

Strumenti operativi per la sicurezza delle Informazioni negli studi professionali

ODCEC Roma

Commissione Informatica e Qualità

Roma 9 novembre 2020

La nostra professione nella storia

Fra Luca Pacioli ritratto da Jacopo de Barberi con Guidobaldo, Duca di Urbino.

Notare nella parte superiore sinistra un rombo-cubododecaedro mentre sul tavolo a destra in basso si nota un solido regolare, dodecaedro platonico.



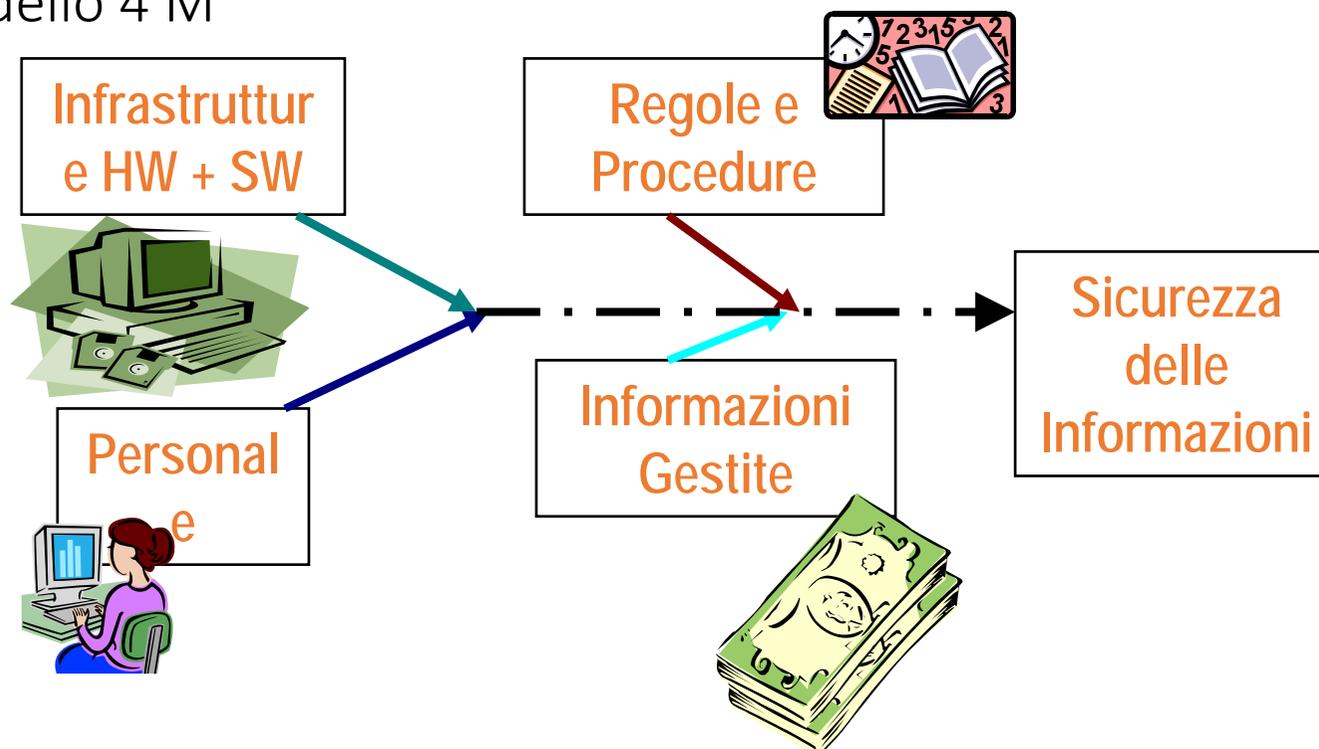
Qualità della Informazione => Qualità del Prodotto/Servizio

Caratteristiche Esplicite : le informazioni di uso del servizio/prodotto, informazione come oggetto della transazione

Normalmente Implicite : la riservatezza e la sicurezza della transazione

Cogenti : GDPR – Normativa in materia di Cyber crime

Il Modello 4 M



La Sicurezza nel modello 4M

Macchine (HW) : Sistemi di Sicurezza HW e SW

Metodi : Procedure Sicure, Coinvolgimento del Cliente

Manodopera : Fedeltà del Personale,

Materia prima (Informazioni Input) : Qualità del dato

Di Cosa stiamo parlando

Sistema di Gestione : Sistema per stabilire politica ed obiettivi e per conseguire tali obiettivi.

+

Sicurezza delle Informazioni : Mantenimento di disponibilità, integrità e riservatezza dell'informazione. possono essere inoltre coinvolte altre proprietà quali autenticità, responsabilità, non ripudio ed affidabilità

=

Sistema di Gestione della Sicurezza delle informazioni (SGSI)

Definizione di Rischio secondo ISO 31000

RISCHIO: Effetto dell'incertezza sugli obbiettivi

Un effetto è uno scostamento da quanto atteso – positivo e/o negativo

Gli obbiettivi possono presentare aspetti differenti (come scopi finanziari, di salute e sicurezza, ambientali) e possono intervenire a livelli differenti (come progetti, prodotti e processi strategici, riguardanti l'intera organizzazione)

Il rischio è spesso caratterizzato dal riferimento a **eventi** potenziali e **conseguenze**, o una combinazione di questi

Il rischio è spesso espresso in termini di combinazione delle conseguenze di un evento (compresi cambiamenti nelle circostanze) e della **verosimiglianza** del suo verificarsi

L'incertezza è lo stato, anche parziale, di assenza di informazioni relative alla comprensione o conoscenza di un evento, delle sue conseguenze o della loro verosimiglianza.



Ordine dei
Dottori Commercialisti e degli
Esperti Contabili di
Roma

Ragioniamo sul concetto di Rischio

Incertezza dei risultati e rischi connessi



FONDAZIONE
TELOS
CENTRO STUDI DELL'ORDINE
DEI DOTTORI COMMERCIALISTI
E DEGLI ESPERTI CONTABILI
DI ROMA

In genere il "rischio" è sempre stato considerato come un aspetto negativo. Il termine "rischio del processo" è qui utilizzato con lo stesso significato di "incertezza", che ha cioè aspetti sia negativi, che positivi.

La gestione del rischio è finalizzata a :

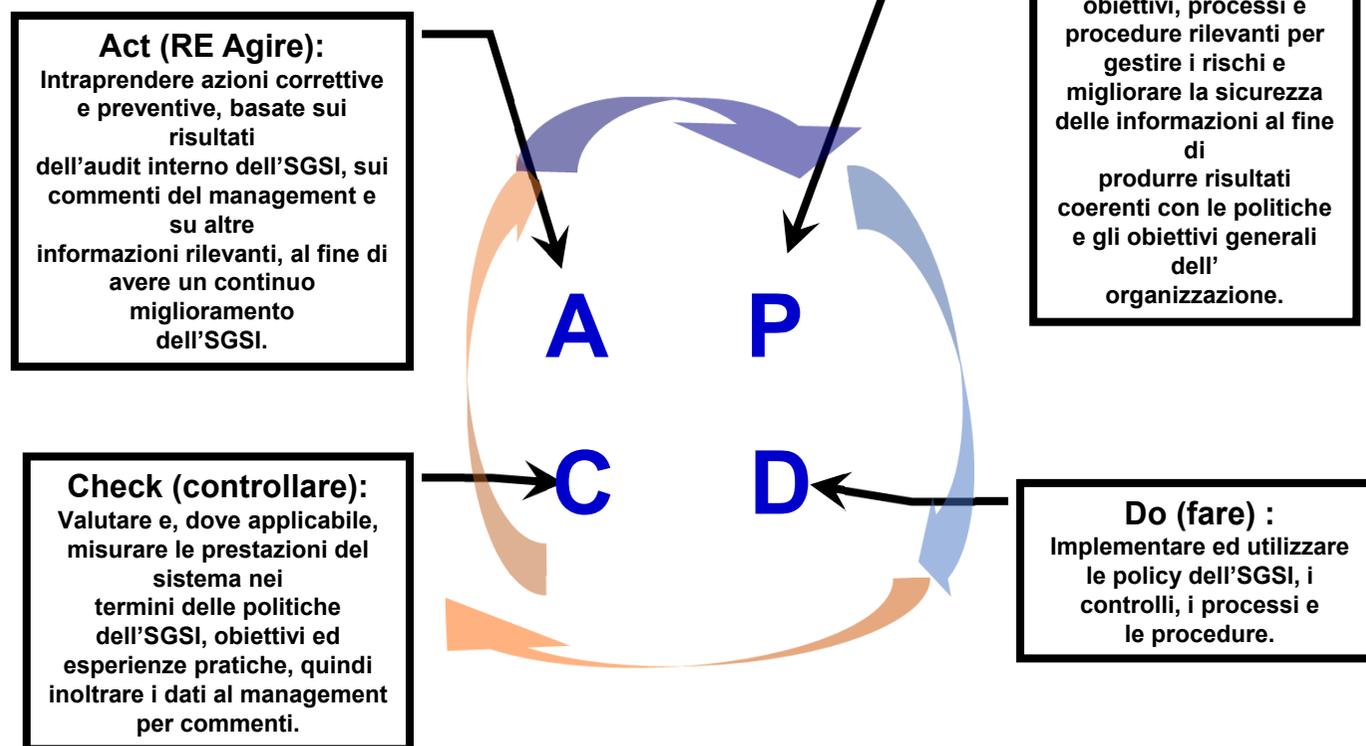
ridurre al minimo l'impatto di eventi potenziali negativi

ed, eventualmente,

trarre pieno vantaggio dalle opportunità.

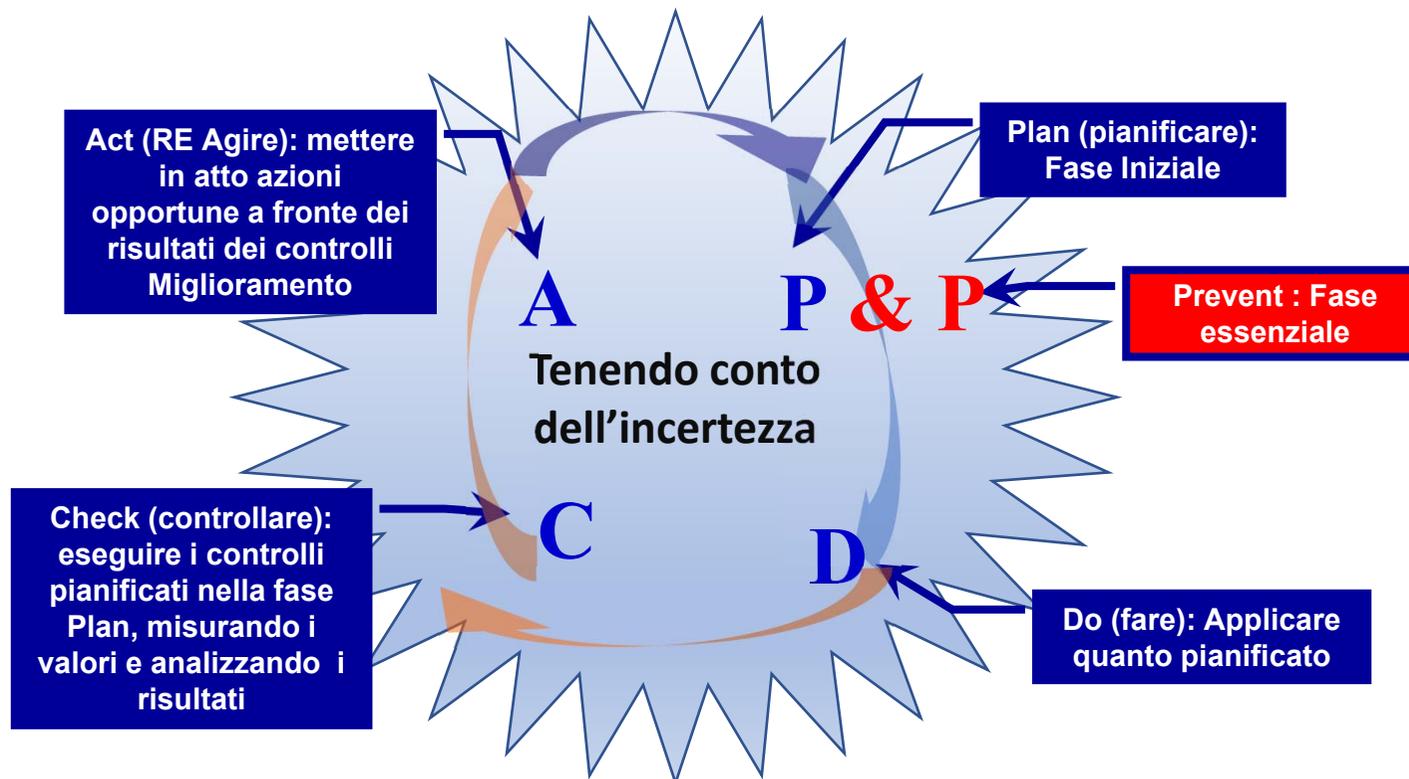


Tramite questo approccio





Tenendo conto dell'incertezza e ..





ISO 27001:13 Sistema di Gestione della Sicurezza delle Informazioni

La norma stabilisce i requisiti per stabilire, sviluppare, mettere in atto, controllare, riesaminare, mantenere in esercizio e migliorare un documentato Sistema di Gestione della Sicurezza delle Informazioni (SGSI) all'interno delle organizzazioni e relativo a tutti i rischi (*informativi*) presenti nelle attività. La norma specifica i requisiti per lo sviluppo e la messa in atto di controlli di sicurezza personalizzati sulle necessità delle singole organizzazioni e di parte di esse.

Il SGSI è sviluppato per assicurare la messa in atto di controlli sulla sicurezza adeguati e proporzionati in modo tale da

- Assicurare una protezione delle risorse informative
- Fornire ai clienti ed alle altre parti interessate la evidenza che tali rischi sono adeguatamente gestiti

Questo può essere trasferito nel mantenimento, nello sviluppo del vantaggio competitivo, dei flussi di cassa, della profittabilità, del rispetto di normativa cogente e dell'immagine sul mercato .



Ordine dei
Dottori Commercialisti e degli
Esperti Contabili di
Roma



FONDAZIONE
TELOS
CENTRO STUDI DELL'ORDINE
DEI DOTTORI COMMERCIALISTI
E DEGLI ESPERTI CONTABILI
DI ROMA

Ovvero ?

Quella parte del sistema di gestione (aziendale)

basata su un approccio rivolto al rischio di business,

**Orientata a impostare, implementare, utilizzare,
monitorare, rivedere, mantenere e migliorare la
sicurezza delle informazioni.**

Sistema di Gestione..... Non solo ICT !



ISO 27001:13 - Elementi del SGSI

4	CONTESTO DELL'ORGANIZZAZIONE
4.1	Comprendere l'organizzazione e il suo contesto.....
4.2	Comprendere le necessità e le aspettative delle parti interessate
4.3	Determinare il campo di applicazione del sistema di gestione per la sicurezza delle informazioni.....
4.4	Sistema di gestione per la sicurezza delle informazioni.....
5	LEADERSHIP
5.1	Leadership e impegno.....
5.2	Politica
5.3	Ruoli, responsabilità e autorità nell'organizzazione.....
6	PIANIFICAZIONE
6.1	Azioni per affrontare rischi e opportunità.....
6.2	Obiettivi per la sicurezza delle informazioni e pianificazione per conseguirli.....

Contesto di oggi

L'unica certezza è che

Operiamo nell'incertezza

- Alcuni esempi :
 - Per Noi Professionisti
 - Dlgs 231/07 : Rischi di riciclaggio
 - D.Lgs. 39/2010 : Rischi legati alla revisione legale
 - GDPR 2016/679: rischi di corruzione delle informazioni
 - Dlgs 81/08 : Rischi legati agli infortuni
 - Per i nostri clienti :
 - Dlgs 231/01 : Rischi di accadimento del reato presupposto
 - GDPR 2016/679 : rischi di corruzione delle informazioni
 - Dlgs 81/08 : Rischi legati agli infortuni

L'incertezza è una componente della nostra Professione



Evoluzione del contesto Tecnologico

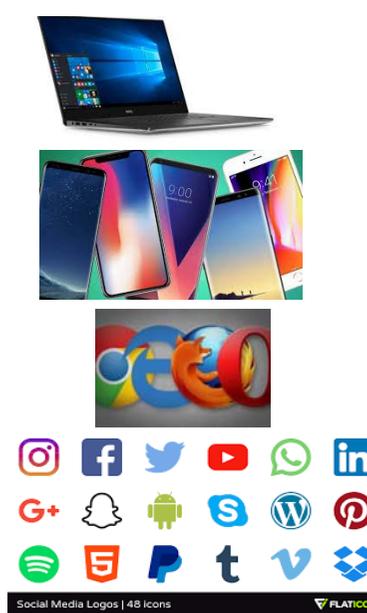
1996



2003



2020





Evoluzione del contesto Normativo

1996

2003

31/12/2018

01/01/2019



DEMO SRL
P.IVA 025514032112
VIA S. CAPPELLO 26 90123 PALERMO (PA)
Tel. 091456 Cell. 333151012
E-mail luca.lopresti@emotori.com

Spett.le
COSTA ENRICO
VIA FRANZIA, 41
20052 MONZA (MB)

Preventivo
Num. 32 Del 15/01/2018 Pagina 1 C. Fiscale: CSTNRC85M01R741T

Marca	Modello	Targa/Telaio	Km Entrata	Immatricolazione	Prossima Revisione
SMART	SMART & PASSION	BE076HM WME01MC01XH054226		09/07/1999	02/05/2018

Codice	Descrizione	Qta/Ore	Prezzo	Sc. 1	Sc. 2	Imp. Sc.	IVA
	PERDITA OLIO						
	SOSTITUZIONE INTERRUTTORE A PRESSIONE OLIO	0,20	35,00	20,00		5,60	22
7532034	INTERRUTTORE A PRESSIONE OLIO	1,00	1,00	10,00		0,90	22
	SOSTITUZIONE COPPA OLIO	0,70	35,00	20,00		19,60	22
3015V0030000	COPPA OLIO	1,00	27,46	10,00		24,71	22



Carta fino al 31/12/18 e poi LA mitica FE



Evoluzione del contesto Normativo Scontrini

1996

2003

31/12/2019

01/01/2020



Carta fino al 31/12/19 e poi ... TTFT



Ordine dei
Dottori Commercialisti e degli
Esperti Contabili di
Roma

La gestione del Rischio – alcuni termini

Contesto esterno

Ambiente esterno nel quale l'organizzazione cerca di conseguire i propri obiettivi,

Lo subiamo

Contesto interno

Ambiente interno nel quale l'organizzazione cerca di conseguire i propri obiettivi,

Lo dobbiamo gestire

Gestire l'incertezza





Sistema di Gestione Basato sulla Prevenzione dei Rischi



Capire il contesto : come gestire gli impatti dei cambiamenti nei processi di Studio e sulla qualità del servizio professionale.

Fatti Noti che si sanno

Fatti non noti che si sanno

Fatti non noti che non si sanno

Fatti noti che NON SI SANNO



**Ordine dei
Dottori Commercialisti e degli
Esperti Contabili di
Roma**



**FONDAZIONE
TELOS**
CENTRO STUDI DELL'ORDINE
DEI DOTTORI COMMERCIALISTI
E DEGLI ESPERTI CONTABILI
DI ROMA

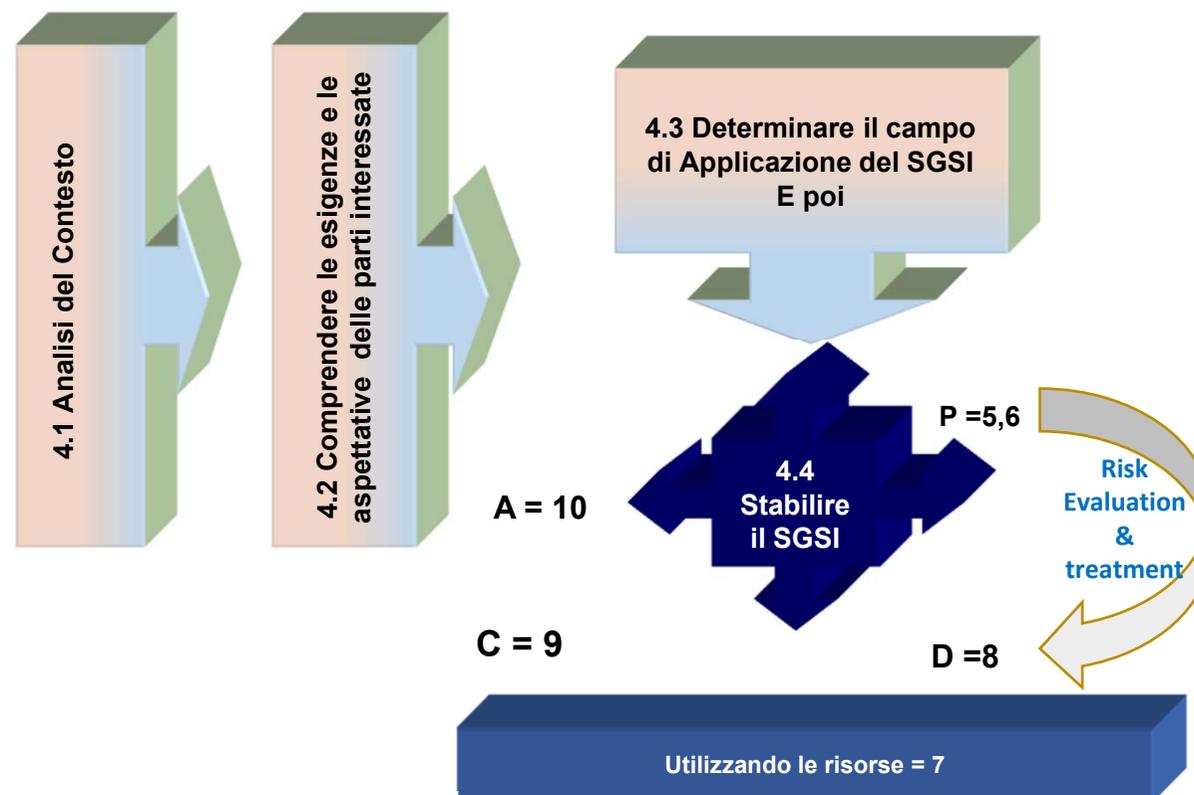
In pratica



CIQ ODCEC ROMA Anno 2020 - Non Divulgabile - USO ESCLUSIVO ISCRITTI

VF 21

Lo sviluppo del SGSI 27001



Pianificazione, Valutazione e trattamento dei rischi

6.1.2 Valutazione del rischio relativo alla sicurezza delle informazioni

6.1.3 Trattamento del rischio relativo alla sicurezza delle informazioni

Rispetto ai controlli dell'Annex A



ISO 27001:13 - Elementi del SGSI

7	SUPPORTO
7.1	Risorse.....
7.2	Competenza
7.3	Consapevolezza
7.4	Comunicazione
7.5	Informazioni documentate.....
8	ATTIVITÀ OPERATIVE
8.1	Pianificazione e controllo operativi
8.2	Valutazione del rischio relativo alla sicurezza delle informazioni...
8.3	Trattamento del rischio relativo alla sicurezza delle informazioni ..
9	VALUTAZIONE DELLE PRESTAZIONI
9.1	Monitoraggio, misurazione, analisi e valutazione.....
9.2	Audit interno.....
9.3	Riesame di direzione
10	MIGLIORAMENTO
10.1	Non conformità e azioni correttive
10.2	Miglioramento continuo



Ordine dei
Dottori Commercialisti e degli
Esperti Contabili di
Roma



I controlli applicabili - Overview

Quelli descritti di seguito sono i controlli che la norma indica quali misure di contenimento dei rischi relativi alle informazioni.

Possono non essere sempre tutti applicabili

Ed infatti vedremo poi quali sono i più importanti per lo studio professionale



ISO 27001:13 - Elementi del SGSI - Controlli

5	POLITICHE PER LA SICUREZZA DELLE INFORMAZIONI
5.1	Indirizzi della direzione per la sicurezza delle informazioni
6	ORGANIZZAZIONE DELLA SICUREZZA DELLE INFORMAZIONI
6.1	Organizzazione interna.....
6.2	Dispositivi portatili e telelavoro
7	SICUREZZA DELLE RISORSE UMANE
7.1	Prima dell'impiego
7.2	Durante l'impiego
7.3	Cessazione e variazione del rapporto di lavoro
8	GESTIONE DEGLI ASSET
8.1	Responsabilità per gli asset.....
8.2	Classificazione delle informazioni.....
8.3	Trattamento dei supporti.....

ISO 27001:13 - Elementi del SGSI - Controlli

9	CONTROLLO DEGLI ACCESSI
9.1	Requisiti di business per il controllo degli accessi
9.2	Gestione degli accessi degli utenti
9.3	Responsabilità dell'utente
9.4	Controllo degli accessi ai sistemi e alle applicazioni
10	CRITTOGRAFIA
10.1	Controlli crittografici
11	SICUREZZA FISICA E AMBIENTALE
11.1	Aree sicure
11.2	Apparecchiature

ISO 27001:13 - Elementi del SGSI - Controlli

12	SICUREZZA DELLE ATTIVITÀ OPERATIVE
12.1	Procedure operative e responsabilità
12.2	Protezione dal malware
12.3	Backup
12.4	Raccolta di log e monitoraggio
12.5	Controllo del software di produzione
12.6	Gestione delle vulnerabilità tecniche.....
12.7	Considerazioni sull'audit dei sistemi informativi.....
13	SICUREZZA DELLE COMUNICAZIONI
13.1	Gestione della sicurezza della rete
13.2	Trasferimento delle informazioni



ISO 27001:13 - Elementi del SGSI - Controlli

14	ACQUISIZIONE, SVILUPPO E MANUTENZIONE DEI SISTEMI	55
14.1	Requisiti di sicurezza dei sistemi informativi	55
14.2	Sicurezza nei processi di sviluppo e supporto.....	58
14.3	Dati di test.....	63
<hr/>		
15	RELAZIONI CON I FORNITORI	64
15.1	Sicurezza delle informazioni nelle relazioni con i fornitori.....	64
15.2	Gestione dell'erogazione dei servizi dei fornitori.....	67
<hr/>		
16	GESTIONE DEGLI INCIDENTI RELATIVI ALLA SICUREZZA DELLE INFORMAZIONI	68
16.1	Gestione degli incidenti relativi alla sicurezza delle informazioni e dei miglioramenti	68



ISO 27001:13 - Elementi del SGSI - Controlli

17	ASPETTI RELATIVI ALLA SICUREZZA DELLE INFORMAZIONI NELLA GESTIONE DELLA CONTINUITÀ OPERATIVA	72
17.1	Continuità della sicurezza delle informazioni	72
17.2	Ridondanze.....	74
18	CONFORMITÀ	75
18.1	Conformità ai requisiti cogenti e contrattuali.....	75
18.2	Riesami della sicurezza delle informazioni.....	78

La Documentazione del SGSI

L'elenco della Documentazione necessaria è contenuto nel requisito 7.5

- a) Dichiarazioni documentate circa la Politica della Sicurezza e gli obiettivi del SGSI**
- b) Il campo di applicazione del SGSI e le procedure ed controlli documentati necessari per il SGSI;**
- c) Le registrazioni relative alla attività di Valutazione dei Rischi;**
- d) il Piano di gestione dei Rischi;**
- e) Le Informazioni Documentate necessarie all'organizzazione per assicurare la efficace pianificazione, funzionamento e controllo dei propri processi di gestione della sicurezza delle informazione;**
- f) Il Documento di Gestione (Statement of applicability)**

Tutta la documentazione deve essere resa disponibile in accordo secondo i requisiti della Politica del SGSI

Naturalmente la estensione della documentazione dipende sia dalle dimensioni e dal tipo di attività svolte dall'organizzazione che dal campo di applicazione e dalla complessità dei requisiti del SGSI che si deve sviluppare - Formato dei documenti "libero".

In conclusione

L'adozione della ISO 27001:13 ha lo scopo di garantire:

- **la conformità,**
- **l'efficacia,**

della sicurezza delle informazioni all'interno di una organizzazione (pubblica o privata).

Sicurezza delle informazioni intesa come:

- **Riservatezza,**
- **Integrità,**
- **Disponibilità.**

Efficacia intesa come:

- **continuità del business,**
- **minimizzazione dei danni in caso di incidenti,**
- **massimizzazione degli investimenti e miglioramento dell'efficacia.**



Selezione delle opzioni di Trattamento del Rischio

Criteri di Selezione :

Bilanciamento delle esigenze

Analisi costi e benefici

Economie di Scala tra i trattamenti

Coinvolgimento con i diversi portatori di interesse

Competenze e Conoscenze

Rischi secondari sorgenti

Aspetti del Trattamento

Il piano di trattamento dovrebbe identificare chiaramente l'ordine di priorità in cui i singoli trattamenti del rischio dovrebbero essere attuati.

Il trattamento stesso del rischio può introdurre rischi.

Un rischio significativo può essere il fallimento o l'inefficacia delle misure di trattamento.

È necessario che il monitoraggio sia una parte integrante del piano di trattamento del rischio per assicurare che le misure rimangano efficaci



**Ordine dei
Dottori Commercialisti e degli
Esperti Contabili di
Roma**



Ed ora ?

Con i successivi interventi dei relatori cercheremo di contestualizzare quanto fin qui condiviso.

Grazie per l'attenzione