PA digitale e cybersecurity

Un approccio sostenibile per le misure minime di sicurezza nelle Università

SAPIENZA
UNIVERSITÀ DI ROMA

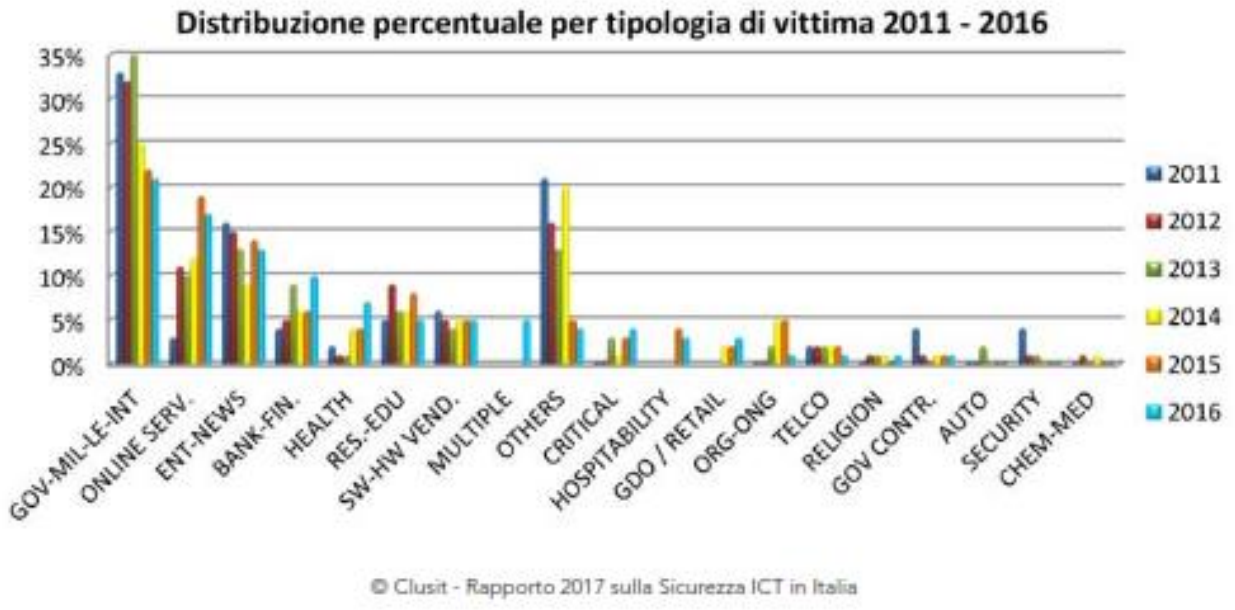
Leonardo Querzoni
Dip. Ing. Automatica e Gestionale

Giuseppe Arrabito
Centro Infosapienza

2017
FORUM PA

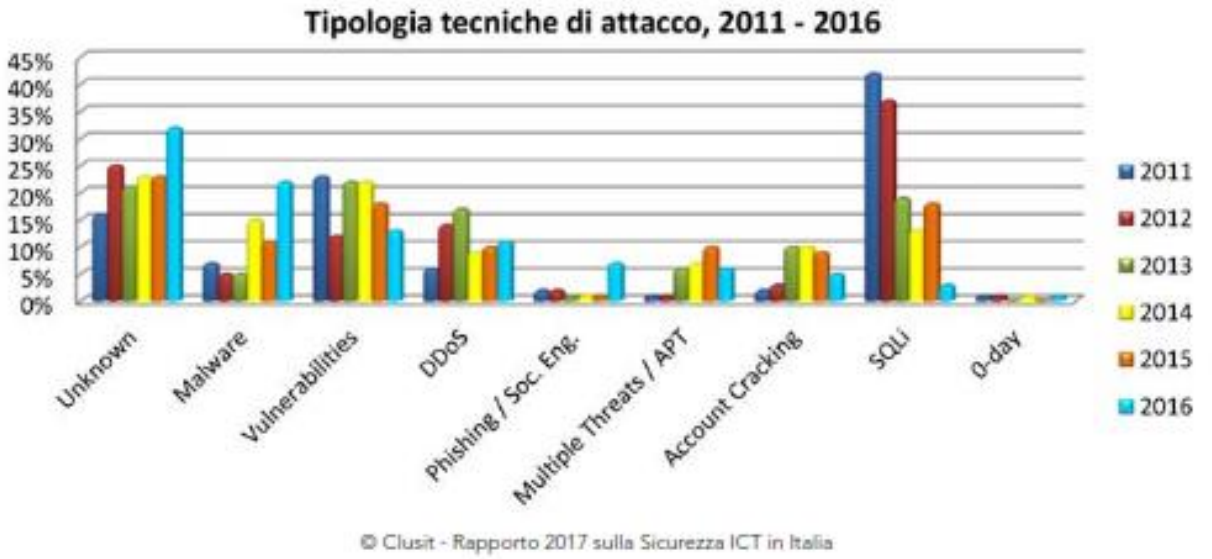
Lo scenario attuale

2016 l'anno peggiore di sempre in termini di evoluzione delle minacce "cyber"



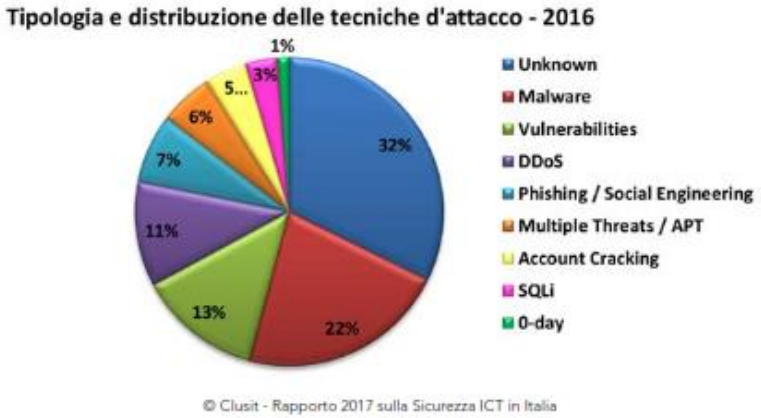
Lo scenario attuale

2016 l'anno peggiore di sempre in termini di evoluzione delle minacce "cyber"



Lo scenario attuale: le vittime illustri

VITTIME PER TIPOLOGIA	2011	2012	2013	2014	2015	2016	Variazioni 2016 su 2015	Trend 2017
Institutions: Gov - Mil - LEAs - Intel	153	374	402	213	223	220	-1,35%	↘
Other targets	97	194	146	172	51	38	-25,49%	↓
Entertainment / News	76	175	147	77	138	131	-5,07%	↘
Online Services / Cloud	15	136	114	103	187	179	-4,28%	↘
Research - Education	26	104	70	54	82	55	-32,93%	↓
Banking / Finance	17	59	108	50	64	105	64,06%	↑
Software / Hardware Vendor	27	59	46	44	55	56	1,82%	↗
Telco	11	19	19	18	18	14	-22,22%	↓
Gov. Contractors / Consulting	18	15	2	13	8	7	-12,50%	↓
Security Industry	17	14	6	2	3	0	-100,00%	↓
Religion	0	14	7	7	5	6	20,00%	↑
Health	10	11	11	32	36	73	102,78%	↑
Chemical / Medical	2	9	1	5	2	0	-100,00%	↓
Critical Infrastructures	-	-	37	13	33	38	15,15%	↑
Automotive	-	-	17	3	5	4	-20,00%	↓
Org / ONG	-	-	19	47	46	13	-71,74%	↓
GDO / Retail	-	-	-	20	17	29	70,59%	↑
Hospitability	-	-	-	-	39	33	-15,38%	↘
Multiple targets (nuova)	-	-	-	-	-	49	-	-



Il quadro normativo per la PA

Con l'avvenuta pubblicazione in Gazzetta Ufficiale (Serie Generale n.103 del 5-5-2017) della Circolare 18 aprile 2017, n. 2/2017, recante «**Misure minime di sicurezza ICT per le pubbliche amministrazioni**. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)», le Misure minime sono ora divenute di obbligatoria adozione per tutte le Amministrazioni. **Scadenza 31/12/2017**

AGID Misure minime di sicurezza

Il **regolamento generale sulla protezione dei dati** (GDPR, *General Data Protection Regulation-Regolamento UE 2016/679)* è un Regolamento con il quale la Commissione europea intende rafforzare e unificare la protezione dei dati personali entro i confini dell'Unione europea). **Applicabile dal 24/05/2018**

GDPR

Il nuovo CAD. Con la pubblicazione sulla Gazzetta Ufficiale n. 214 del **13 settembre 2016**, il decreto legislativo 26 agosto 2016, n. 179 recante *Modifiche ed integrazioni al Codice dell'amministrazione digitale, in materia di riorganizzazione delle amministrazioni pubbliche*, entra in vigore oggi, 14 settembre 2016

Codice Amministrazione Digitale

DPCM 17 febbraio 2017
Decreto del Presidente del Consiglio dei ministri del 17 febbraio 2017
Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali (pubblicato sulla GU n. 87 del 13/4/2017)

Strategia nazionale e piano di cybersecurity

I possibili rischi per l'Ateneo

- Rischio di perdita di disponibilità, integrità e confidenzialità delle informazioni e dei dati: violazioni informatiche
- Rischio di sanzioni amministrative e penali: perdite economiche
- Rischio reputazionale: danno all'immagine
- Perdita di fiducia degli utenti nell'utilizzo delle tecnologie informatiche e nell'innovazione digitale: possibile calo di nuove iscrizioni

IL DANNO DI IMMAGINE

«…consiste nella considerazione e nella credibilità di cui il soggetto gode nella società e ne costituisce il primo driver di valore….»
[Corradini, Nardelli 2013]

Vincoli del contesto accademico

VINCOLI STATUTARI

- Autonomia gestionale ed amministrativa delle strutture periferiche
- Organizzazione e gestione delle attività di ricerca e della didattica
- Le strutture periferiche si avvalgono dei servizi centrali della Sapienza
- Libertà accademica della ricerca

VINCOLI LEGALI

- Aderenza alle normative vigenti in termini di sicurezza cibernetica
- Rispetto delle normative in termini di dati personali e di misure di sicurezza

VINCOLI INTERNI

- Sostenibilità delle contromisure adottate

Le misure minime di sicurezza - AGID

CIRCOLARE 17 marzo 2017, n. 1/2017
Misure minime di sicurezza ICT per le pubbliche amministrazioni. *(Direttiva del PDCM 1/08/2015). (17A02399)* *(GU Serie Generale n.79 del 04-04-2017)*

Obiettivo della presente circolare è indicare alle pubbliche amministrazioni **le misure minime per la sicurezza ICT che debbono essere adottare al fine di contrastare le minacce più comuni** e frequenti cui sono soggetti i loro sistemi informativi.

Ai sensi dell'art. 3 della Circolare citata, "**il responsabile dei sistemi informativi** di cui all'art. 10 del decreto legislativo 12 febbraio 1993, n. 39, ovvero, in sua assenza, il **dirigente allo scopo designato**, ha la responsabilità della attuazione delle misure minime di cui all'art. 1".

Obbligo per le pubbliche amministrazioni, in ossequio a quanto previsto al successivo art. 5 della Circolare, entro il **31 dicembre 2017** dovranno attuare gli adempimenti necessari ed uniformarsi.

Le misure minime di sicurezza - AGID

In **data 5 maggio 2017** è stata pubblicata sulla G.U. la circolare AgID n. 2/2017 del 18 aprile 2017 che sostituisce integralmente la precedente **circolare n. 1/2017 del 17 marzo 2017**, recante: «*Misure minime di sicurezza ICT per le pubbliche amministrazioni (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)*»

In realtà tale sostituzione non comporta alcuna variazione sostanziale e la nuova circolare corregge solo alcune imprecisioni di carattere formale relative a riferimenti normativi ormai superati dal Codice dell'Amministrazione Digitale (CAD), che proprio di recente è stato modificato sostanzialmente dal **d.lgs. n. 179/2016**.

In particolare all'art. 2 si precisa che i destinatari della circolare sono i soggetti di cui all'art. 2, comma 2 del C.A.D. Inoltre all'art. 3 si chiarisce che il responsabile della struttura per l'organizzazione, l'innovazione e le tecnologie di cui all'art. 17 del C.A.D., ovvero, in sua assenza, il dirigente allo scopo designato, ha la responsabilità dell'attuazione delle misure minime.

Le misure minime di sicurezza - AGID

- Tali misure, il cui rispetto è richiesto a tutte le PA, prevedono **tre livelli di attuazione: minimo, standard e alto:**

  I livelli successivi rappresentano situazioni evolutive in grado di fornire livelli di protezione più completi, e dovrebbero essere adottati fin da subito dalle organizzazioni maggiormente esposte a rischi (ad esempio per la criticità delle informazioni trattate o dei servizi erogati) ma anche visti come obiettivi di miglioramento da parte di tutte le altre organizzazioni.

- Fra le misure minime è previsto anche che le pubbliche amministrazioni accedano sistematicamente a **servizi di early warning** che consentano loro di rimanere aggiornate sulle nuove vulnerabilità di sicurezza. A tal proposito il CERT-PA fornisce servizi proattivi ed informativi a tutte le amministrazioni accreditate.

- Le misure minime di sicurezza ICT- che costituiscono parte integrante del più ampio disegno delle Regole Tecniche per la sicurezza informatica della Pubblica Amministrazione di futura emanazione

Le misure minime di sicurezza – i controlli

AgID Basic Security Control(s) (ABSC) sono un estratto di 5 dei 20 Critical Security Check (CSC) del SANS Institute

Tipologia	Descrizione
ABSC1 (CSC1)	INVENTARIO DEI DISPOSITIVI AUTORIZZATI
ABSC2 (CSC2)	INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI
ABSC3 (CSC3)	PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER
ABSC4 (CSC4)	VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ
ABSC5 (CSC5)	USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE
ABSC8 (CSC8)	DIFESE CONTRO I MALWARE
ABSC10 (CSC10)	COPIE DI SICUREZZA
ABSC13 (CSC13)	PROTEZIONE DEI DATI

Le misure minime di sicurezza – i controlli

ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

Acquisire, valutare e intraprendere continuamente azioni in relazione a nuove informazioni allo scopo di individuare vulnerabilità, correggere e minimizzare la finestra di opportunità per gli attacchi informatici.

ABSC_ID #			Descrizione	FNSC	Min.	Std.	Alto
4	1	1	Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.	ID.RA-1 DE.CM-8	X	X	X
		2	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	ID.RA-1 DE.CM-8		X	X
		3	Usare uno SCAP (Security Content Automation Protocol) di validazione della vulnerabilità che rilevi sia le vulnerabilità basate sul codice (come quelle descritte dalle voci Common Vulnerabilities ed Exposures) che quelle basate sulla configurazione (come elencate nel Common Configuration Enumeration Project).	DE.CM-8			X
	2	1	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	DE.CM-8		X	X
		2	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	DE.CM-8		X	X
		3	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	DE.CM-8		X	X
	3	1	Eseguire le scansioni di vulnerabilità in modalità privilegiata, sia localmente, sia da remoto, utilizzando un account dedicato che non deve essere usato per nessun'altra attività di amministrazione.	DE.CM-8		X	X
		2	Vincolare l'origine delle scansioni di vulnerabilità a specifiche macchine o indirizzi IP, assicurando che solo il personale autorizzato abbia accesso a tale interfaccia e la utilizzi propriamente.	DE.CM-8		X	X
	4	1	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	DE.CM-8	X	X	X
		2	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione	ID.RA-2		X	X

Le misure minime di sicurezza – i controlli

ABSC_ID #			Descrizione	FNSC	Min.	Std.	Alto
4	5	1	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	PR.MA-1	X	X	X
		2	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.	PR.MA-1	X	X	X
	6	1	Verificare regolarmente che tutte le attività di scansione effettuate con gli account aventi privilegi di amministratore siano state eseguite secondo delle policy predefinite.	ID.RA-1 DE.CM-8		X	X
	7	1	Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.	PR.IP-12 RS.MI-3	X	X	X
		2	Rivedere periodicamente l'accettazione dei rischi di vulnerabilità esistenti per determinare se misure più recenti o successive patch possono essere risolutive o se le condizioni sono cambiate, con la conseguente modifica del livello di rischio.	PR.IP-12 RS.MI-3		X	X
	8	1	Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità , del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).	ID.RA-4 ID.RA-5 PR-IP.12	X	X	X
		2	Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.	PR.IP-12	X	X	X
	9	1	Prevedere, in caso di nuove vulnerabilità, misure alternative se non sono immediatamente disponibili patch o se i tempi di distribuzione non sono compatibili con quelli fissati dall'organizzazione.	PR.IP-12 RS.MI-3		X	X
	10	1	Valutare in un opportuno ambiente di test le patch dei prodotti non standard (es.: quelli sviluppati ad hoc) prima di installarle nei sistemi in esercizio.	PR.DS-7		X	X

Le misure minime di sicurezza: le criticità per le Università

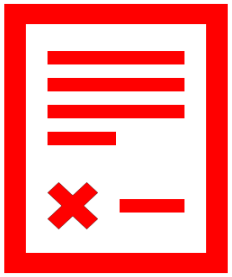
- Pubblicazione e periodo di applicabilità
- Criticità legate al contesto accademico
- Sostenibilità delle contromisure: budget di previsione già redatti
- Gruppo di lavoro CODAU per consultazione con AGID
- Dubbi riguardanti alcune definizioni (risorse attive, dispositivi informatici, etc)
- Applicabilità e sostenibilità interna
- Mancanza di un processo di verifica di quanto dichiarato
- Obbligo senza un sistema sanzionatorio: solo attività preventiva?

GDPR – il nuovo regolamento privacy

INVARIATO O VARIATO MARGINALMENTE

- Definizione di trattamento
- Definizione di dato personale
- Principi relativi al trattamento di dati
- Liceità del trattamento
- Obbligo di informativa
- Obbligo di consenso
- Soggetti che effettuano il trattamento (salvo incaricati e DPO)
- Protezione delle sole persone fisiche

NOVITA'



- Registro dei trattamenti
- Valutazione d'impatto (**sostituisce la notifica**)
- Adozione di misure tecniche e organizzative adeguate
- Entità delle sanzioni
- DPO
- Certificazione dei trattamenti
- Responsabilità solidale di titolare e responsabile
- Accountability del titolare

GDPR – il nuovo regolamento privacy

ADEMPIMENTO	CODICE PRIVACY	GDPR
NOTIFICA DEL TRATTAMENTO	SI (art. 37)	**NO**
INFORMATIVA	SI (art. 13)	SI (art. 13)
CONSENSO	SI (art. 23)	SI (art. 6)
MISURE DI SICUREZZA MINIME	SI (allegato B)	**NO**
MISURE IDONEE / ADEGUATE	SI (art. 31)	SI (art. 29)
NOMINA DPO	NO	SI (art. 37)
VALUTAZIONE D'IMPATTO	NO	SI (art. 35)
CONSULTAZIONE PREVENTIVA	NO	SI (art. 36) non sempre
PRIVACY BY DESIGN / DEFAULT	NO	SI (art. 25)
REGISTRO TRATTAMENTI	NO	SI (art. 30)
CERTIFICAZIONE	NO	SI (artt. 25 e 42) non obbligatoria
VIOLAZIONE DATI	NO	SI (artt. 33 e 34)

Sicurezza per InfoSapienza: obiettivi

- Analizzare e quantificare il livello di sicurezza rispetto a standard comuni
- Accrescere il livello di sicurezza dei servizi e sistemi informatici
- Raggiungere la conformità normativa alle leggi specifiche
- Definire un sistema di gestione della sicurezza delle informazioni
- Sviluppare piani di rimedio a mitigazione delle criticità e vulnerabilità rilevate
- Ottenere livelli di sicurezza adeguati rispetto alle nuove minacce
- Ottimizzare gli investimenti in sicurezza delle informazioni

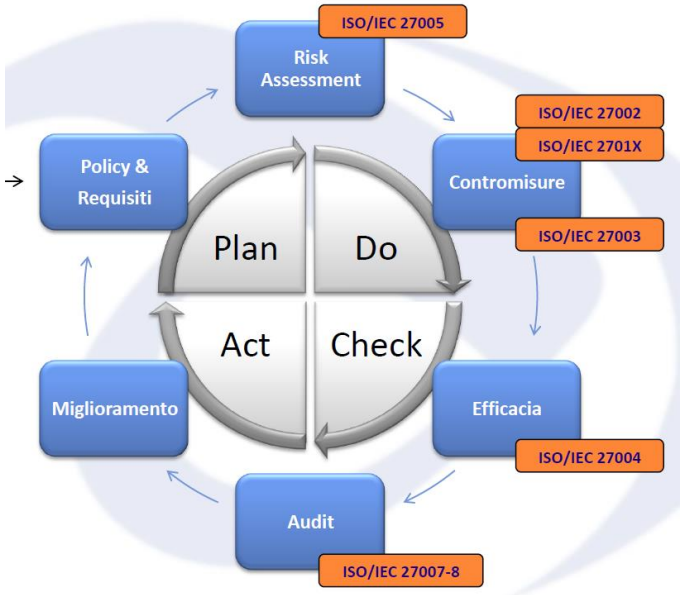
Infosapienza: il processo di gestione della sicurezza

CULTURALE

ORGANIZZATIVO

TECNICO

COMUNICATIVO



Il percorso di InfoSapienza

ORGANIZZATIVO

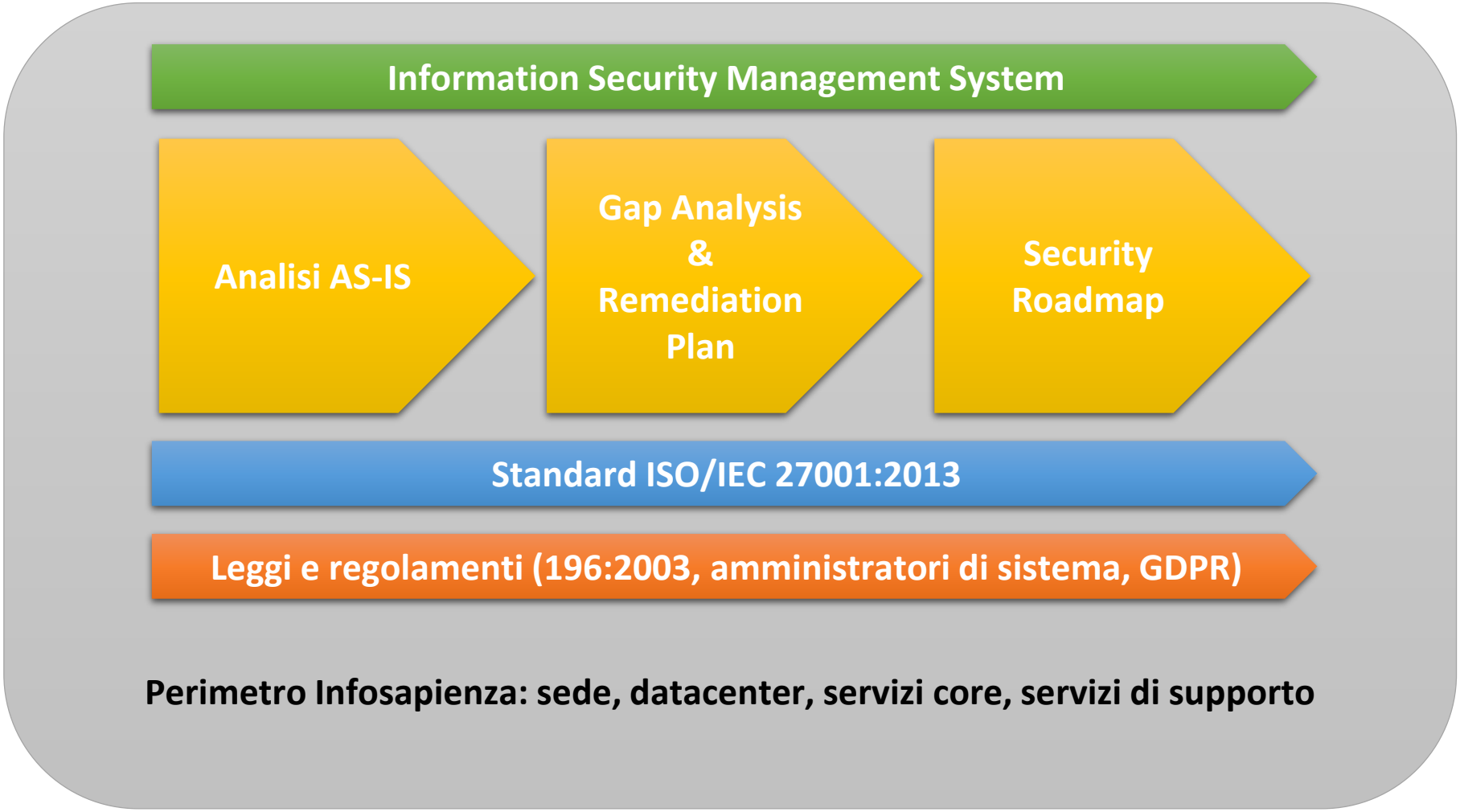
- Acquisizione di competenze in tema di information security
- Collaborazione con il CIS
  - Analisi delle vulnerabilità dei siti web delle strutture
  - Supporto in casi di incidenti di rilevanza mediatica
  - Organizzazione dell'evento Cyber Security Forum
- Definizione di un budget dedicato alla sicurezza informatica
- Restrizione della navigazione web per l'Amm. Centrale
- Incremento della percezione del rischio informatico
- Formazione ai referenti informatici
- Compliance alla normativa sulla privacy: il GDPR

Il percorso di InfoSapienza

TECNICO

- Analisi delle vulnerabilità delle web aplication: piani di rimedio
- Rafforzamento delle connessioni https (TLS)
- Restrizione della navigazione web per l'Amm. Centrale
- Definizione di un processo di protezione dei dati: patch management, backup, continuità operativa dei servizi
- Diminuzione della superficie di attacco: hosting dei siti web delle strutture periferiche
- Definizione di un processo di incident management: il SIEM
- Gap Analisys: analisi dallo scostamento dei livelli di sicurezza rispetto allo standard ISO 27001

Gap Analisys



Attacchi rilevati per l'Ateneo

- Attacchi di tipo DDOS sulla rete: il caso della rete scientifica
- Casi di ramsonware/cryptolocker sui pc dell'amministrazione.
- Furti di credenziali
- Spam
- Phishing e truffe on line
- Wi-Fi Rogue Access point
- Attacchi a forza bruta sulle form di autenticazione: il caso www.uniroma1.it
- Attacchi ai siti web istituzionali sfruttando vulnerabilità note: caso dipartimenti e facoltà
- PC appartenenti a reti botnet

Gestione efficace degli incidenti

#EyePyramid

Infezione di un malware del tipo Remote Control adibito a compromettere i sistemi delle vittime ed esflitrare un gran quantitativo di informazioni riservate.

- Supporto congiunto CIS ed Infosapienza
- Analisi e verifica dell'infezione
- Nessun caso riscontrato sui dispostivi dell'Amm. Centrale

#WannaCry

Infezione virale di un malware del tipo ransomware che ha colpito circa 99 paesi con più di 200.000 infezioni.

- Attivazione del team Infosapienza
- Analisi del worm e successive contromisure
- Emanazione di linee guida preventive e correttive
- Nessun caso riscontrato nell'amministrazione Centrale
- 6 casi isolati all'interno di strutture dipartimentali

Conclusioni generali

- ✓ Necessità di un approccio integrato della sicurezza: tecnico, organizzativo e gestionale.
- ✓ Superamento della dicotomia libertà vs sicurezza: libertà **e** sicurezza
- ✓ Occorre una visione della sicurezza condivisa e partecipata
- ✓ Necessità di una politica di sicurezza delle informazioni per l'Ateneo: definizione della funzione security
- ✓ Accrescere la consapevolezza degli utenti: l'elemento più vulnerabile del processo è l'uomo
- ✓ Inserire gli aspetti di sicurezza in ogni processo riguardante le informazioni e i dati
- ✓ InfoSapienza riferimento dei processi di sicurezza della Sapienza con mansioni di supporto alle varie strutture dipartimentali
- ✓ Creare sinergie proattive tra i dipartimenti, centri di ricerca e InfoSapienza

PA digitale e cybersecurity

Un approccio sostenibile per le misure minime di sicurezza nelle Università

SAPIENZA
UNIVERSITÀ DI ROMA

Leonardo Querzoni
Dip. Ing. Automatica e Gestionale

Giuseppe Arrabito
Centro Infosapienza

2017
FORUM PA