

Roma, 20 aprile 2016

Il percorso di certificazione ISO/IEC 27001:2013

***Alla base di un nuovo modello di gestione
del processo-sicurezza***

Francesco Ciclosi

***(Responsabile UNICAM del Sistema di Gestione della
Sicurezza delle Informazioni)***

Come tutto ebbe inizio ...

II° Semestre 2012



Il dott. Paolo Gaspari,
già Direttore Tecnico
del CINFO



Avvia il processo
di certificazione



Primo quesito

- Un organizzazione certificata ISO/IEC 27001 è un'organizzazione sicura?
 - VERO
 - FALSO



Secondo quesito

- Lo standard ISO/IEC 27001 misura il livello o la qualità della sicurezza di un'organizzazione?
 - VERO
 - FALSO



Terzo quesito

- Lo standard ISO/IEC 27001 e la relativa certificazione sono dei meri adempimenti formali che non servono a migliorare il livello o la qualità della sicurezza di un'organizzazione?
 - VERO
 - FALSO

Prima risposta: FALSO

- Un organizzazione certificata ISO/IEC 27001 è un'organizzazione sicura?
- Non è vero che il possesso della certificazione ISO/IEC 27001 garantisce la sicurezza del possessore
- In generale dal possesso della **certificazione non è possibile inferire nulla** in merito al **livello di sicurezza** del possessore

Seconda risposta: FALSO

- Lo standard ISO/IEC 27001 misura il livello o la qualità della sicurezza di un'organizzazione?
- Lo standard ISO/IEC 27001
 - non misura il livello o la qualità della sicurezza
 - da indicazioni sul modo di operare per gestire la sicurezza

Terza risposta: FALSO

- Lo standard ISO/IEC 27001 e la relativa certificazione sono dei meri adempimenti formali che non servono a migliorare il livello o la qualità della sicurezza di un'organizzazione?
- Lo standard richiede l'adozione di policy anche se il grado di libertà è enorme (dal quasi niente al quasi tutto), la differenza la fa l'ente certificatore che non verifica solo la presenza del cartaceo, bensì avvia la sua analisi a partire da questo e dall'analisi del rischio

Lo scopo dello standard ISO 27001

- È quello di certificare la qualità della gestione dei processi di sicurezza
- Non quello di certificare la qualità delle soluzioni, delle tecnologie o delle configurazioni adottate
- Eredita l'approccio degli standard di qualità dei processi industriali (ISO 9000 family):
 - focus non sulla qualità dello strumento, ma sulla qualità del processo di gestione dello strumento

Il trattamento del rischio

- È richiesta la definizione di un processo di security risk threatment (conforme ISO 27005:2011) per:
 - Determinare tutti i controlli necessari a implementare il trattamento del rischio ritenuto appropriato
 - Paragonare tali controlli con quelli definiti nell'Annex A, verificando la non omissione di quelli necessari
 - Produrre una SOA – Statement of Applicability
 - Formulare un piano di trattamento del rischio complessivo
 - Ottenere l'approvazione del piano di trattamento del rischio e del rischio residuo dai **RISK OWNER**

Annex A – Reference control objectives and controls

- È la sezione della norma dove sono definiti
 - i controlli
 - i corrispondenti obiettivi
- che rappresentano i requisiti richiesti per la conformità del SGSI con lo standard

Annex A	ISO 27001:2005	ISO 27001:2013
N°. Aree di controllo	11	14
N°. Obiettivi di controllo	39	35
N°. Controlli	133	114

I controlli

- Sono divisi in **sezioni** tematiche di ampio respiro
 - Che coprono gli aspetti tecnologici, la sicurezza logica e fisica, le risorse umane, i processi aziendali, ecc.
- Ogni sezione ha una o più **sottosezioni**
- Ogni sottosezione è organizzata con:
 - Un **Obiettivo generale** e una relativa breve descrizione
 - Una o più coppie del tipo **Controllo/Obiettivo del controllo**

Definizione del perimetro del SGSI

- Prima fase di studio e ricognizione per definire:
 - del perimetro del SGSI
 - del campo di applicazione (SOA) con i limiti e le eventuali esclusioni
- → **Ambito di certificazione: «Erogazione di servizi di connettività, posta elettronica, portale web, telefonia, hosting e gestionali per l'Ateneo e per la clientela che lo richiedesse»**

Analisi dei principali servizi erogati

- Con attenzione a organizzazione, infrastrutture, dati, dispositivi, reti e tecnologie di supporto.
- Per ogni servizio è stato definito un asset tree per mappare la sua articolazione e contenente sei entità informative

IF (Informazioni)	SW (Software)
HW (Hardware)	COM (Apparati di comunicazione)
L (Luoghi)	P (Persone - Risorse umane)

Individuazione degli stakeholders

- Con riferimento all'erogazione/fruizione dei servizi
 - studenti
 - personale docente
 - personale tecnico-amministrativo
 - personale esterno
 - soggetti pubblici
 - soggetti privati
 - utenti esterni

Definizione dell'infrastruttura documentale

- È costituita da un gruppo di norme regolamentari, ruoli e regole che determinano come le informazioni sono gestite, protette e distribuite nell'ateneo.
- Ogni documento tratta in modo specifico un singolo aspetto di sicurezza, descrivendolo sotto ogni possibile punto di vista

L'infrastruttura documentale

- È composta da 4+1 tipologie di documenti:
 - documenti di sistema (DS)
 - procedure organizzative (PO)
 - procedure tecniche (PT)
 - istruzioni operative (IOP)
 - registri elettronici (allegati a PO, PT e IOP)
- Ogni documento è classificato mediante l'indicazione di un numero progressivo

- Home
- My Page
- Attività
- SGSI**
- CIM
- CINFO
- Normativa
- CCNL/Codici/Regola...
- Ateneo
- Formazione
- SFT
- CLUSIT
- Avvisi
- Area Riservata
- Garr-cert
- Link Sicurezza
- Link Sicurezza
- Mappa del sito
- Attività personali recenti
- Area Riservata
allegato da Mail Francesco Ciclosi
- Accordi di riservatezza
allegato da Mail Francesco Ciclosi
- Area Riservata
allegato da Mail Francesco Ciclosi

SGSI

Biometria Sistema di Gestione della Sicurezza delle Informazioni - Documenti di Progetto

Il SGSI in uso presso il Centro Servizi Informatici e Sistemi Informativi è composto dalle seguenti tipologie di documenti:

- [Documenti di Sistema](#)
- [Procedure Operative](#)
- [Procedure Tecniche](#)
- [Istruzioni Operative](#)
- [Registri elettronici](#) (allegati alle PO, PT o IO)
- [Allegati](#)

Per poter consultare una qualsiasi delle precedenti tipologie di documento sarà sufficiente fare clic sul collegamento relativo.

A margine del sistema è possibile consultare le pratiche che il CINFO ha predisposto nel corso del processo propedeutico all'installazione di apparati di [videosorveglianza](#) e di rilevamento degli accessi mediante [biometria](#).

Per accedere ai verbali del SGSI --> [Clicca qui](#)

Per accedere agli accordi di riservatezza --> [Clicca qui](#)

Per accedere ai verbali di consegna chiavi --> [Clicca qui](#)

Per accedere ai contratti di assistenza ed ai livelli di servizio garantiti --> [Clicca qui](#)

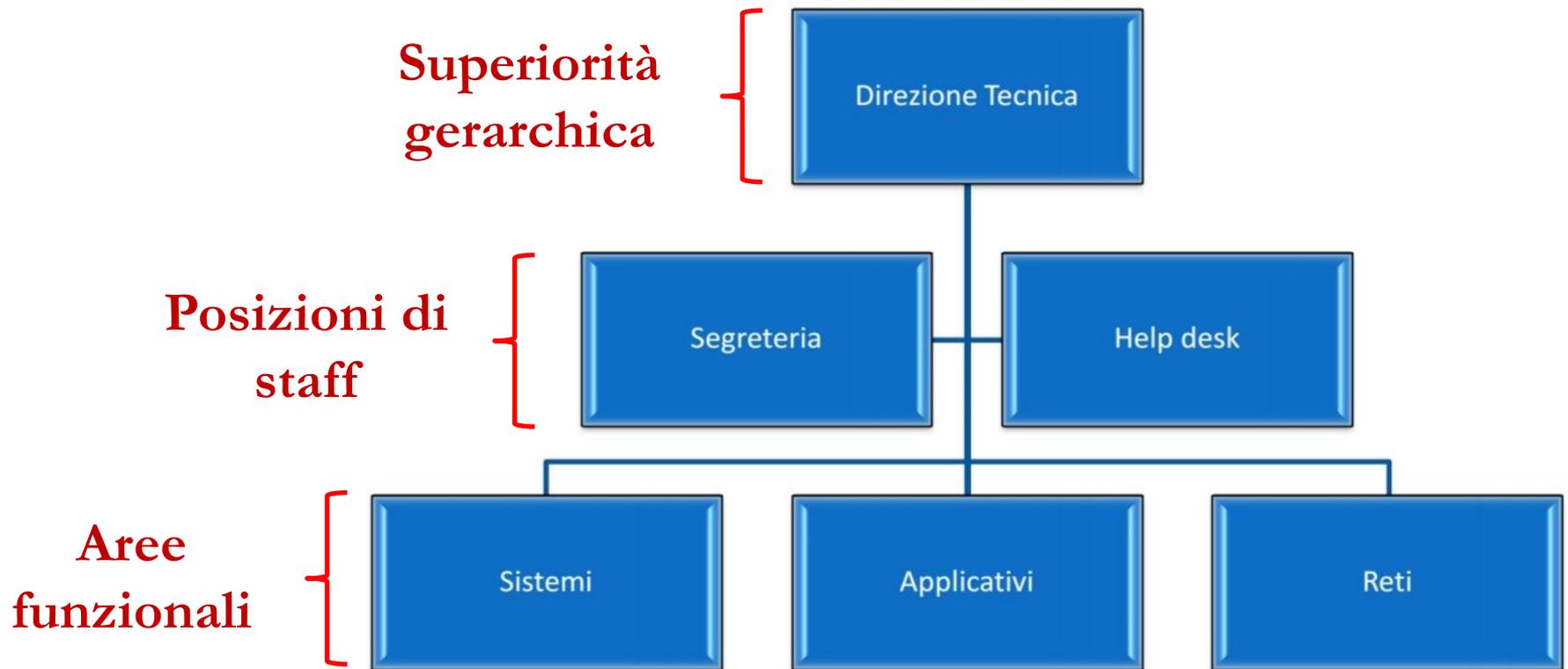
Pagine secondarie (14): [Accordi di riservatezza](#) [Allegati](#) [Biometria](#) [Consegna delle chiavi](#) [Contratti-SLA](#) [Documenti di sistema](#) [Evidenze](#) [Istruzioni Operative](#) [Procedure Operative](#) [Procedure Tecniche](#) [Registri elettronici](#) [SLA-Contratti](#) [Verbali](#) [Videosorveglianza](#)

Definizione della matrice di correlazione

- Tra gli obiettivi di controllo e i controlli (di cui all'Annex A) e l'applicabilità al perimetro del SGSI
- Identifica e dettaglia anche lo stato attuale di implementazione delle indicazioni dei controlli

Annex A - Obiettivi di controllo e controlli			Stato attuale	Applicabile	Note
A.5.1 Management direction for information security <i>Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.</i>					
A.5.1.1	Policies for information security	Control A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties.	DS 07 - Politica SGSI	SI	NOT NEW

Ridefinizione della struttura organizzativa



Strategia di analisi e valutazione del rischio

- È stata personalizzata e tarata sul perimetro oggetto del SGSI
- La metodologia adottata è stata quella di **Magerit** implementata con il tool software **Pilar**
- La metodologia scelta è conforme ai dettami dello standard ISO/IEC 27005:2011 «*Information security risk management*»
- L'approccio utilizzato si articola in 5 passaggi

Analisi del rischio: I° passaggio

- Definizione degli asset di rilievo per l'ateneo
 - Partendo dai dati e dai processi che li elaborano
 - Facendo attenzione alla «dipendenza tra gli asset»
- Divisione degli asset in 5 livelli
- Valorizzazione degli asset con scala qualitativa
 - Anche per ordinare tra loro gli asset in base al valore relativo

Analisi del rischio: II° passaggio

- **Determinazione di tutti i threat**
 - Che possono interessare le varie tipologie di asset
- **Abbinamento tra gruppi di asset e threat**
 - Non tutti i threat interessano tutti gli asset
 - Differenti asset interessati dallo stesso threat non lo subiscono necessariamente in tutte le sue dimensioni e allo stesso modo
- **Determinazione del livello di vulnerabilità di un asset**
 - Attraverso la **valorizzazione di frequenza e impatto**

Analisi del rischio: III° passaggio

- Provvedere in alla misurazione dell'esposizione di un asset a impatti e rischi
 - La misurazione è effettuata in via cautelativa, quindi si ipotizza il caso peggiore
 - L'approccio mostra cosa accadrebbe se tutte le contromisure fossero disattivate
- Le contromisure rientrano nel calcolo del rischio
 - **preventive**, riducono la frequenza dei threat
 - **contenitive**, limitano l'impatto causato

Analisi del rischio: IV^o passaggio

- Determinazione dell'impatto che i threat possono avere sul sistema
 - considerando il valore degli asset
 - considerando il livello di compromissione teorica
- Sono state utilizzate due tipologie di calcolo
 - impatto cumulativo
 - impatto riflesso

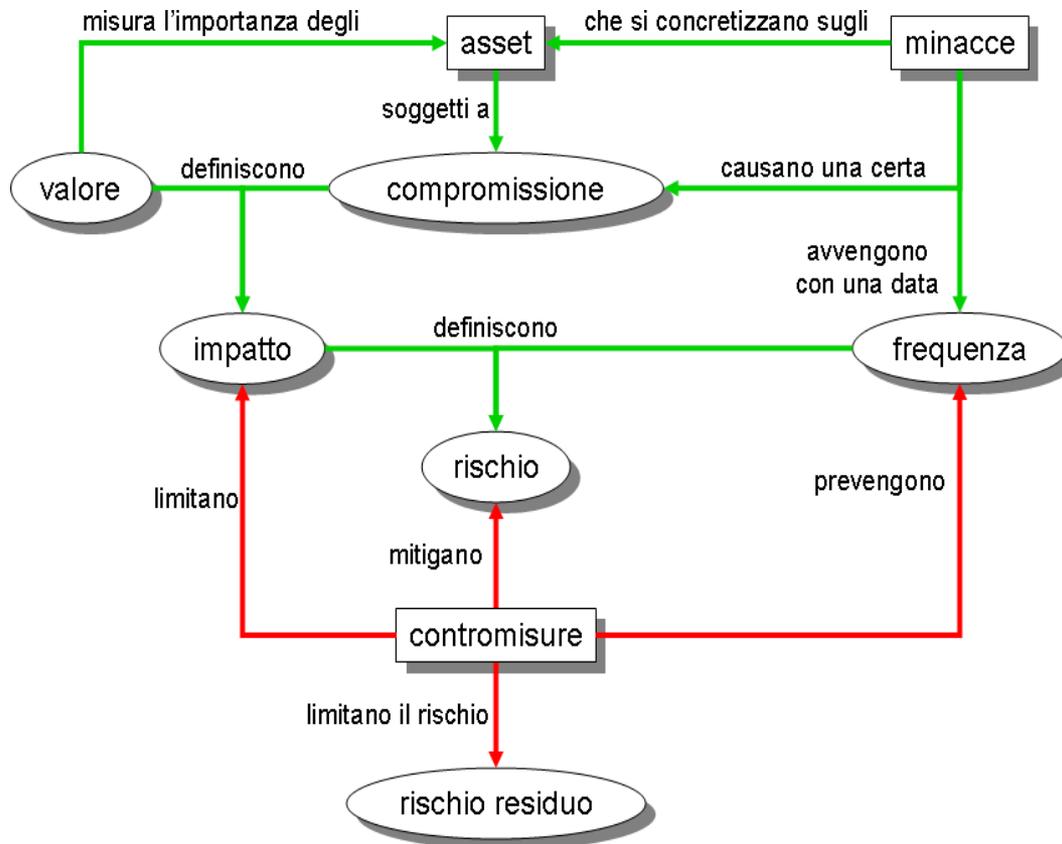
Analisi del rischio: V° passaggio - (1)

- Coincide con il vero e proprio **calcolo del valore di rischio, considerando impatto e frequenze di accadimento dei threat**
- I singoli rischi sono stati combinati o raggruppati con riferimento a ogni asset
- In uscita dal processo di analisi, il valore globale del rischio relativo al singolo asset è stato espresso in una scala a otto valori

Analisi del rischio: V° passaggio - (2)

- Nella scala sono stati definiti due valori di soglia
 - **allerta**, sotto cui non si ritiene necessario applicare ulteriori contromisure
 - **intervento**, sopra il quale devono essere individuate immediatamente contromisure atte a riportare il valore del rischio al di sotto della soglia stessa
- In tale ottica si è ritenuto di accettare il valore di rischio residuo se lo stesso è minore di quello della soglia di intervento fissata

La metodologia di trattamento del rischio



- I rischi individuati sono stati trattati con una metodologia incentrata sulle azioni di miglioramento da adottare, per diminuirne il valore associato

Le azioni di miglioramento

- Sono raccolte in un apposito registro
- Sono sottoposte a monitoraggio continuo
- Diventano input per ogni nuovo processo (almeno annuale) di analisi e gestione del rischio
- È possibile verificare in via indiretta la loro efficacia
- Il processo di miglioramento è ciclico e conforme con la norma ISO/IEC 27005:2011 «Information security risk management»

#	Fonte	Rif. Doc.	Punto ISO27001	Debolezza	Azione
1	AR	DS-03, § 6.3.1, contromisure [AUX6]	9.2.3	I cablaggi non sono tutti protetti e identificabili	Errori di configurazione, interferenze ed operazioni di intercettazione dei dati possono accadere facilmente senza un controllo dei cablaggi

Conseguenze	Priorità	Respons.	Risorse	Entro il	Stato al 25/06/2015 evidenze	%
Etichettare tutti i cavi rilevanti per i sistemi, separare i cablaggi di alimentazione da quelli per i dati, controllare che non sia possibile intercettare in maniera non autorizzata del traffico di dati accedendo ai cablaggi	Media	Rossi	Interne	31/12/14	PT-45 - Sicurezza e schema dei cablaggi.doc - V.3 del 22/1/2014	100

La tabella degli indicatori

- Nel SGSI sono stati definiti appositi indicatori
 - finalizzati al monitoraggio continuo dell'efficacia dei controlli attivati
 - associati puntualmente alla norma di riferimento

<i>cod</i>	<i>descrizione</i>	<i>frequenza</i>	<i>rif. Annex A</i>	<i>2012</i>	<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>	<i>5</i>	<i>6</i>	<i>7</i>	<i>8</i>	<i>9</i>	<i>10</i>	<i>11</i>	<i>12</i>	<i>2014</i>	<i>minimo</i>	<i>ideale</i>
127	Qualità delle password	6m	A.11.3.1	2			3			4			5			5	5	2	4

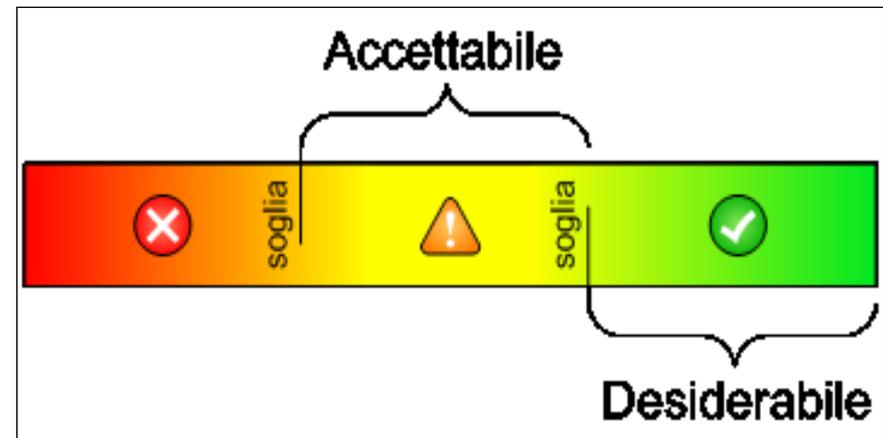
Le soglie degli indicatori

■ Accettabilità

- definisce se il valore è considerato rischioso oppure no
- può innescare potenziali azioni di miglioramento

■ Desiderabilità

- definisce se il valore si trova nella norma o no
- può attivare messaggi rivolti ai responsabili del sistema



Miglioramento continuo

- Il miglioramento continuo de sistema è garantito dall'effettuazione periodica di:
 - **Audit interni** (programmati su base triennale)
 - **Riesame annuale** dell'intero Sistema di Gestione della Sicurezza delle Informazioni effettuato dalla Direzione
 - **Audit esterni** (effettuati dall'ente certificatore RINA S.p.a.)

Gli audit interni

- In tale attività vengono puntualmente analizzati tutti i requisiti indicati dai punti della norma
- In caso di rilievo si procede alla creazione di un'azione correttiva nel registro di miglioramento

Punto	Requisito	Evidenza oggettiva	Rilievi
4.2	Understanding the needs and expectations of interested parties	DS13 (Contesto e ambito) – DS03 (Perimetro SGSI) – DS05 (Organizzazione SGSI)	NO

Il riesame della Direzione

- In tale sede si raccolgono tutti gli **elementi** in **entrata** e in **uscita** utili a **valutare** correttamente il **SGSI** per assicurarne la continua:
 - idoneità
 - adeguatezza
 - efficacia
- In tale sede sono valutate le opportunità per:
 - il miglioramento
 - l'esigenza di apportare cambiamenti

Transizione alle nuova versione

- Il processo di adeguamento del SGSI è avvenuto a settembre del 2015
- Ha richiesto alcune modifiche per l'adeguamento:
 - dei riferimenti normativi
 - della struttura di alcuni documenti
- A livello organizzativo
 - non sono stati richiesti particolari accorgimenti
 - si era già provveduto a organizzazione il sistema per favorirne la transizione alla nuova versione della norma

Risultati ottenuti

- La scelta di intraprendere il percorso di certificazione si è dimostrata particolarmente lungimirante
 - ha determinato un cambio di approccio metodologico incentrato sulla gestione del «processo sicurezza»
 - ha determinato la progettazione/riprogettazione dei sistemi di servizi distribuiti erogati dall'ateneo
 - ha determinato un cambiamento culturale

Possibili evoluzioni future

- Estendere il perimetro di applicazione anche agli asset collocati fuori dai datacenter
- Revisionare il processo di analisi e gestione del rischio considerando l'adozione di approcci di tipo quantitativo

Ringraziamenti

- I colleghi Gian Paolo Gentili e Giampaolo Rappi, che insieme a me sono coautori del paper
- Il dott. Paolo Gaspari, che ha avviato il processo di certificazione
- I colleghi del CINFO che contribuiscono operativamente nel processo di certificazione
- RINA S.p.a. (certificatore) per la serietà dimostrata

I miei contatti

linkedin

<http://it.linkedin.com/pub/francesco-ciclosi/62/680/a06/>

facebook

<https://www.facebook.com/francesco.ciclosi>

twitter

@francyciclosi

www

<http://www.francescociclosi.it>

