA of the treatment plan developed in order to avoid conflicts and violations between those responsible and increase their awareness and sense of responsibility.
A thorough exercise of risk communication should be carried out in order to:
• provide assurance of the outcome of the organization’s risk management
• collect risk information
• share the results from the risk assessment and present the risk treatment plan

• avoid or reduce both occurrence and consequence of information security breaches due to the lack of mutual understanding among decision-makers and stakeholders
• support decision making
• obtain new information security knowledge
• coordinate with other parties and plan responses to reduce consequences of any incident
• give decision-makers and stakeholders a sense of responsibility about risks
• improve awareness
• The risk communication activity should be performed continually

ISMS Monitoring and Review

We must collect information, verify the effectiveness of the proposed approach and possibly improve it. We are in fact ready to start the process all over again.
Monitoring ⇒ Control and supervise activities.
Review ⇒ Identify what is not working in order to increase the efficiency and effectiveness of the process.
We will apply monitoring and review to the entire applied framework, to the risk management process, to the identified risks and to the measures taken by the organization to address them. This phase is important to verify that the controls are effective and efficient, to see if there are new risks on the horizon, to analyze and learn something even from negative situations such as accidents, to obtain additional information to face future risks (⇒ the risks are NOT static and evolve over time).

Study cases:

1. Ospedale e farmacologia.
2. FS di termini (sistema IT), ENISA --> different trains, what could happen in that system? --> il software decide dove i treni devono andare, quando partire ecc (rischio)
3. System IT in terremoto ad Amatrice --> organize the troupe
4. Un fiume che straripa, la protezione civile deve intervenire nell'area
5. Sistema IT per un'azienda di assicurazione
6. Archivio della banca d'Italia (focalizzandosi sulla gestione dei dati)
7. Organizzazione che conserva dati dei dipendenti e dei customers
8. Sistema IT di Ferrovie delle stato
9. Sistema IT di un Aeroporto