QUALITY FOR ITALY

ITALY FOR QUALITY

Qualità: Il valore dei dati e delle informazioni.

Ezio Boiani - Gruppo Galgano

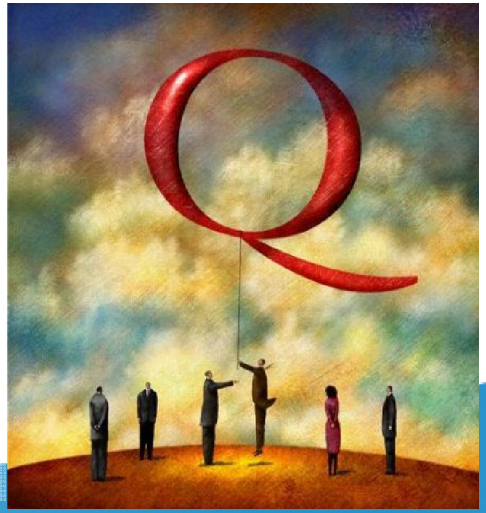
Contenuti

1. La sicurezza delle informazioni

2. Le Logiche e i vantaggi di un Sistema di Gestione

3. La norma ISO 27001:
la struttura di riferimento e i requisiti

4. La visita di certificazione ISO 27001



Il valore dei dati e delle informazioni

Il Patrimonio Aziendale:

E' più importante il barattolo di Nutella o la formula per realizzare la Nutella?

E' più importante la bottiglia di CocaCola o la formula per realizzare la CocaCola ?

Scenari nuovi e applicazioni in diversi contesti

Premessa … cosa pensiamo ?

Quale sensibilità alla sicurezza dei dati

- **Rapporto dell'Osservatorio Cermes Bocconi-Affinion, su un campione di mille persone fra i 18 e i 75 anni**
- Lo studio ha chiesto agli italiani **cosa ritengano faccia parte dei propri dati personali e quali siano la rilevanza e il rischio del loro furto**
- Nel complesso gli italiani sono legati a un'idea tradizionale di "dati personali":
  - il 92% concorda che sia composto dai dati anagrafici,
  - l'85% comprende i dati sanitari,
  - oltre l'80% annovera quelli economico-finanziari,
  - ma solo il 58% include i dati sugli spostamenti

Premessa … cosa pensiamo ?

- La navigazione sul web è considerata molto pericolosa, mentre si pensano un po' meno pericolosi l'uso delle informazioni in ambiente mobile - come l'inserimento di dati via telefono - e l'uso in ambiente reale, come il dare la carta di credito al cameriere.

- Tradizionali anche le cautele:
  - il 69% si protegge mentre digita i pin,
  - il 67% tiene i pin separati dalle carte,
  - il 59% non comunica le proprie password.
  - Però soltanto il 33% le cambia frequentemente,
  - il 37% ne costruisce di complesse e
  - il 38% paga online solo con carte prepagate.
  - Il 77% non possiede un database protetto dei propri dati personali

- Fonte: www.repubblica.it del 26 Novembre 2013

Premessa … cosa pensiamo ?

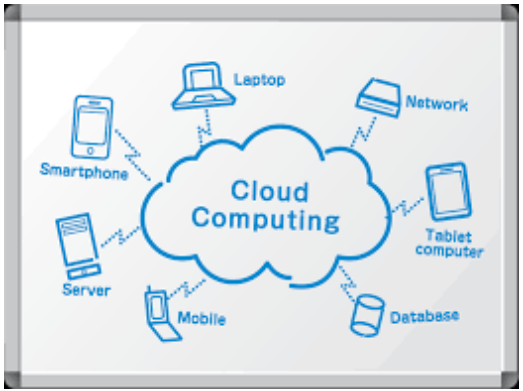
Rapporto Clusit 2013

- …….. In sostanza, ad un anno dal Rapporto 2012 ci troviamo oggi di fronte ad una vera e propria emergenza nella quale nessuno può più ritenersi al sicuro, dove tutti sono in qualche modo ed a vario titolo minacciati, dai singoli cittadini alle PMI fino agli stati nazionali ed alle più grandi imprese del mondo, mentre la frequenza degli incidenti è aumentata del 250% in un solo anno, ed il Cyber Crime è diventato la causa del 54% degli attacchi (era il 36% nel 2012), con una crescita anno su anno del numero di attacchi di oltre il 370% ……..

QUALITY FOR ITALY
ITALY FOR QUALITY

Premessa … cosa pensiamo ?

- Entro il 2016 il traffico cloud globale costituirà quasi due terzi di tutto il traffico di data center.
- Nei prossimi 5 anni il traffico di data center crescerà di 4 volte
- Si stima che essendo già connessi a Internet circa 50 miliardi di «oggetti», il numero di connessioni crescerà raggiungendo entro il 2020 il numero di 13.311.666.640.184.600



- Fonte: Cisco Report annuale sulla sicurezza 2013

Sicurezza aziendale (schema organizzativo)

Sicurezza aziendale

- **Sicurezza dei beni materiali ed immateriali**
- **Sicurezza delle persone e tutela ambientale**
- **Sicurezza dell'informazione**
  - Sicurezza informatica
  - Sicurezza del sistema informativo non automatizzato (informazioni e know how)

La norma ISO/IEC 27001
Il Sistema di Gestione della Sicurezza delle Informazioni [SGSI]

Cosa sono le «INFORMAZIONI»

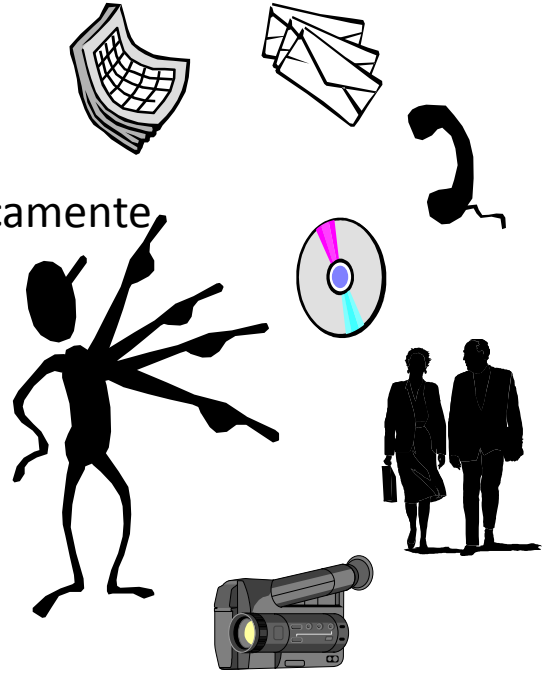
- **L'informazione è un asset che, come altri importanti asset aziendali, è essenziale per il business di un'organizzazione e conseguentemente necessita di essere adeguatamente protetto (ISO/IEC 27000)**

- Le informazioni sono parte del patrimonio aziendale comparabili con ogni altro bene nell'azienda

- Sono le conoscenze, i documenti, i contratti, le pianificazioni di attività future, gli studi di fattibilità, i brevetti, i progetti, i lay-out impiantistici …
  … ed anche le idee nella testa delle persone

Dove risiedono le «INFORMAZIONI»

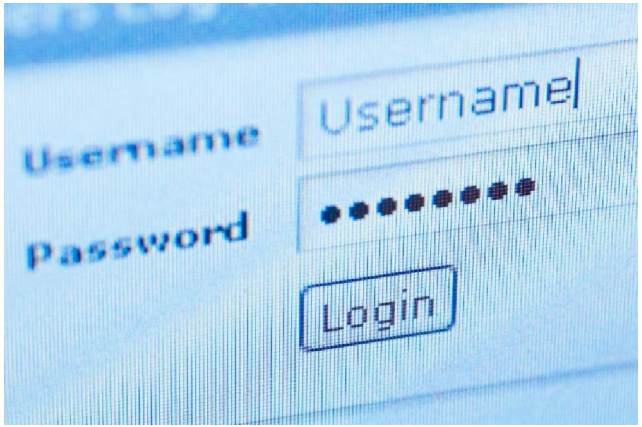
- Stampate o scritte su carta
- Memorizzate o trasmesse elettronicamente
- Mostrate in disegni, figure, immagini, filmati
- Passate a voce ad altre persone



Cosa è la sicurezza delle «INFORMAZIONI»

- La sicurezza delle informazioni è definita come la protezione dei requisiti di **integrità**, **diponibilità** e **confidenzialità** delle informazioni acquisite, comunicate, archiviate, processate ecc.

- Esistono altri requisiti per la sicurezza delle informazioni e dei sistemi connessi in rete quali **l'autenticità** e il **non ripudio**



Cos'è la sicurezza delle INFORMAZIONI

Significato della «Sicurezza» delle informazioni come preservazione di:

RISERVATEZZA

Assicurazione che le informazioni siano **accessibili** solo a coloro che sono autorizzati ad avere accesso

INTEGRITÀ

La salvaguardia della **precisione** e della **completezza** dell'informazione e del metodo di elaborazione

DISPONIBILITÀ

L'assicurazione che gli utenti autorizzati abbiano **accesso** alle informazioni e ai ben quando richiesto

In pratica …

- **Integrità**: è la proprietà dell'informazione di non essere stata alterata. L'integrità descrive il grado di correttezza, completezza e consistenza dell'informazione. I sistemi ICT sia a livello HW che SW debbono operare correttamente e con adeguate protezioni.
- **Disponibilità**: è la proprietà dell'informazione di essere accessibile e utilizzabile quando richiesto dai processi e dagli utenti autorizzati. Essa implica la disponibilità dei sistemi che la trattano.
- **Confidenzialità**: è la proprietà dell'informazione di essere nota solo a chi ne ha diritto. In taluni casi viene riformulata in termini di segretezza e riservatezza.
- **Autenticità**: la certezza da parte del destinatario dell'idenitità dell'autore dell'informazione
- **Non ripudio**: il mittente o il destinatario di un'informazione non ne possono negare l'invio o il possesso.

Sicurezza FISICA delle informazioni

Il ruolo della sicurezza fisica è quello di proteggere:

Sicurezza LOGICA delle informazioni

Il ruolo della sicurezza logica è quello di proteggere:

- Il software di base e di ambiente (inclusi gli applicativi vari e quello di controllo di gestione)
- Le informazioni trattate, quindi gli archivi e le banche dati
- Le reti e i protocolli di comunicazione

Cos'è un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI)

SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

L'insieme del personale, delle responsabilità, delle risorse e delle procedure impiegate dall'organizzazione per raggiungere e mantenere gli obiettivi di integrità, riservatezza e disponibilità definiti in termini di sicurezza delle informazioni.

La norma internazionale **ISO/IEC 27001:2013** è la norma per poter certificare il sistema di gestione per la sicurezza delle informazioni

La norma internazionale **ISO/IEC 27002:2013** è la guida per mettere a punto la sicurezza delle informazioni

- Tutti i beni dell'azienda devono essere protetti in maniera adeguata …… (anche le informazioni!), creando un sistema di gestione che permetta di coordinare, controllare, misurare, migliorare le attività svolte, accrescendo l'attenzione e consapevolezza nei confronti della sicurezza delle informazioni

Lo standard ISO/IEC 27001:2013

- Dal momento che l'informazione è un bene che aggiunge valore all'impresa, ogni organizzazione deve essere in grado di garantire la **sicurezza** dei propri dati.
- L'obiettivo del nuovo standard ISO 27001 per i SGSI è dunque di fornire un **quadro di riferimento** per l'implementazione di un sistema di gestione a protezione dei dati e delle informazioni da minacce di ogni tipo, al fine di assicurarne l'integrità, la riservatezza e la disponibilità.
- La **ISO 27001** è strutturata per essere compatibile con altri sistemi di gestione quali la ISO 9001 e tecnologie indipendenti dal produttore, il che significa che è completamente indipendente da qualsiasi piattaforma di Information Technology
- Di fondamentale importanza è **l'Annex A** che contiene i **114 "controlli"** (o contromisure) a cui, l'organizzazione che intende applicare la norma, deve attenersi

High Level Structure HLS della ISO/IEC 27001:2013

- Per la nuova ISO/IEC 27001:2013 è stata utilizzata la nuova **High Level Strutture** per i sistemi di gestione richiesta dalle direttive ISO dal 2009 per tutte le norme di gestione (qualità, ambiente, sicurezza, energia, ecc..)

- I **requisiti** sono contenuti nei punti:
  - Contesto dell'organizzazione
  - Leadership
  - Pianificazione
  - Supporto
  - Attività Operative
  - Valutazione delle prestazioni
  - Miglioramento

"Struttura di alto livello" uguale per tutti i SG

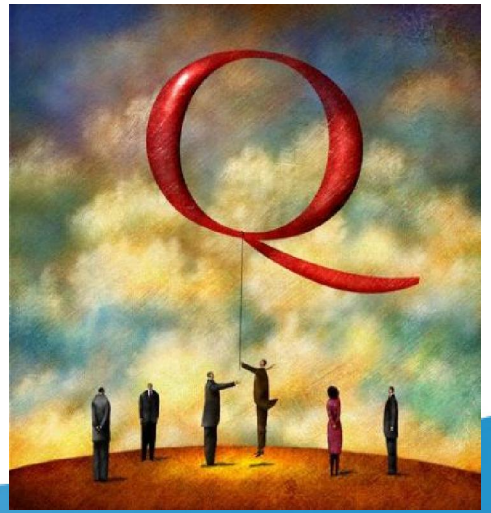
Contenuti

1. La sicurezza delle informazioni

2. Le Logiche e i vantaggi di un Sistema di Gestione

3. La norma ISO 27001:
   la struttura di riferimento e i requisiti

4. La visita di certificazione ISO 27001



QUALITY FOR ITALY
ITALY FOR QUALITY

Le logiche di un Sistema Gestione

Alcune parole chiave di un SG

a) Regole
b) Processi
c) Rischio
d) Misura
e) Leadership
f) Stakeholder
g) Miglioramento

QUALITY FOR ITALY
ITALY FOR QUALITY

a) Regole

L’operare senza regole

è il più faticoso e difficile

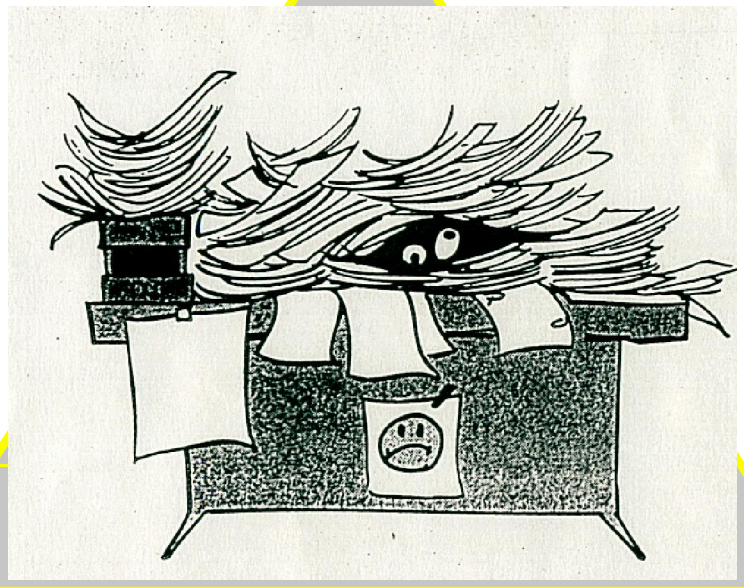
mestiere di questo mondo

(Alessandro Manzoni: “Storia della colonna infame” - 1840)

Quando NON ci sono «regole» NON c'è qualità ne sicurezza...

- Non è chiaro come operare, le attività non sono standardizzate
- Non c'è chiarezza organizzativa
- Il personale si comporta in maniera diversa
- La normativa è interpretata in maniera diversa
- Le attività sono conosciute e svolte solo da alcuni operatori
- Non è stato recepito un cambiamento normativo
- Non si trovano e non sono sicure i documenti in archivio o in lavorazione
- Non abbiamo misure e dati a supporto delle decisioni
- Gli incidenti di sicurezza non sono gestiti
- Ecc. ...

La «piramide» della documentazione



Attenzione agli aspetti burocratici

b) Processi

Processo :

Vedere la foresta

e non solo gli alberi

Occorre saper VEDERE I PROCESSI non le singole attività

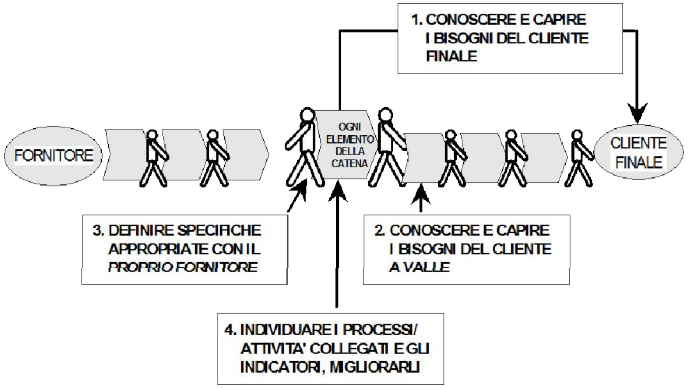
I Processi di un'organizzazione

Processo :

«Un insieme di attività

che trasformano input in output

che hanno valore per il cliente»



I processi come catene fornitori - clienti

I processi di security da considerare in un SGSI

1. CONTROLLO ACCESSI (LOGICO)
2. GESTIONE ASSET
3. GESTIONE PROFILI DI AUTORIZZAZIONE
4. BACKUP
5. BUSINESS CONTINUITY
6. GESTIONE DEI CAMBIAMENTI
7. GESTIONE CONFIDENZIALITÀ
8. GESTIONE CONTRATTI
9. RISORSE UMANE
10. GESTIONE INCIDENTI DI SICUREZZA
11. ASPETTI LEGALI
12. GESTIONE CODICE MALEVOLO
13. GESTIONE RETE
14. SICUREZZA FISICA
15. POLITICHE E PROCEDURE

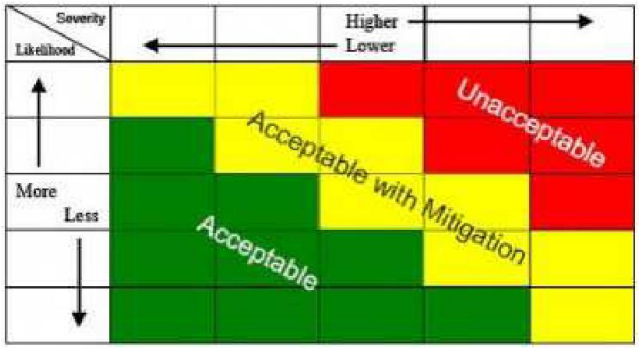
c) Rischio

Rischio: possibilità di pericolo,

di danno materiale o morale,

dipendente da situazioni spesso

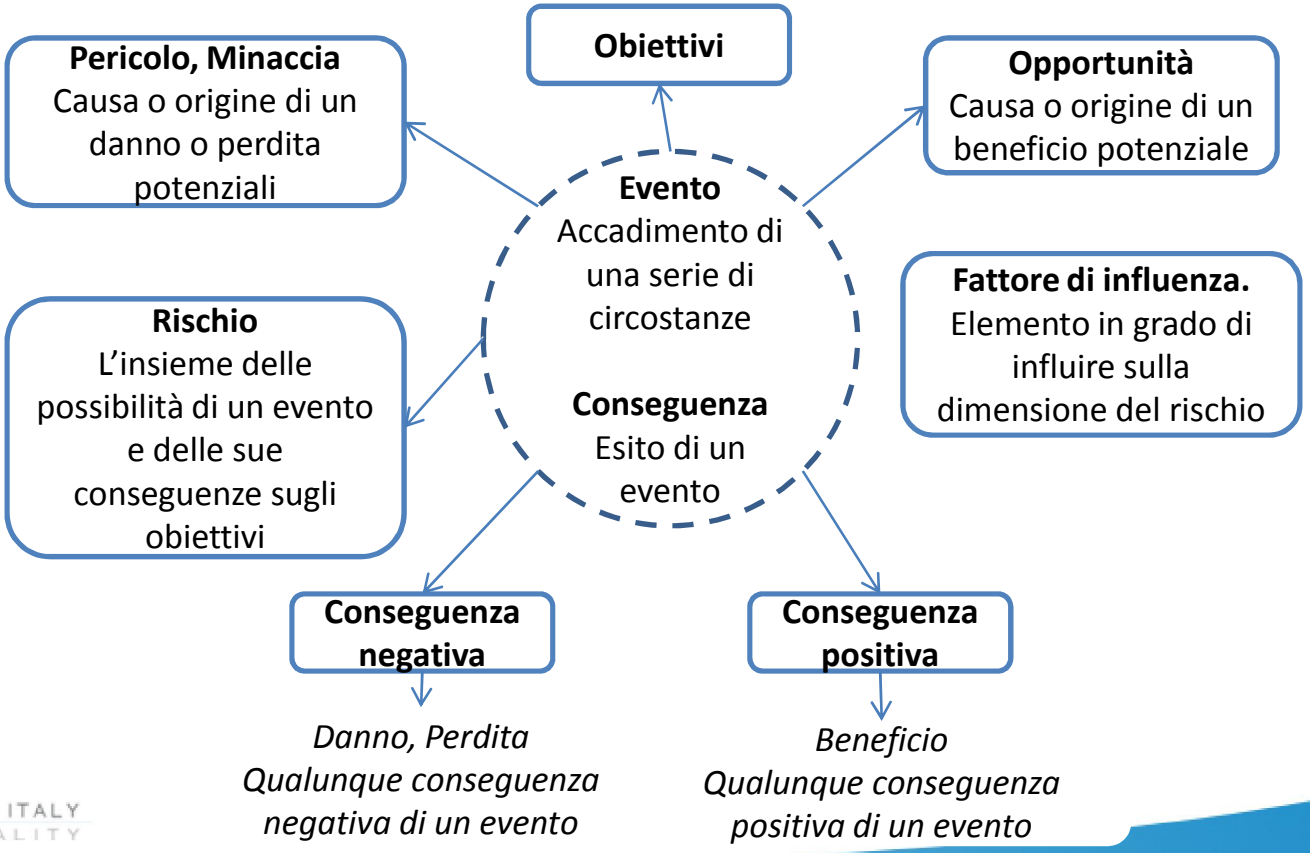
di imprevedibilità



Gestione del rischio: Attività coordinate per guidare e tenere sotto controllo una organizzazione con riferimento al rischio

I concetti relativi al rischio

(da UNI 11230:2007 Gestione del rischio- Vocabolario)



Benefici

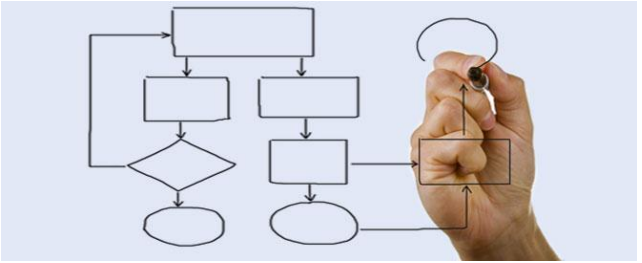
- Indirizzo Strategico **condiviso** nei processi dell'Organizzazione
- Immagine di **solidità** e fiducia verso gli stakeholder
- Criticità **ridotte** grazie ad analisi e valutazione del rischio
- Performance **migliori** dei processi gestionali e operativi
- Risposta più **veloce** ai cambiamenti di strategia e contesto

Cosa fare, in pratica?

- **Identificare, analizzare e gerarchizzare i rischi e le opportunità nell'organizzazione**
  - Che cosa è accettabile?
  - Che cosa non lo è?
- **Pianificare azioni per affrontare i rischi**
  - Come posso evitare o eliminare il rischio?
  - Come posso mitigare il rischio?
- **Attuare il piano *(condurre le azioni)***
- **Controllare l'efficacia delle azioni *("funziona"?)***
- **Apprendere dall'esperienza *(miglioramento continuo)***

L’analisi del rischio: l’esempio della FMEA

FMEA
Failure Mode and Effect Analysis



Passi metodologici semplici:

1. Individuare i **rischi** («modi di guasto») connessi con le fasi (o macro fasi) di un processo
2. Stimare la **probabilità** di accadimento dell’effetto del modo di guasto **(P)**
3. Stimare la **gravità** dell’effetto del modo di guasto **(G)**
4. Stimare la probabilità di prevenire l’effetto del modo di guasto ossia la **rilevabilità** della causa, del modo o dell’effetto stesso **(R)**
5. Calcolare l’indice di priorità di rischio per ogni causa del modo di guasto **(IPR)**
6. Individuare le **azioni correttive** sulla base del valore dell’indice di priorità di rischio

Esempio di attribuzione dei punteggi

Legenda/Istruzioni

Sulla base delle informazioni in vostro possesso, identificate i principali rischi connessi con i processi che state analizzando.

Per ogni rischio identificato definite:

a) **P**: probabilità/frequenza con cui il rischio si può verificare
b) **G**: gravità delle conseguenze dovute al verificarsi del rischio identificato
c) **R**: possibilità che il verificarsi del rischio possa essere intercettato/individuato dalle misure di controllo presenti nel sistema

dando un giudizio qualitativo su una scala da 3 a 1 (alto, medio, basso) secondo lo schema della tabella seguente:

P - Probabilità	G – Gravità	R - Rilevabilità
3 alta probabilità: almeno 1 volta al mese	3 effetti gravi: danno economico oltre 50.000€	3 bassa rilevabilità (es. mi accorgo solo dopo che l'evento sia accaduto)
2 media probabilità: entro 6 mesi	2 effetti medi: danno economico oltre 10.000€	2 media rilevabilità (mi accorgo nel momento in cui accade)
1 bassa probabilità: oltre 6 mesi	1 effetti modesti: danno economico inferiore a 10.000€	1 alta rilevabilità (mi posso accorgere prima che l'evento accada)

Calcolate quindi l' **IPR** (Indice di Priorità di Rischio: G*P*R) e almeno per i rischi con indice più elevato (circa il 20% del totale), definite delle possibili contromisure/ azioni di miglioramento

Esempio di tabella FMEA

Tabelle per la valutazione dei rischi e per la valutazione successiva,
una volta adottate le contromisure
(es. *nel Riesame diDirezione*)

Nel caso di contromisure già in essere, se ne valuterà comunque l'efficacia

Gestione dei rischi connessi con i processi "xxx"

Processo e Fase del processo	Rischio connesso	P	G	R	IPR	Contromisure	Già in essere	Da Attuare	Evidenze	Considerazioni sull'efficacia
1.										
2.										
3.										
4.										
5.										
6.										

Rischi e Minacce

Esempi di rischi riferibili al contesto/parti interessate:

- Interruzione di forniture
- Furti di materiale
- Perdita o furto di dati e informazioni
- Non recepimento di nuove leggi e regolamenti
- Incendi, allagamenti, , inacessibilità della sede, interruzione prolungata dell'erogazione elettrica e di gas…
- Malattie/epidemie/indisposizioni

Gestione del rischio e Business Impact Analisys

- Riduzione % rischi a livello alto e medio
- Con riferimento alla Business Impact Analysis e in termini di :

MAO – Maximun Acceptable Outage, termine equivalente al MTPD – Maximun Tolerable Period of Disruption: oltre questo periodo l'esistenza dell'organizzazione sarà minacciata irrevocabilmente se le sue attività critiche per il business non possono essere ripristinati.

RTO – Recovery Time Objective: massimo periodo di indisponibilità delle attività critiche per il business, ovvero tempo entro il quale le attività critiche per il business devono essere ripristinate.

RPO – Recovery Point Objective: perdita dati sostenibile, in termini di distanza temporale tra il verificarsi dell'emergenza e l'ultimo salvataggio utile e ripristinabile dei dati (full back up e aggiornamenti successivi).

d) Misura

- Se non possiamo esprimere ciò che sappiamo su un processo in numeri, non ne sappiamo molto
- Se non sappiamo molto su un processo, non possiamo controllarlo
- Se non possiamo controllarlo, siamo in balia del caso

“Se non possiamo misurare, non possiamo migliorare”

Genichi Taguchi

Ma quali misure/monitoraggi?

- Monitoraggi eventi applicativi
- Monitoraggi sulle utenze
- Monitoraggi sugli asset
- Test sul disaster recovery
- Monitoraggi a cura di 3° parti
- Monitoraggi sugli accessi

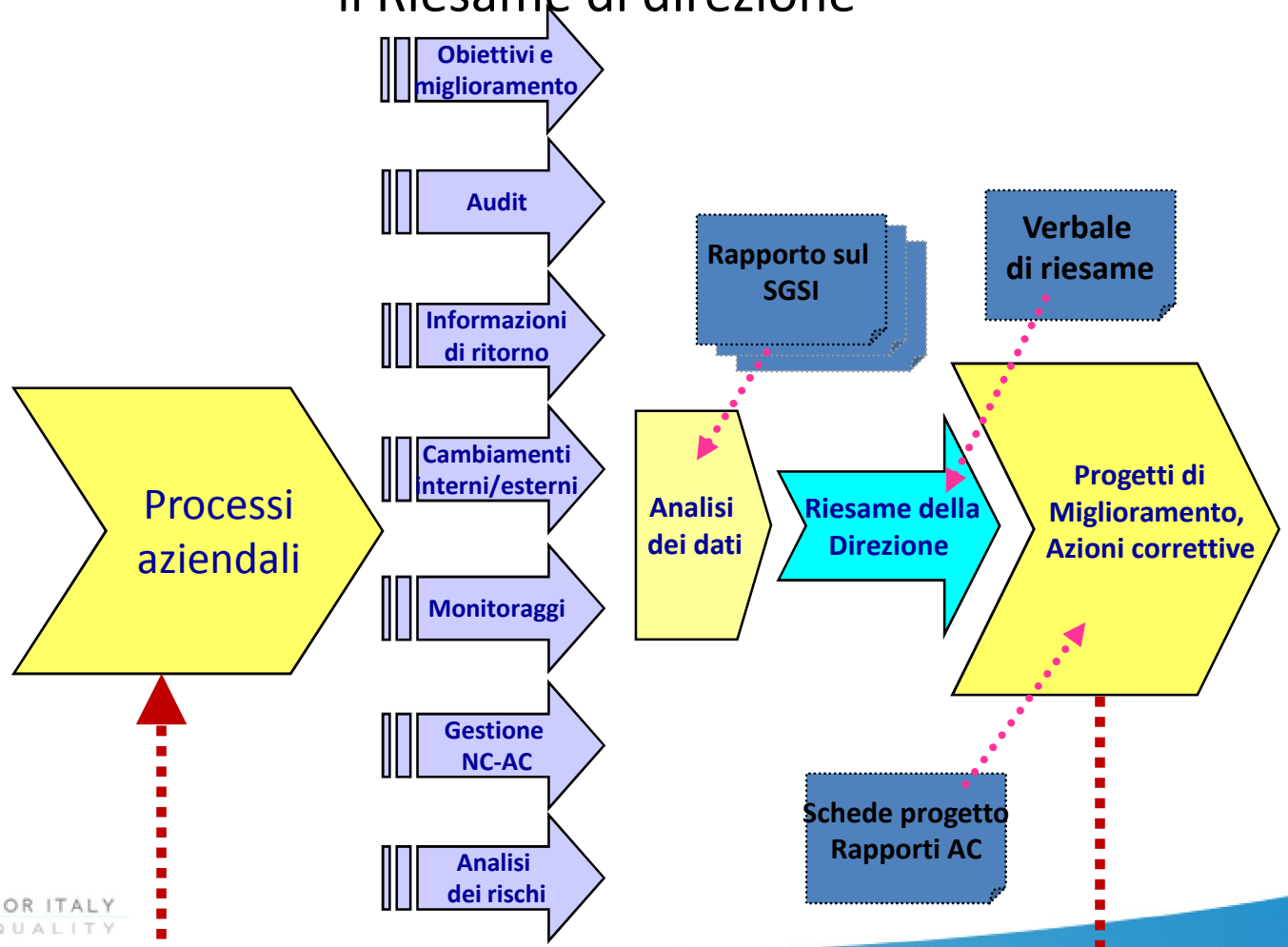
e) Leadership

La Direzione deve dimostrare leadership e commitment:

- in linea con la ragion d'essere dell'Organizzazione,
- secondo le strategie e il contesto nel quale opera,
- assicurando le risorse,
- garantendo dell'efficacia del SGSI,
- coinvolgendo il personale.

La norma accentua ed assegna un ruolo più proattivo alla Direzione per la Gestione del SGSI, allo scopo di favorire l'integrazione fra sistema di gestione reale e sistema di gestione per la sicurezza delle informazioni

il Riesame di direzione



f) Stakeholders

Non solo i **Clienti**, ma tutti i **Portatori di interesse:**

occorre comprendere i bisogni e le aspettative delle parti interessate e far si che questi indirizzino le pertinenti azioni del SGSI.

Stakeholders:

- Proprietà
- Management
- Clienti
- Fornitori
- Personale interno
- …

g) Miglioramento

Le organizzazioni devono dimostrare di aver innescato un processo di miglioramento :

- sistematico
- incrementale

del SGSI in essere

Risposta alle esigenze di sicurezza delle informazioni

Esigenze crescenti

MIGLIORAMENTO CONTINUO

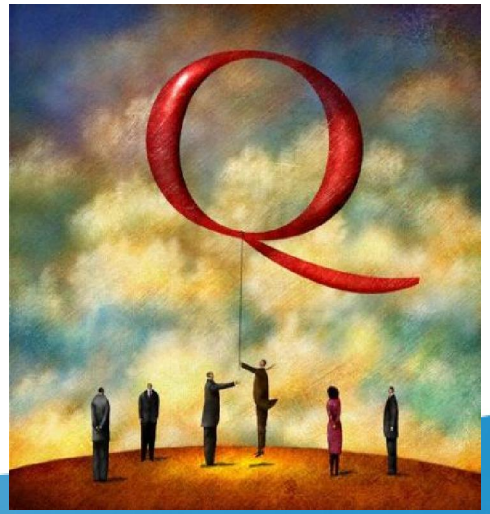
Contenuti

1. La sicurezza delle informazioni

2. Le Logiche e i vantaggi di un Sistema di Gestione

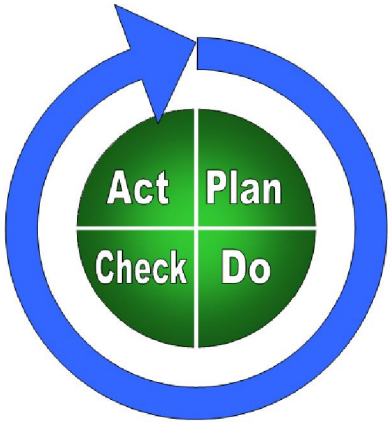
3. La norma ISO 27001:
   la struttura di riferimento e i requisiti

4. La visita di certificazione ISO 27001



Struttura della ISO 27001:2013

- **Applicabile a realtà di ogni dimensione**
- **Quasi 20 anni di esistenza sul mercato**
- **Ambito definibile a piacimento**
- **Approccio ciclico (PDCA)**
- **Costituisce un framework completo**
- **Dice cosa fare, non come farlo**
- **Rivolto al miglioramento continuo**
- **E' un riferimento universale e certificabile**
- **Integrazione ed allineamento con le altre norme ISO che specificano i requisiti di un modello di Sistema di Gestione per la Qualità, per l'Ambiente, per la Sicurezza, ecc.**



Struttura della ISO 27001:2013

Punti chiave

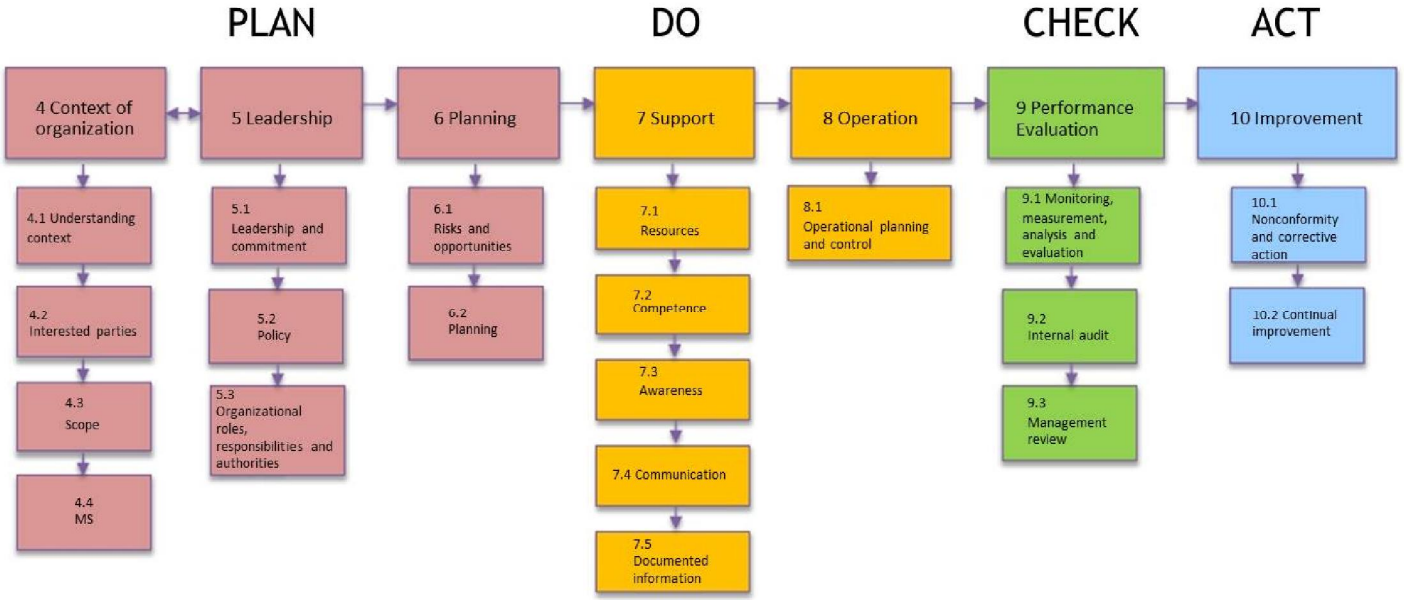
- il concetto di **informazione** (o risorsa informativa) con relativa valorizzazione;
- la valutazione dei **rischi** coerentemente al contesto di riferimento;
- gli aspetti **economico-finanziari** inerenti la Sicurezza delle Informazioni;
- l'aspetto **organizzativo** (e non solo **tecnologico**) della Sicurezza delle Informazioni;
- **l'efficacia** del SGSI e delle **contromisure** adottate per trattare i rischi.
- Di fondamentale importanza è l'**Annex A** che contiene i **114 "controlli"** (o contromisure) a cui, l'organizzazione che intende applicare la norma, deve attenersi.

Struttura della ISO 27001:2013

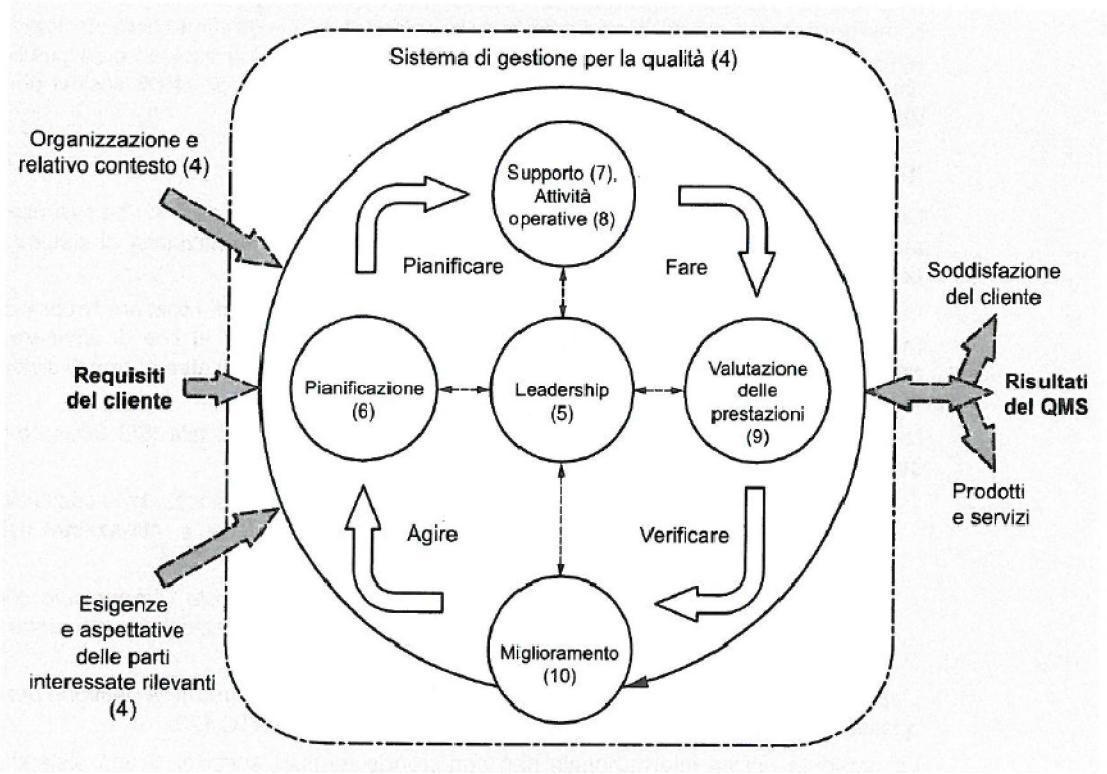
I 114 "controlli" riguardano :

- **la politica e l'organizzazione per la sicurezza delle informazioni**
- **la sicurezza delle risorse umane**
- **la gestione degli asset**
- **il controllo degli accessi logici**
- **la crittografia**
- **la sicurezza fisica e ambientale**
- **la sicurezza delle attività operative**
- **la sicurezza delle comunicazioni**
- **la gestione della sicurezza applicativa**
- **la relazione con i fornitori coinvolti nella gestione della sicurezza delle informazioni**
- **il trattamento degli incidenti (relativi alla sicurezza delle informazioni)**
- **la gestione della Business Continuity**
- **il rispetto normativo**

HLS – Struttura base



Rappresentazione della struttura della norma nel ciclo PDCA



Nota: I numeri tra parentesi fanno riferimento ai punti della norma internazionale ISO 27001

I paragrafi della 27001: 2013 e l'Annex A

1. Scopo
2. Referenze normative
3. Termini e definizioni
4. Contesto dell'organizzazione
5. Leadership
6. Pianificazione
7. Supporto
8. Attività Operative
9. Valutazione delle prestazioni
10. Miglioramento

5. Information security policies
6. Organisation of information security
7. Human Resources Security
8. Asset management
9. Access control
10. Cryptography
11. Physical and environmental security
12. Operations security
13. Communications security
14. Systems acquisition, development and maintenance
15. Supplier Relationships
16. Information Security incident Management
17. IS aspects of business continuity
18. Compliance

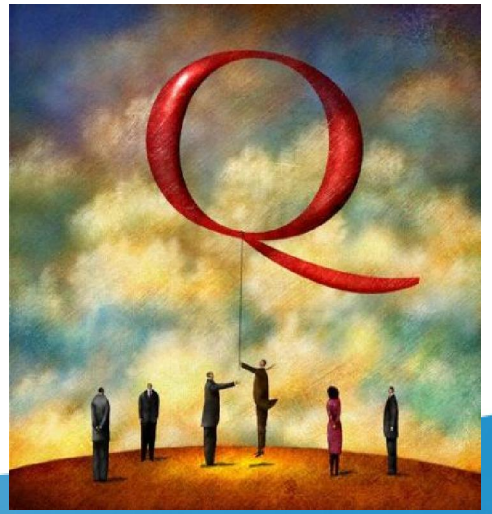
Contenuti

1. La sicurezza delle informazioni

2. Le Logiche e i vantaggi di un Sistema di Gestione

3. La norma ISO 27001:
   la struttura di riferimento e i requisiti

4. La visita di certificazione ISO 27001



La visita di certificazione

Si articola in 2 step:

- **Stage 1** – verifica documentale
- **Stage 2** – Verifica effettiva sul campo

ACCREDIA
L'ENTE ITALIANO DI ACCREDITAMENTO

Stage 1

- **Stage 1 –** verifica documentale
- **Documenti indispensabili**
  - Politica per la sicurezza delle informazioni
  - Analisi dei rischi
  - SOA
  - Audit interni
  - Riesame di Direzione