CONSIGLIO NAZIONALE INGEGNERI

GDPR
REGOLAMENTO EU 679/2016

Ing. Biagio Garofalo
direzionetecnica@cni-online.it
+39 3939505301
17 maggio 2018

Introduzione ai Sistemi Informativi Aziendali



Un sistema informativo è l'insieme di dati e processi di qualsiasi forma che abbiamo correlazioni rispetto ad un business o ad un progetto.

Infatti quando parliamo di dati intendiamo elementi d'informazioni, per cui non diamo alcuna specifica in merito alla tipologia del supporto che li identifica e caratterizza. Le informazioni sono parte integrante dei sistemi informativi e la gestione, strutturazione e finalità d'utilizzo ne sono il "kernel".

Quindi, quando parliamo di sistema informativo identifichiamo un unicum, ossia un sistema che gestisce informazioni.

- Le informazioni sono digitali e cartacee:
  - le informazioni digitali sono strutturate su supporto digitale
  - le informazioni cartacee sono tutte quelle che non possono essere ricondotte ad un sistema informatico

Progettare un sistema informativo, significa identificare le informazioni che bisogna trattare, manipolare e finalizzare

- Trattare
  - Sono dati anagrafici, militari, strategici, giudiziari, genetici, marketing, etc..
- Manipolare
  - Chi ha accesso ai dati, come può effettuarlo, quali sono gli strumenti e qual è il grado di sicurezza, etc…
- Finalizzare
  - Il fine della gestione dei dati è il business, l'investigazione cognitiva di eventi, la ricerca, la formazione, il marketshare, etc….

- Un sistema informativo è così strutturato:
  - Sistema informatico
    - Ossia strutture tecnologiche che supportano servizi tecnologici
  - Sistema di processi cartacei e non
    - Processi e strutture burocratiche a supporto del busniness o delle finalità precipue
  - Risorse umane e skils
    - Le conoscenze e ruoli necessari per muovere le informazioni
  - Comunicazione e collaborazione
    - L'interazione tra skils, progetti e strutture

Esempi di sistemi informativi





Dietro strutture complesse ci sono sistemi digitali, cartacei e processi di comunicazione ed interazione umana



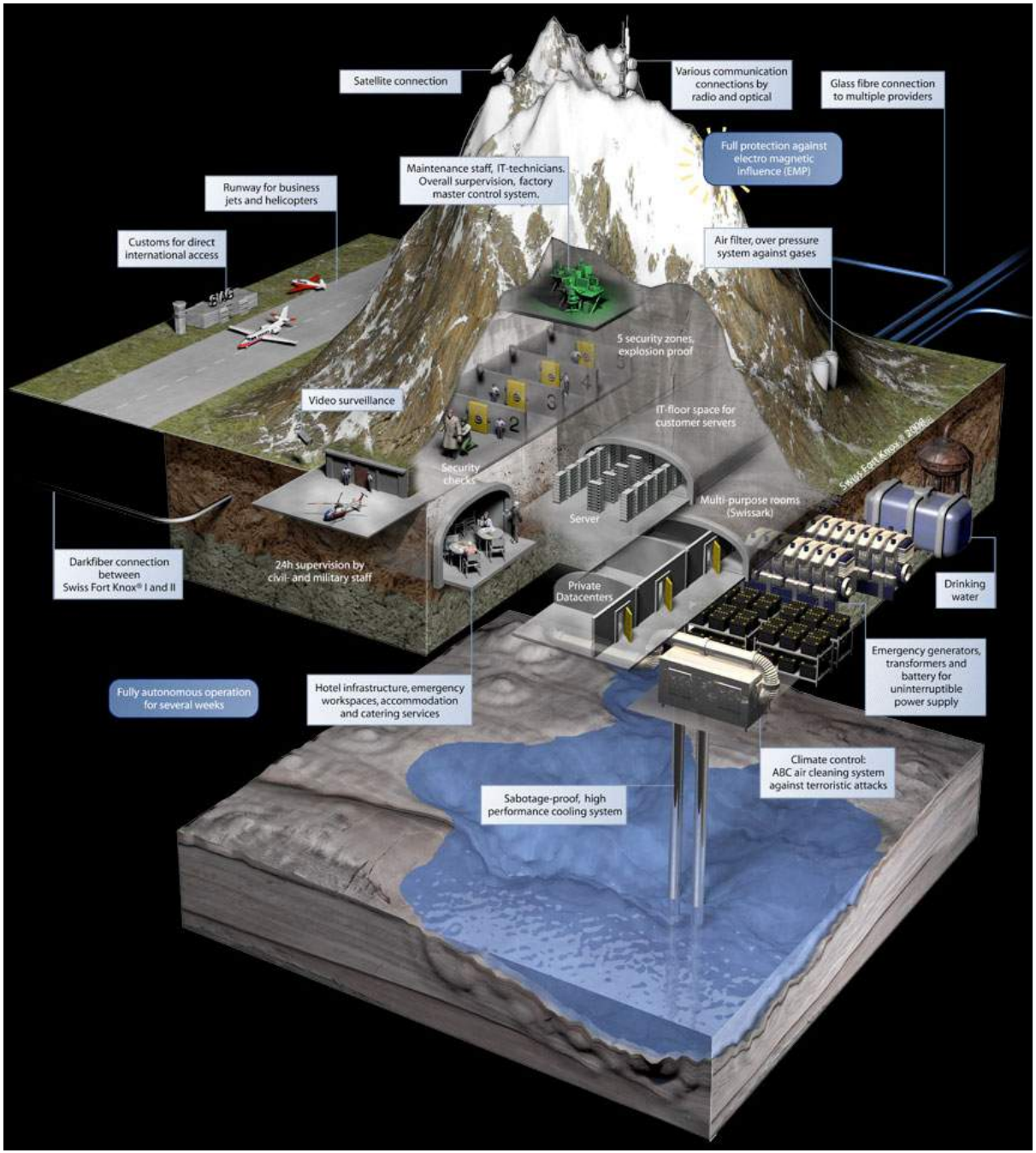




I

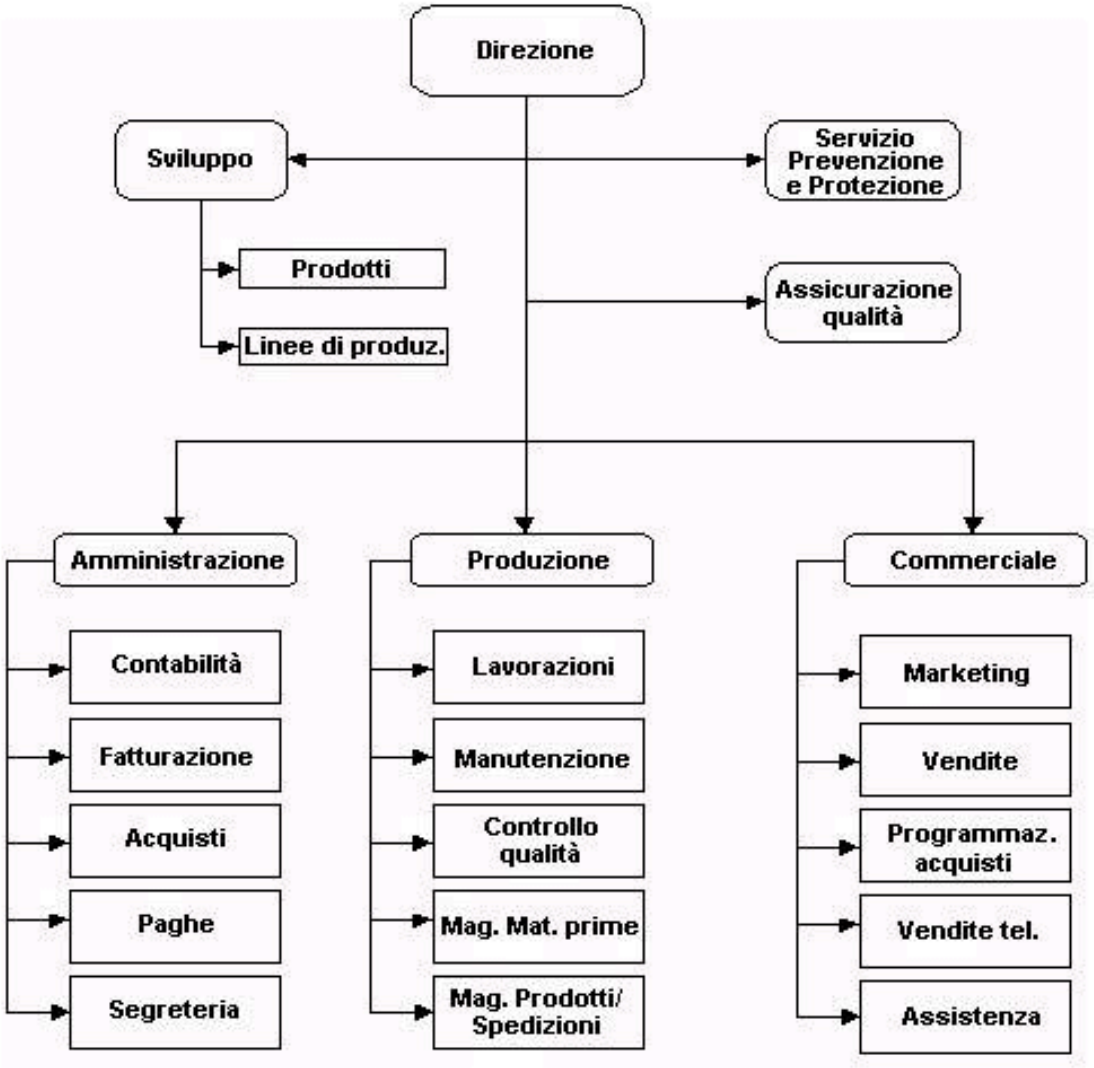


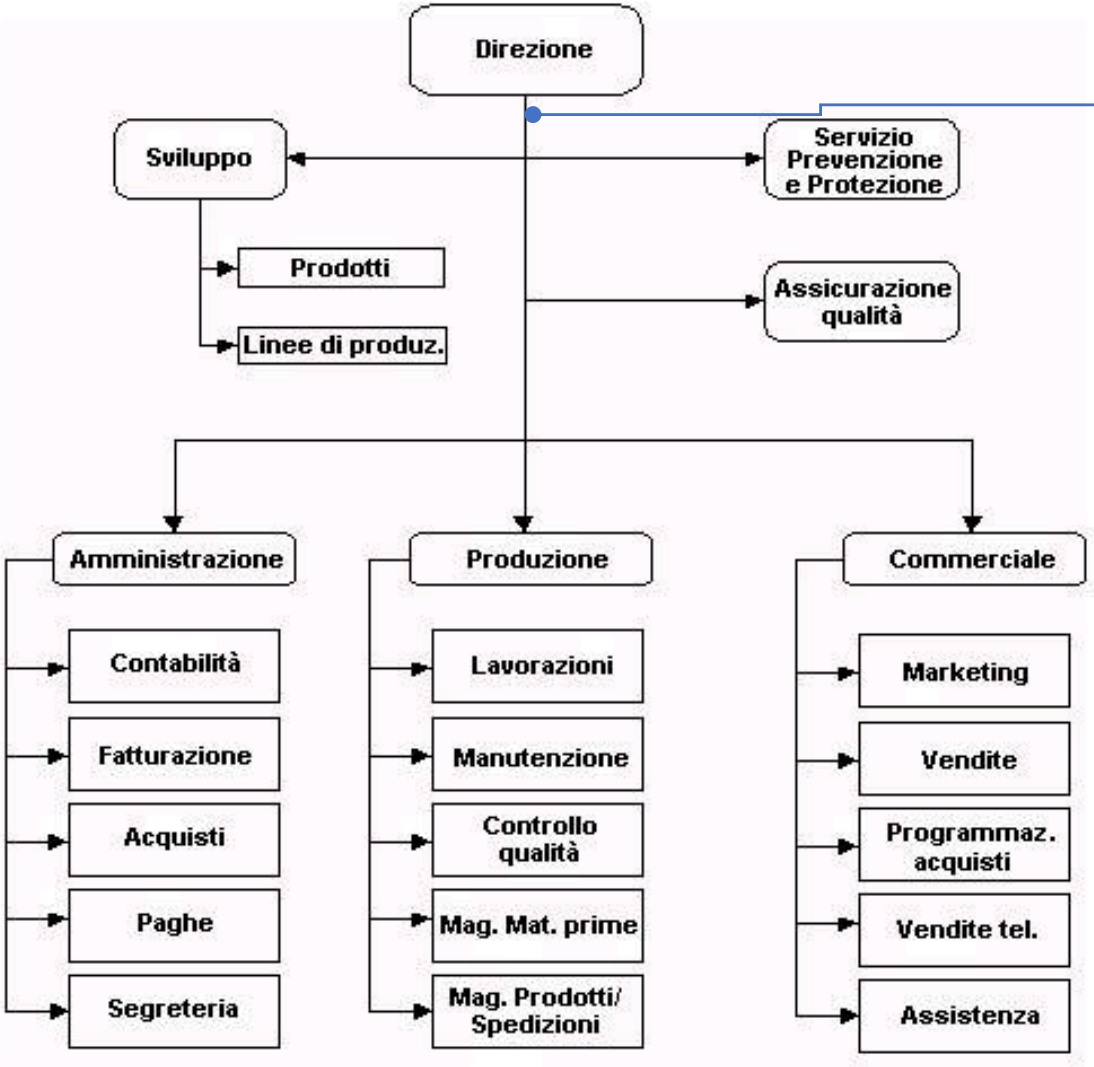
- Ecco un esempio diretto di sistema complesso che richiede la gestione delle informazioni



Comunication and collaboration

Organigramma standard





ICT : C.I.O.

DPO

C.E.O.: CHIEF EXECUTIVE OFFICER

C.I.O.: CHIEF INFORMATION OFFICER

LETTURA ARTICOLO SULLA PRIVACY E SISTEMI INFORMATIVI



PRIVACY

- Decreto legislativo n°196 del 30 giugno 2003
  - Codice in materia di protezione dei dati personali
    - B. Disciplinare tecnico in materia di misure minime di sicurezza

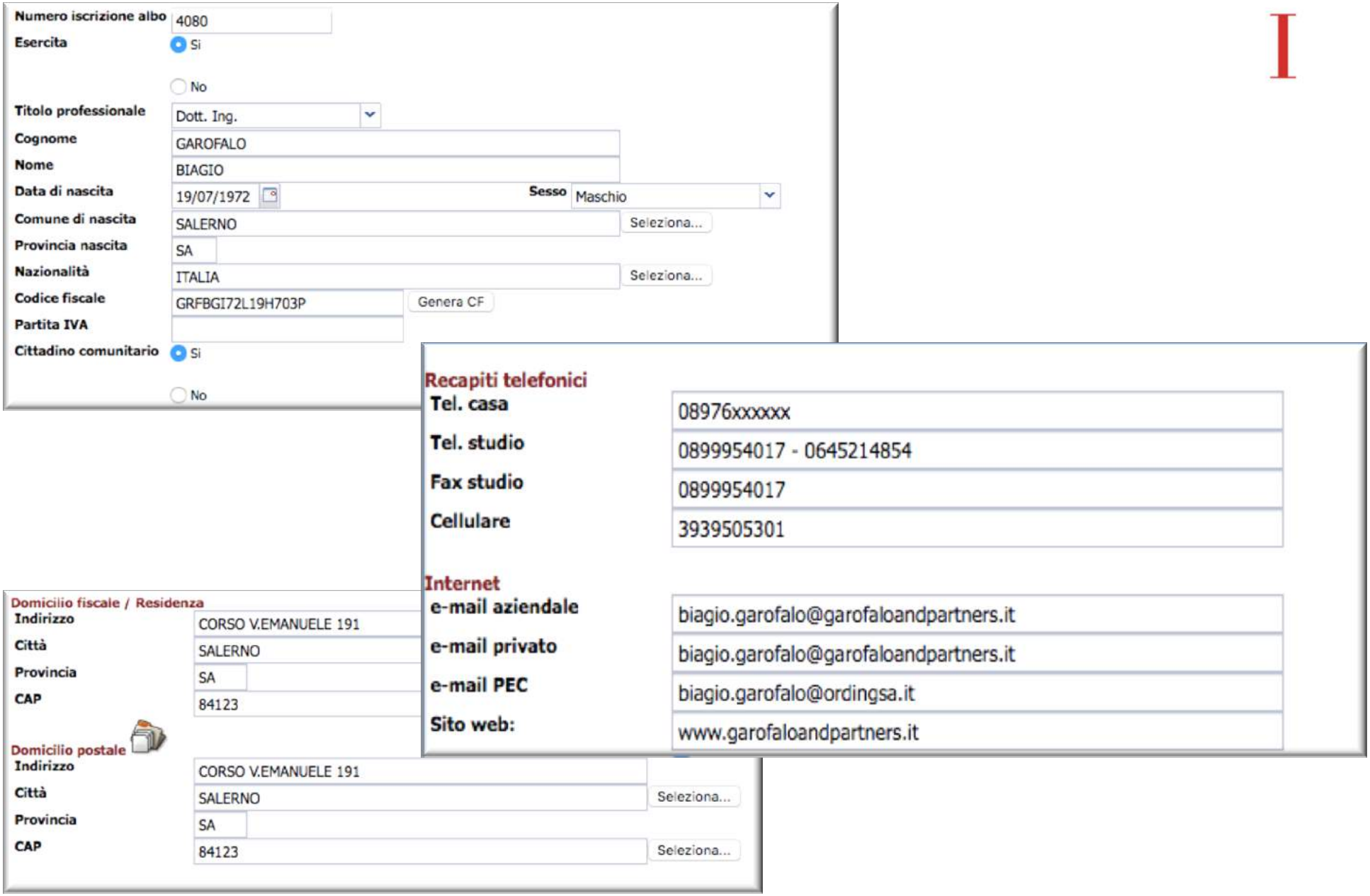
Priorità e passi operativi

- Creare organigramma funzionale nell'Ordine di riferimento
- Designare il responsabile del sistema informatico
- Designare l'amministratore di sistema
- Designare il responsabile dei dati e gli incaricati
- Designare il DPO e comunicarlo al Garante
- Identificare la tipologia di dati trattati
- Acquisire le informative dagli associati al trattamento dei dati per le finalità precipue
- Acquisire le informative dagli associati al trattamento dei dati per finalità diverse da quelle istituzionali
- Acquisire il consenso al trattamento dei dati da parte dei dipendenti, dei collaboratori e dei fornitori
- Formazione strutturata per dipendenti e collaboratori
- Definire il registro del trattamento dei dati
- Impostare il piano di gestione del rischio associato al trattamento dei dati
- Manutenere con frequenza almeno trimestrale quanto sopra elencato

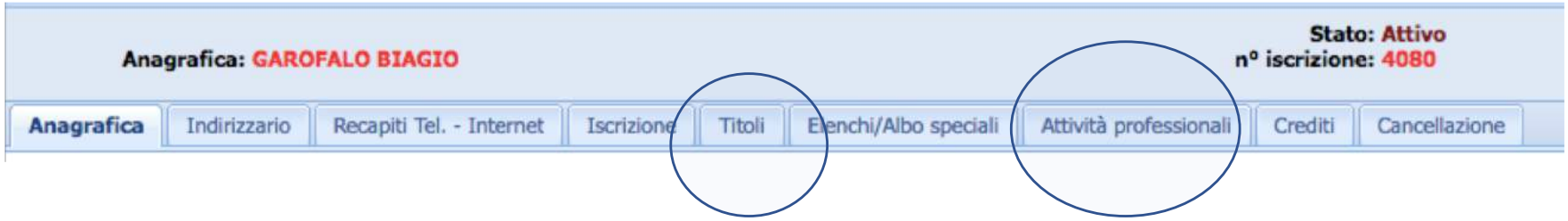
Tipologia dati

Dati personali

- dati anagrafici
- dati identificazione professioale
- dati sensibili
  - *preferenze sessuali*
  - *preferenze religiose*
  - *etnici*
  - *Sanitari (e genetici)*
  - *genetici*
  - *biometrici*
  - *giudiziari*
- dati marketing
- dati stategici


Numero iscrizione albo 4080
Esercita Si
No
Titolo professionale Dott. Ing.
Cognome GAROFALO
Nome BIAGIO
Data di nascita 19/07/1972
Sesso Maschio
Comune di nascita SALERNO
Seleziona...
Provincia nascita SA
Nazionalità ITALIA
Seleziona...
Codice fiscale GRFBGI72L19H703P
Genera CF
Partita IVA
Cittadino comunitario Si
No
Recapiti telefonici
Tel. casa 08976xxxxxx
Tel. studio 0899954017 - 0645214854
Fax studio 0899954017
Cellulare 3939505301
Internet
e-mail aziendale biagio.garofalo@garofaloandpartners.it
e-mail privato biagio.garofalo@garofaloandpartners.it
e-mail PEC biagio.garofalo@ordingsa.it
Sito web: www.garofaloandpartners.it
Domicilio fiscale / Residenza
Indirizzo CORSO V.EMANUELE 191
Città SALERNO
Provincia SA
CAP 84123
Domicilio postale
Indirizzo CORSO V.EMANUELE 191
Città SALERNO
Seleziona...
Provincia SA
CAP 84123
Seleziona...

Ulteriori dati di dettaglio



Registro Trattamenti

Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:						
l nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati	le finalità del trattamento	una descrizione delle categorie di interessati e delle categorie di dati personali	le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali	ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate	ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati	ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1. 2.

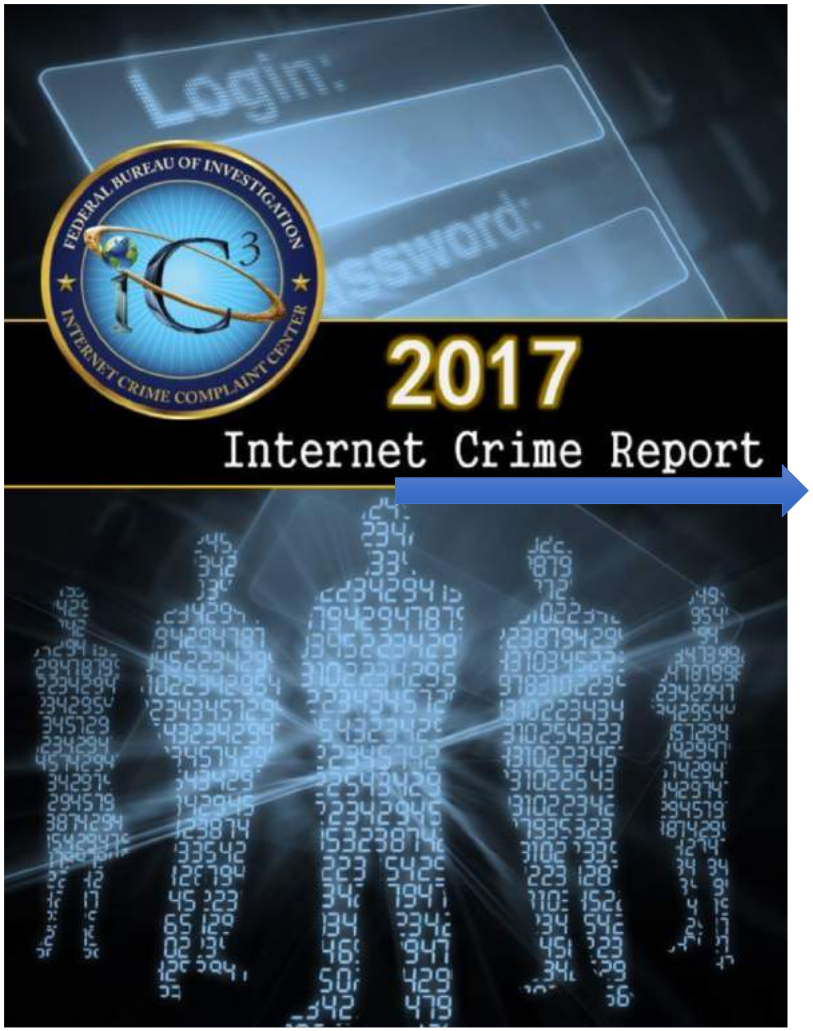
Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente			
il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;	le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento	ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate	ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

Modello di comunicazione al Garante per la designazione del DPO

- Facsimile

Software per la compilazione del Privacy Impact Assessment [PIA]

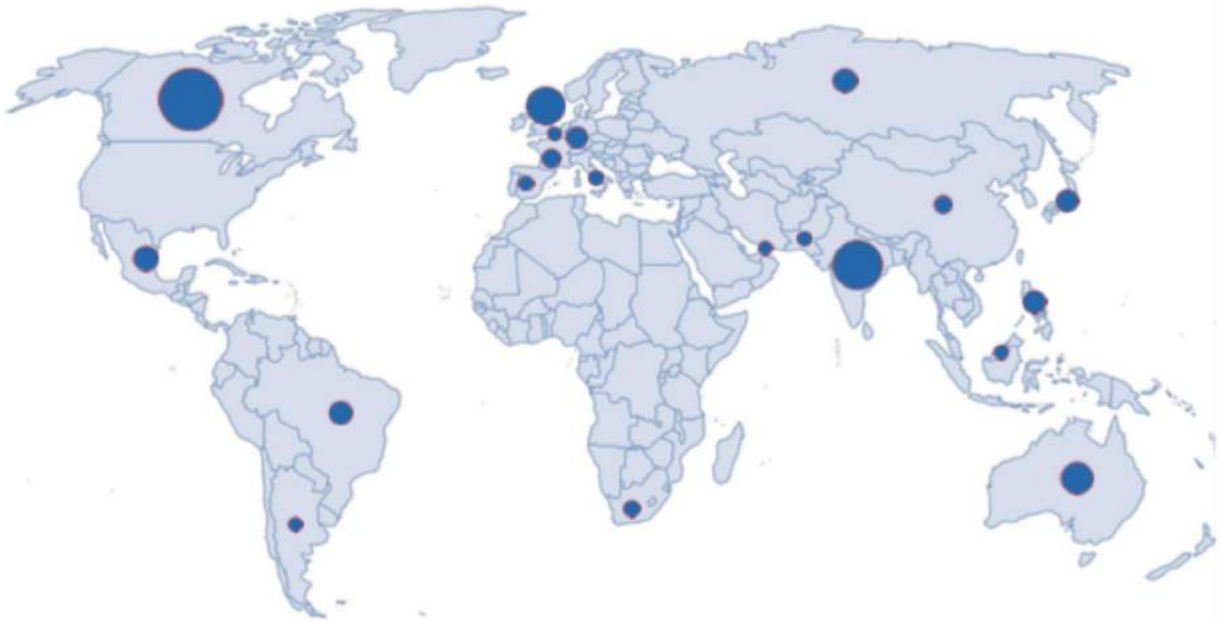
Software Download


Login:
Password:
FEDERAL BUREAU OF INVESTIGATION
IC3
INTERNET CRIME COMPLAINT CENTER
2017
Internet Crime Report

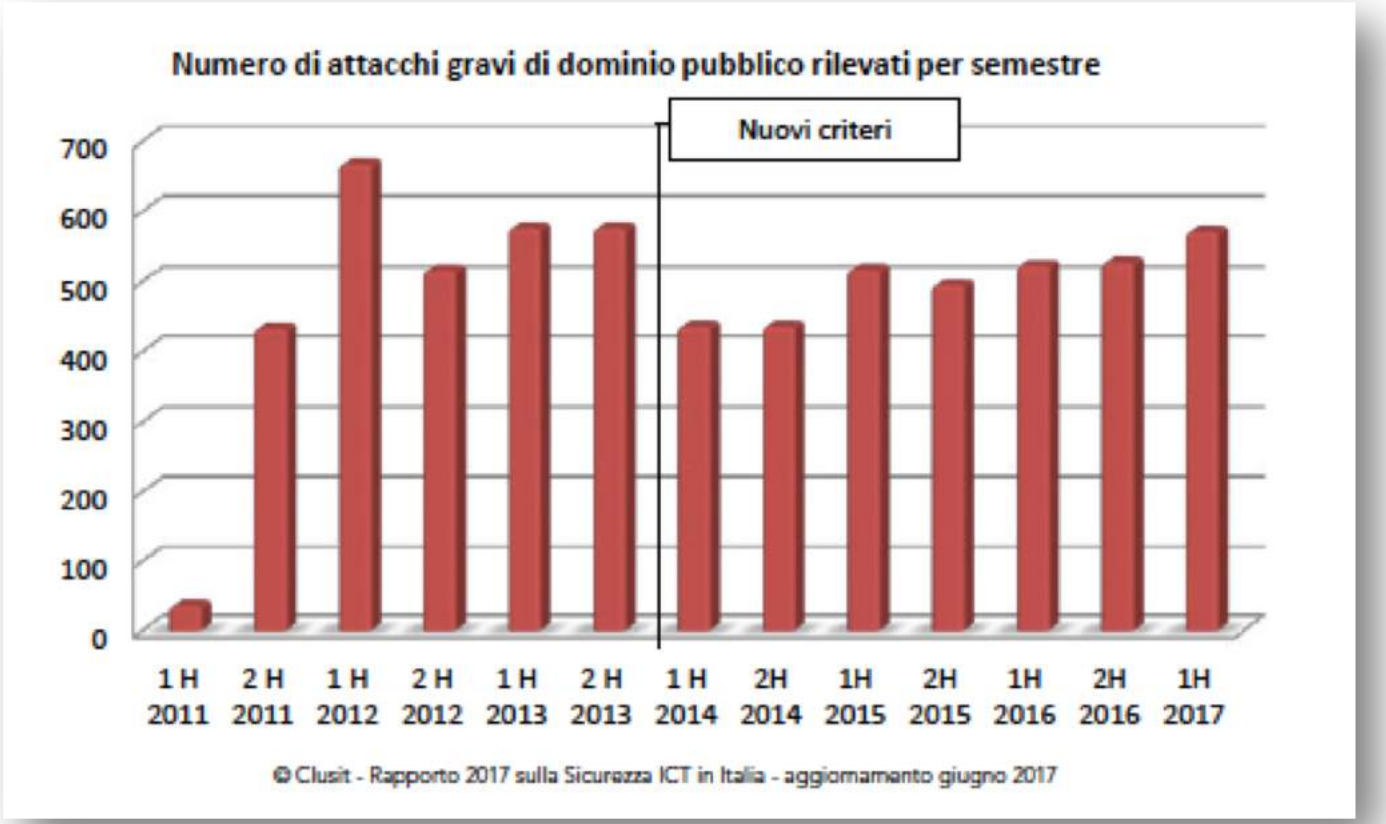

FEDERAL BUREAU OF INVESTIGATION
IC3
INTERNET CRIME COMPLAINT CENTER
Interne

Top 20 Foreign Countries by Victim

Excluding the United States[17]



1. Canada	3,164	6. Russian Federation	594	11. France	368	16. Netherlands	266
2. India	2,819	7. Brazil	558	12. China	366	17. Malaysia	265
3. United Kingdom	1,383	8. Germany	466	13. South Africa	349	18. United Arab Emirates	259
4. Australia	989	9. Philippines	453	14. Italy	291	19. Spain	248
5. Mexico	632	10. Japan	413	15. Pakistan	276	20. Argentina	238



Garofalo&Partners

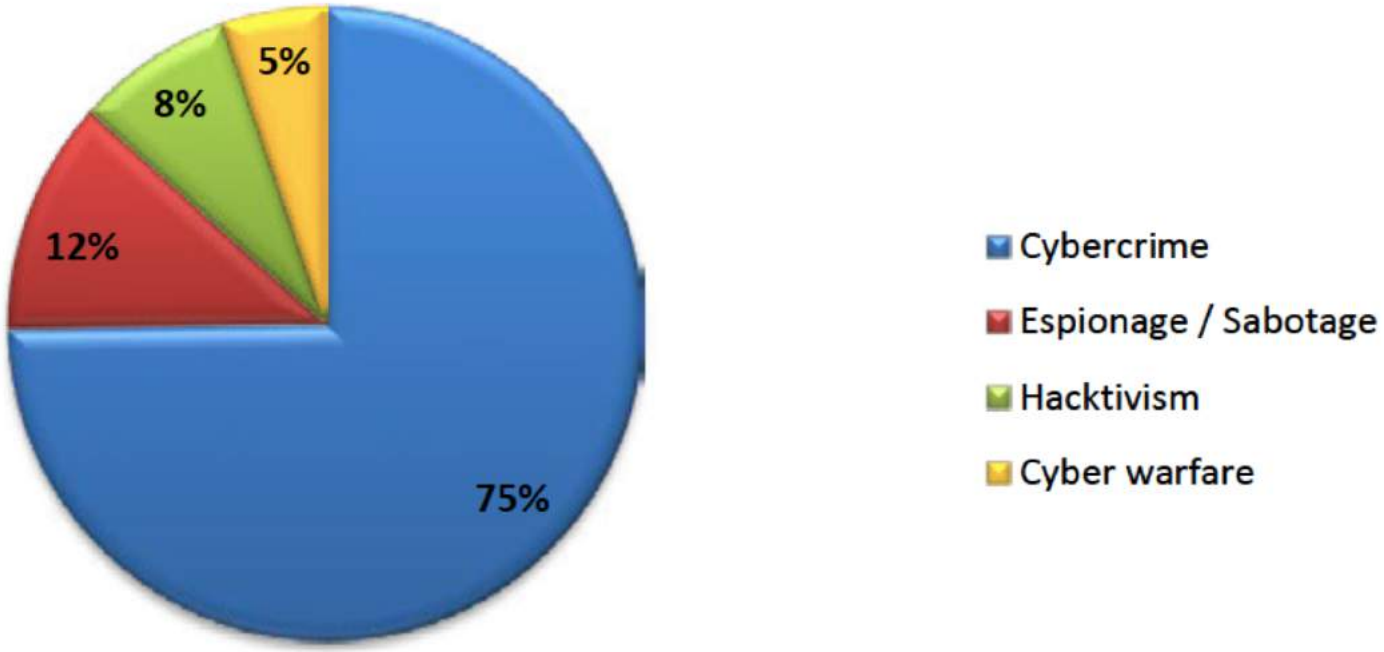
Distribuzione degli attaccanti per tipologia e trend evolutivi

ATTACCANTI PER TIPOLOGIA	2011	2012	2013	2014	2015	2016	2H 2016	1H 2017	1H 2017 su 2H 2016	Trend 2016
Cybercrime	170	633	609	526	684	751	377	427	13,26%	↑
Hacktivism	114	368	451	236	209	161	78	46	-41,03%	↓
Espionage / Sabotage	23	29	67	69	96	88	30	68	126,67%	↑
Information Warfare	14	43	25	42	23	50	42	30	-28,57%	↘
TOTALE	469	1.183	1.152	873	1.012	1.050	527	571	+8,35%	↗



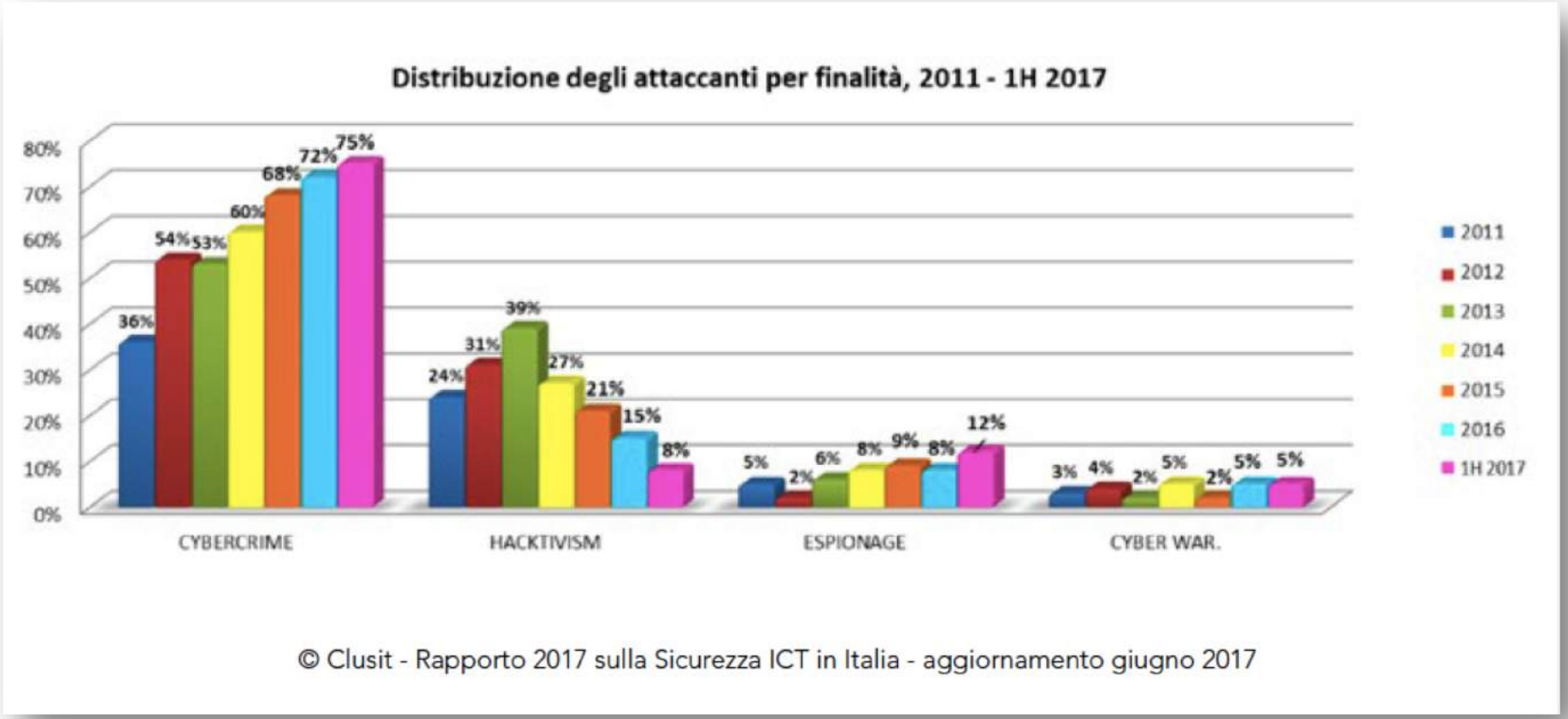
Garofalo&Partners

Tipologia e distribuzione degli attaccanti - 1H 2017



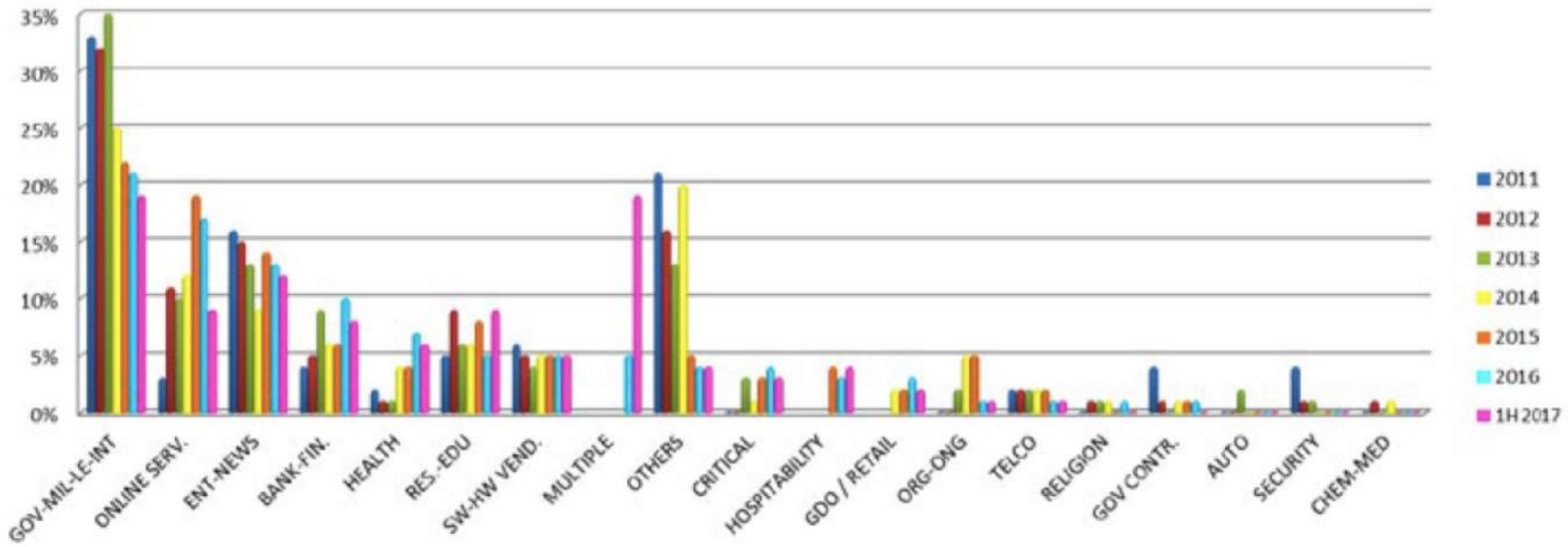
© Clusit - Rapporto 2017 sulla Sicurezza ICT in Italia - aggiornamento giugno 2017

Garofalo&Partners



© Clusit - Rapporto 2017 sulla Sicurezza ICT in Italia - aggiornamento giugno 2017

Distribuzione percentuale per tipologia di vittima 2011 - 1H 2017



© Clusit - Rapporto 2017 sulla Sicurezza ICT in Italia - aggiornamento giugno 2017

Come si arriva al GDPR



Il nuovo regolamento dell' Unione Europea n. 2016/679

- Pubblicato in gazzetta ufficiale il 4 maggio 2016, è frutto di un iter legislativo durato quattro anni;
- Gli Stati membri dell' UE hanno avuto due anni di tempo, a partire dal ventesimo giorno dalla pubblicazione (24 maggio), per allineare la normativa nazionale alle nuove prescrizioni introdotte dal Nuovo Regolamento, che diventerà definitivamente e direttamente applicabile in tutto il territorio UE a partire dal 25 maggio 2018.
- Viene abrogata la direttiva 95/46/ce che per prima aveva fissato la normativa in materia di dati personali.

E il Codice Privacy ?

Per quanto riguarda il D.lgs 196/2003 , il Regolamento sostituirebbe (non integralmente) il " Codice Privacy" , e anche se in due decenni si è creata una stratificazione molto solida nella disciplina italiana sarà, tuttavia, necessario un coordinamento normativo da parte del legislatore domestico.

Ambito di applicazione materiale del Regolamento

Il Reg. UE si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio

Il Reg. UE non si applica ai trattamenti di dati personali:

- Effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell' Unione;
- Effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico;
- Effettuati dalle autorità competenti a fini di prevenzione, indagine, o perseguimento di reati

Ambito di applicazione territoriale

Il Reg. UE ha per oggetto diritti e libertà delle persone fisiche …

Si applica :

- Al trattamento di dati personali effettuato da un Titolare stabilito nella UE;
- Al trattamento di dati personali effettuato da Titolari non stabiliti nell' UE , quando le attività di trattamento riguardano l'offerta di beni o la prestazione di servizi agli interessati nell'Unione, oppure il monitoraggio del loro comportamento, nella misura in cui tale comportamento ha luogo all'interno dell'Unione.

Alcune definizioni giuridiche - Art 4

Dato personale: *qualsiasi informazione* riguardante una persona fisica identificata o identificabile "(interessato)" . E' identificabile la persona che può essere identificata *direttamente o indirettamente* ;

Es: nome, cognome o denominazione, indirizzo,codice fiscale, ma anche un'immagine, la registrazione della voce di una persona, ecc..

Trattamento: *qualsiasi operazione* o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, la conservazione, etc;

Categorie particolari di dati personali Art 9

Nel Codice si definiscono dati sensibili, e sono i dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale , nonché i dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla vita sessuale e alla salute .

Sono dati oggetto di una **protezione rafforzata**, consistente, soprattutto, nel fatto che essi non possono essere usati senza il consenso scritto della persona e che non possono essere diffusi.

Le figure Privacy in generale:

TITOLARE DEL TRATTAMENTO



RESPONSABILE DEL TRATTAMENTO



INCARICATO

A questi si devono aggiungere:

- ✓l'amministratore di sistema (A.D.S.), introdotto con un provvedimento ad hoc dell'Autorità Garante
- ✓Il Contitolare del trattamento, introdotto dall'art. 26 del Reg. UE
- ✓Il Data Protection Officer (D.P.O.), introdotto con il Reg. UE all' art. 37

Titolare del Trattamento
Art 4 Reg. UE

La persona fisica o giuridica, l'Autorità pubblica, il servizio o qualsiasi altro organismo,che singolarmente o insieme ad altri**, determina le finalità e i mezzi del trattamento.**

La definizione è sostanzialmente conforme a quella del Codice Privacy.

Nei casi in cui il trattamento sia svolto da una società o da una pubblica amministrazione per titolare va intesa l'entità nel suo complesso e non l'individuo o l'organo che l'amministra o la rappresenta (presidente, amministratore delegato, sindaco, ministro, direttore generale, ecc.). I casi in cui il trattamento può essere imputabile ad un individuo riguardano semmai liberi professionisti o imprese individuali.

Responsabile del Trattamento
Art. 28 Reg. UE

La persona fisica o giuridica, l 'Autorità pubblica, il servizio o qualsiasi altro organismo **che tratta dati personali per conto del Titolare.**

Nel Codice Privacy, si fa riferimento alla figura del responsabile sia come figura interna, che come figura esterna all'organizzazione del Titolare; nel Regolamento, che pure non esclude figure manageriali interne, si riferisce a soggetti esterni.

Tale soggetto deve essere **nominato obbligatoriamente** dal Titolare e ciò va documentato con un atto giuridico o contratto che regola la materia disciplinata, la durata, la natura e la finalità del trattamento.

La nuova figura del Data Protection Officer

Art 37 del Regolamento:

Il titolare del trattamento e il responsabile designano sistematicamente un responsabile della protezione dei dati ogniqualvolta:

A. Il trattamento è effettuato da una autorità o da un organismo pubblico;

B. le attività principali del titolare o del responsabile consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;

C. le attività principali del titolare o del responsabile consistono nel trattamento, su larga scala, di dati personali di tipo sensibili

Concetti da considerare :

- Trattamento dei *“ dati su larga scala”* Cons. 91.

  Sono i trattamenti relativi ad una notevole quantità di dati personali a livello regionale, nazionale e sovranazionale e che potrebbero incidere su un vasto numero di interessati .

Bisogna considerare :

1) Il numero di interessati coinvolti;
2) Il numero dei dati trattati;
3) La durata del trattamento;
4) L’estensione geografica

Raggiungibilità del DPO

Un gruppo imprenditoriale può nominare un unico DPO, a condizione che questo sia facilmente raggiungibile da ciascuno stabilimento.

WP29 interpreta la facile raggiungibilità in termini di efficiente e tempestivo supporto del DPO.

Data Protection Officer – DPO
Art. 38 a 39

Il DPO deve godere di indipendenza nel suo lavoro ed essere coinvolto in tutti i progetti ad impatto privacy; riferisce direttamente al vertice gerarchico del titolare del trattamento.

Il DPO **deve**:

1. *Informare e consigliare* il titolare, il responsabile nonché i dipendenti che eseguono il trattamento, in merito agli obblighi derivanti dal Regolamento UE;
2. *Verificare e sorvegliare* l'osservanza del Regolamento
3. *Partecipare alle valutazioni* di *privacy impact assesment* ai sensi dell'art. 35 ;
4. *Interloquire con l'autorità garante .*

- ✓E ammessa la designazione di un unico DPO per più Titolari, tenuto conto della loro struttura organizzativa e dimensione;
- ✓è designato in funzione della CONOSCENZA SPECIALISTICA della normativa e dei TRATTAMENTI di dati del Titolare, e della documentata capacità di assolvere i suoi compiti;
- ✓deve conoscere lo specifico settore di attività e struttura organizzativa del Titolare, e i relativi sistemi informativi e esigenze di sicurezza e protezione dati;
- ✓Il DPO ha un ruolo chiave nel promuovere la cultura della protezione dei dati in azienda;
- ✓La funzione di DPO può essere esercitata anche avvalendosi di risorse esterne in base a un contratto di servizi

- ✓Gode di piena autonomia e indipendenza; non deve ricevere istruzioni condizionanti per quanto concerne l'esecuzione dei suoi compiti
- ✓non è rimosso o penalizzato dal titolare per l'adempimento dei suoi compiti , nel caso in cui sia stato individuato come risorsa interna

- ✓ I suoi compiti e funzioni non devono dar adito a un conflitto di interessi

  esempio : NON può essere il RESPONSABILE ICT

Principi del Regolamento

I dati devono essere:

- Trattati in modo lecito equo e trasparente
- Raccolti per finalità determinate, esplicite e legittime
- successivamente trattati in modo NON incompatibile con tali finalità
- Adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità (minimizzazione dati)
- Esatti e se necessario aggiornati
- Conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati
- Trattati in modo da garantire un'adeguata SICUREZZA dei dati personali, compresa la protezione, con misure TECNICHE e ORGANIZZATIVE adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (integrità e riservatezza)
- **Di tali principi è RESPONSABILE IL Titolare e il RESPONSABILE DEL TRATTAMENTO che deve comprovarne il rispetto**

Principi del Regolamento

Approccio basato sul rischio : considerando n. 77 e 78 del Regolamento → il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato; l'individuazione di migliori prassi per attenuare il rischio potrebbero essere forniti mediante un'analisi del contesto

Accountability → necessità che il responsabile adotti misure appropriate ed efficaci per attuare i principi di protezione dei dati , e necessità di dimostrare che sono adottate misure appropriate ed efficaci

Privacy by design → protezione dei dati fin dalla progettazione (pseudonimizzazione)

Privacy by default → la tutela della protezione del dato deve diventare l'impostazione predefinita

I diritti degli interessati

Il Regolamento assegna all'interessato , salvo eccezioni stabilite nell'art 23, i seguenti diritti:

- ✓Informativa e consenso
- ✓Accesso
- ✓Rettifica
- ✓Oscuramento
- ✓Limitazione del trattamento
- ✓Portabilità dei dati
- ✓Opposizione del trattamento

In particolare ….. Informativa

il Regolamento prevede numerose informazioni aggiuntive da fornire all'interessato in forma concisa, intelligibile, trasparente con un linguaggio chiaro e semplice . Va resa per iscritto o anche con altri mezzi elettronici e anche oralmente.

Nell' Art 13 del Regolamento sono specificati alcuni punti che non possono mancare nell'informativa , tra cui:

- I dati di contatto del DPO
- La base giuridica del trattamento
- Il periodo di conservazione dei dati personali
- L'esistenza del diritto dell'interessato di revocare il consenso, accedere ai suoi dati e/o rettificarli
- L'inadempimento del titolare è sanzionato fino a € 20.000.000, o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

Consenso al Trattamento (ART. 4.11 – 7)

Il consenso è una manifestazione di volontà recettizia con la quale l'interessato autorizza il trattamento dei propri dati. L'obbligo di basare il trattamento sul consenso incombe esclusivamente sul titolare del trattamento.

- Per i dati "sensibili" (si veda art. 9 regolamento) il consenso DEVE essere "esplicito"; lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati (compresa la profilazione – art. 22).
- DEVE essere, in tutti i casi, libero, specifico, informato e inequivocabile e NON è ammesso il consenso tacito o presunto

Adempimenti da parte del titolare e del responsabile del trattamento

1)Art. 30 - Registro dei trattamenti



Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio, devono tenere un registro delle operazioni di trattamento i cui contenuti sono indicati all'art. 30.

Si tratta di uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico – indispensabile per ogni valutazione e analisi del rischio.

Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

Sanzioni: fino a 10.000.000,00, o per le imprese fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente.

2)Valutazione d'impatto sulla protezione dei dati (DPIA) e consultazione preventiva Art 35

Quando un tipo di trattamento, allorchè prevede l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e la finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare effettua, prima di procedere al trattamento, una valutazione d'impatto dei trattamenti previsti, e se quest'ultima indica che il trattamento presenta un rischio elevato, il titolare deve consultare preventivamente l'Autorità (Art 36)

Le linee guida dei Garanti Europei (WP29) adottate il 04.10.17 definiscono ancor meglio l'oggetto della DPIA, la tipologia di trattamenti soggetti alla valutazione e in che modo deve essere effettuata una DPIA.

Profili sanzionatori

Risarcimento e responsabilità Art 82 , natura civilistica del danno: chiunque subisca un danno materiale o immateriale causato dalla violazione del regolamento ha il diritto di ottenere il risarcimento del danno dal titolare o dal responsabile; sono meglio chiariti i principi di ripartizione della responsabilità tra titolare e responsabile e tra contitolari del trattamento

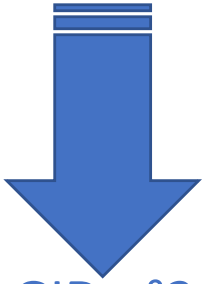
All'art 83, per quanto riguarda l'applicazione delle sanzioni amministrative pecuniarie, vengono fissate sanzioni fino a 10.000.000 Eur (20.000.000 in altri casi) o,per le imprese, fino al 2% (4% in altri casi) del fatturato mondiale totale annuo dell'esercizio precedente

…..sanzioni penali?

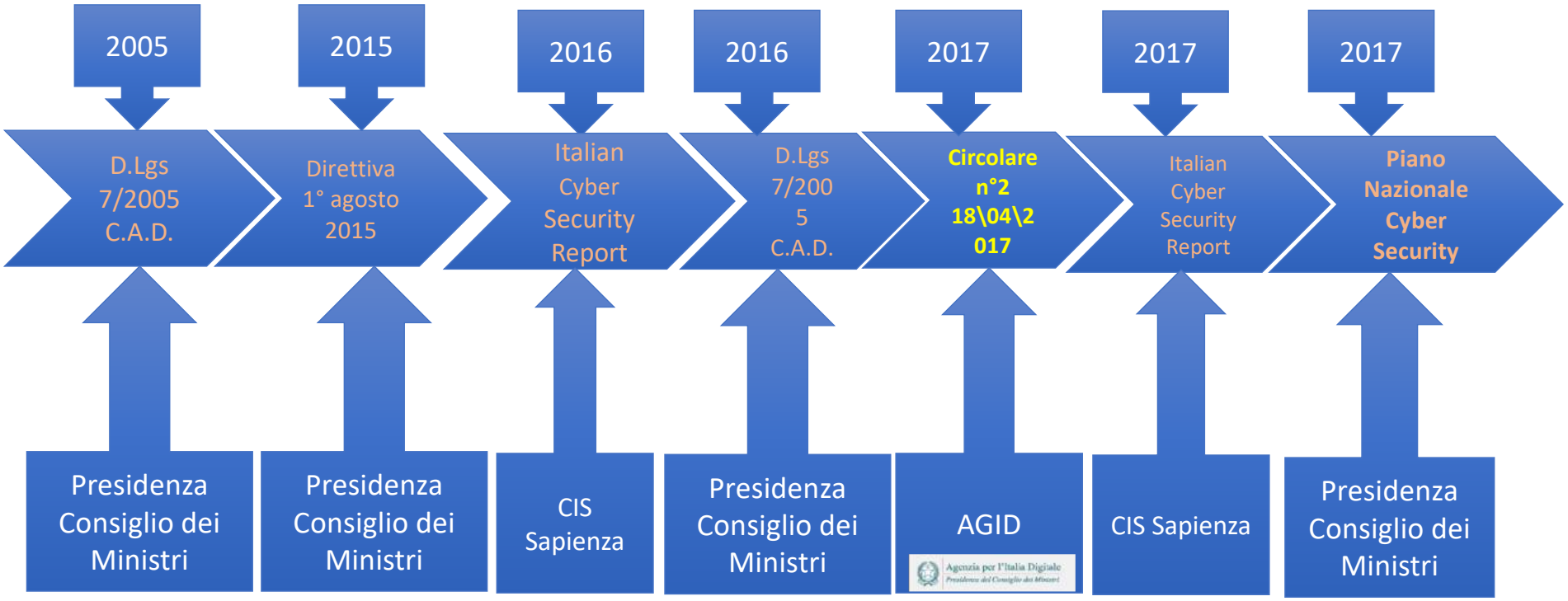


La materia penale è di respiro nazionale, quindi il Regola[illegible] può disciplinarla . Occorre verificare, in sede di abrogazione del Codice Privacy, come sarà attuata la disciplina attuale dell'art 167 che prevede il reato di trattamento illecito di dati personali.

Allegato B D.Lgs 196\2003



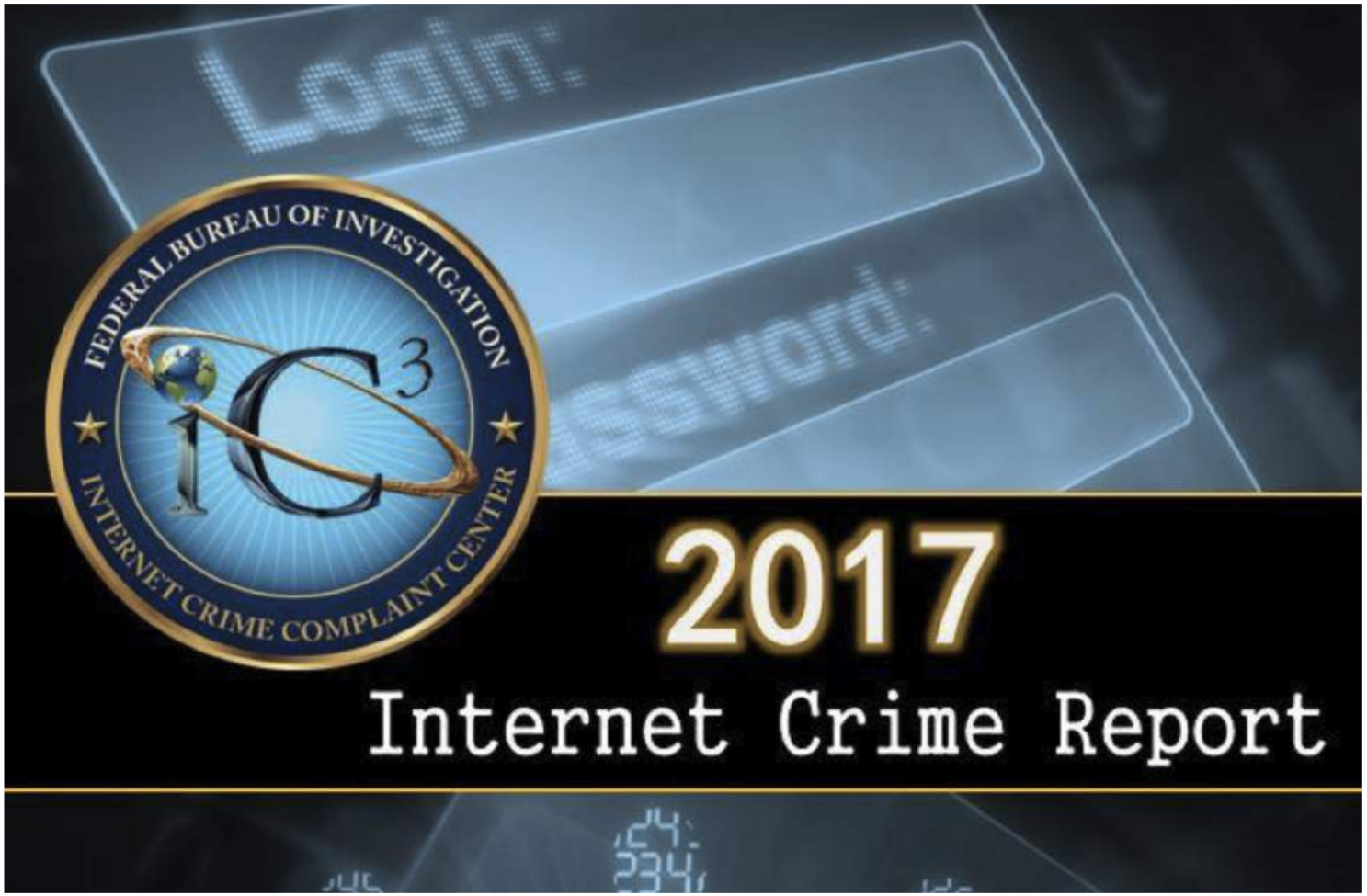
Circolare AGID n°2 Aprile 2017


2005
D.Lgs 7/2005 C.A.D.
Presidenza Consiglio dei Ministri
2015
Direttiva 1° agosto 2015
Presidenza Consiglio dei Ministri
2016
Italian Cyber Security Report
CIS Sapienza
2016
D.Lgs 7/200 5 C.A.D.
Presidenza Consiglio dei Ministri
2017
Circolare n°2 18\04\2 017
AGID
Agenzia per l'Italia Digitale
2017
Italian Cyber Security Report
CIS Sapienza
2017
Piano Nazionale Cyber Security
Presidenza Consiglio dei Ministri

Direttiva 1 agosto 2015

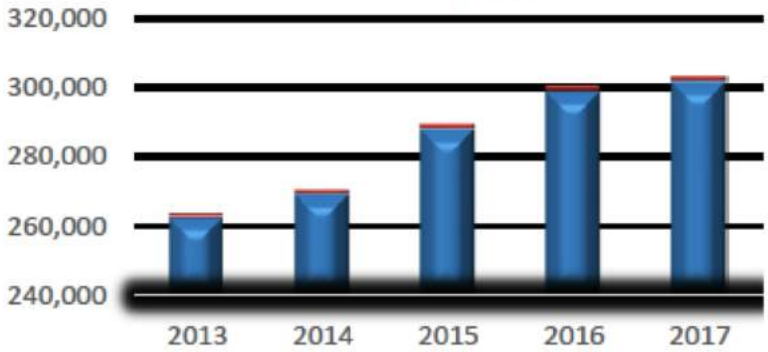
……..La definizione dei punti cardine del sistema ha consentito di approvare in breve tempo il Quadro strategico nazionale per la sicurezza dello spazio cibernetico e il correlato Piano nazionale, strumenti rivolti a porre il Paese in linea con i principali partner internazionali…….




Login:
Password:
FEDERAL BUREAU OF INVESTIGATION
IC3
INTERNET CRIME COMPLAINT CENTER
2017
Internet Crime Report

IMPORTANT STATS

IC3 COMPLAINTS LAST 5 YEARS



 # Of Complaints Reported Since Inception ('00)

4,063,933

Approximately 284,000

Average Complaints Received Each Year

$1.42 Billion

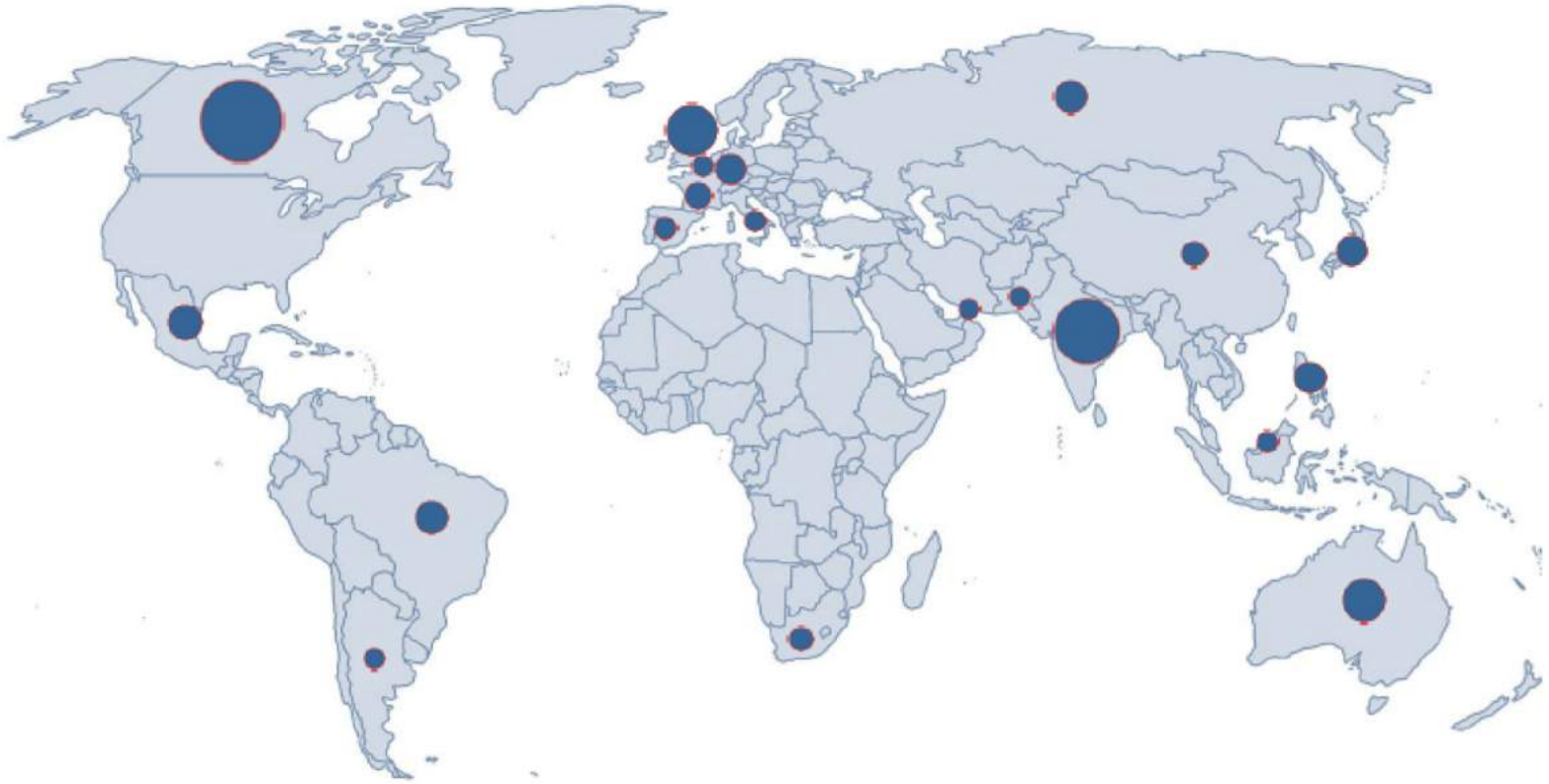
Victim Losses in **2017**

Over 800

Average Complaints Received Per Day

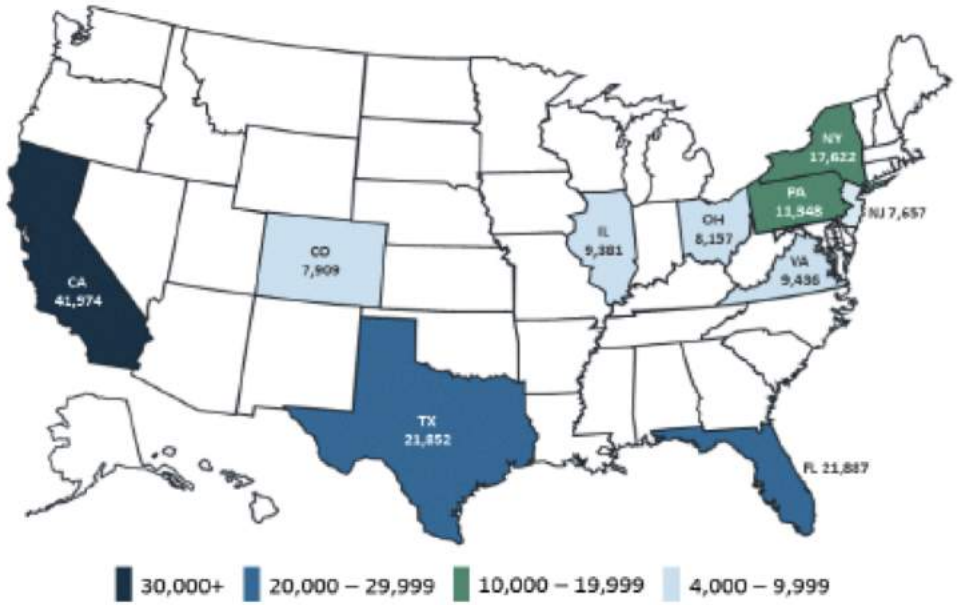
Top 20 Foreign Countries by Victim

Excluding the United States[17]

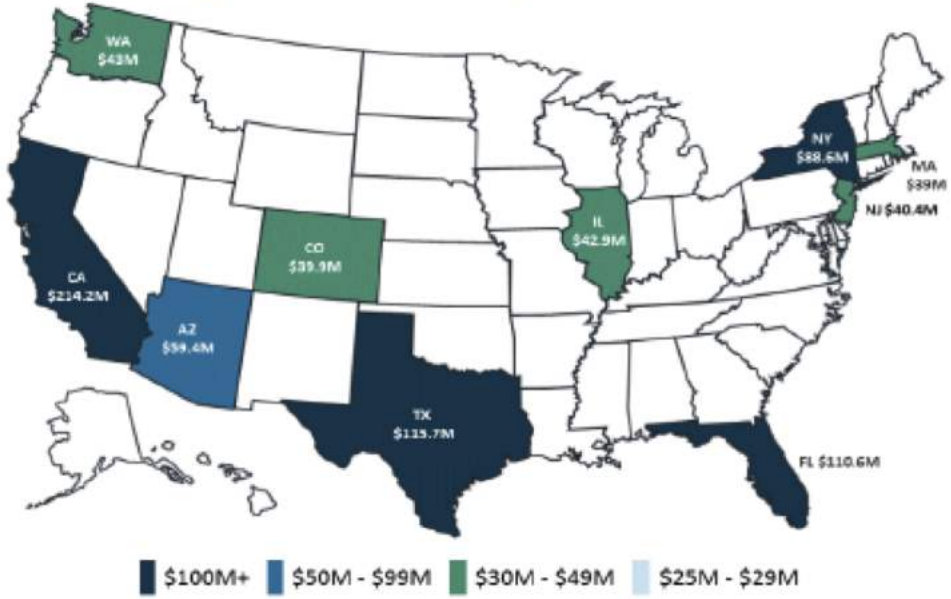


1. Canada	3,164	6. Russian Federation	594	11. France	368	16. Netherlands	266
2. India	2,819	7. Brazil	558	12. China	366	17. Malaysia	265
3. United Kingdom	1,383	8. Germany	466	13. South Africa	349	18. United Arab Emirates	259
4. Australia	989	9. Philippines	453	14. Italy	291	19. Spain	248
5. Mexico	632	10. Japan	413	15. Pakistan	276	20. Argentina	238

Top 10 States by Number of Victims [18]



Top 10 States by Victim Loss [19]



È stata comunicata sulla Gazzetta ufficiale n. 125 del 31 maggio 2017 l'adozione del nuovo Piano nazionale per la protezione cibernetica e la sicurezza informatica

Il documento – adottato dal Presidente del Consiglio su deliberazione unanime del CISR (Comitato interministeriale per la sicurezza della Repubblica), e registrato dagli Organi di controllo – mira a sviluppare gli indirizzi strategici previsti, tra i quali si ricordano:

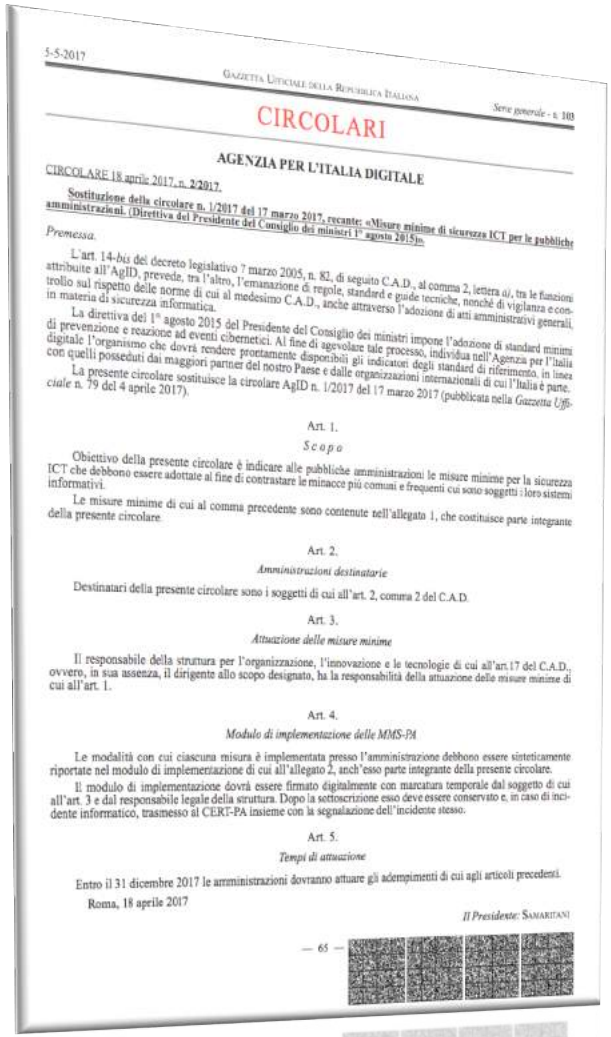
- il potenziamento delle capacità di difesa delle infrastrutture critiche nazionali e degli attori di rilevanza strategica per il sistema Paese;
- il miglioramento delle capacità tecnologiche, operative e di analisi degli attori istituzionali interessati;
- l'incentivazione della cooperazione tra istituzioni ed imprese nazionali;
- la promozione e diffusione della cultura della sicurezza cibernetica;
- il rafforzamento della cooperazione internazionale in materia di sicurezza cibernetica,
- ed, infine, il rafforzamento delle capacità di contrasto alle attività e contenuti illegali on-line.

Il nuovo Piano è stato rivisitato congiuntamente dalle Amministrazioni che compongono l'architettura nazionale cyber (Comparto intelligence, Ministero degli affari esteri e della cooperazione internazionale, Ministero dell'interno, Ministero della difesa, Ministero della giustizia, Ministero dell'economia e delle finanze, Ministero dello sviluppo economico, Agenzia per l'Italia digitale, Ufficio del Consigliere militare del Presidente del Consiglio), e fa tesoro sia dell'esperienza maturata negli ultimi anni, sia delle scelte operate nel settore dai Paesi tecnologicamente più avanzati.

QUADRO STRATEGICO NAZIONALE (QSN)

INDIRIZZI STRATEGICI

1. Potenziamento delle capacità di difesa delle Infrastrutture Critiche nazionali e degli attori di rilevanza strategica per il sistema-Paese
2. Miglioramento, secondo un approccio integrato, delle capacità tecnologiche, operative e di analisi degli attori istituzionali interessati
3. Incentivazione della cooperazione tra istituzioni ed imprese nazionali
4. Promozione e diffusione della cultura della sicurezza cibernetica
5. Rafforzamento della cooperazione internazionale in materia di sicurezza cibernetica
6. Rafforzamento delle capacità di contrasto alle attività e contenuti illegali *on-line*



5-5-2017 GAZZETTA UFFICIALE DELLA REPUBBLICA ITALIANA Serie generale - n. 103

CIRCOLARI

AGENZIA PER L'ITALIA DIGITALE

CIRCOLARE 18 aprile 2017, n. 2/2017.

Sostituzione della 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)».

Premessa.

L'art. 14-*bis* del decreto legislativo 7 marzo 2005, n. 82, di seguito C.A.D., al comma 2, lettera *a)*, tra le funzioni attribuite all'AgID, prevede, tra l'altro, l'emanazione di regole, standard e guide tecniche, nonché di vigilanza e controllo sul rispetto delle norme di cui al medesimo C.A.D., anche attraverso l'adozione di atti amministrativi generali, in materia di sicurezza informatica.

La direttiva del 1° agosto 2015 del Presidente del Consiglio dei ministri impone l'adozione di standard minimi di prevenzione e reazione ad eventi cibernetici. Al fine di agevolare tale processo, individua nell'Agenzia per l'Italia digitale l'organismo che dovrà rendere prontamente disponibili gli indicatori degli standard di riferimento, in linea con quelli posseduti dai maggiori partner del nostro Paese e dalle organizzazioni internazionali di cui l'Italia è parte.

La presente circolare sostituisce la circolare AgID n. 1/2017 del 17 marzo 2017 (pubblicata nella *Gazzetta Ufficiale* n. 79 del 4 aprile 2017).

Art. 1.

Scopo

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

Le misure minime di cui al comma precedente sono contenute nell'allegato 1, che costituisce parte integrante della presente circolare.

Art. 2.

Amministrazioni destinatarie

Destinatari della presente circolare sono i soggetti di cui all'art. 2, comma 2 del C.A.D.

Art. 3.

Attuazione delle misure minime

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 della attuazione delle misure minime di cui all'art. 1.

Art. 4.

Modulo di implementazione delle MMS-PA

Le modalità con cui ciascuna misura è implementata presso l'amministrazione debbono essere sinteticamente riportate nel modulo di implementazione di cui all'allegato 2, anch'esso parte integrante della presente circolare.

Il modulo di implementazione dovrà essere firmato digitalmente con marcatura temporale dal soggetto di cui all'art. 3 e dal responsabile legale della struttura. Dopo la sottoscrizione esso deve essere conservato e, in caso di incidente informatico, trasmesso al CERT-PA insieme con la segnalazione dell'incidente stesso.

Art. 5.

Tempi di attuazione

Entro il 31 dicembre 2017 le amministrazioni dovranno attuare gli adempimenti di cui agli articoli precedenti.

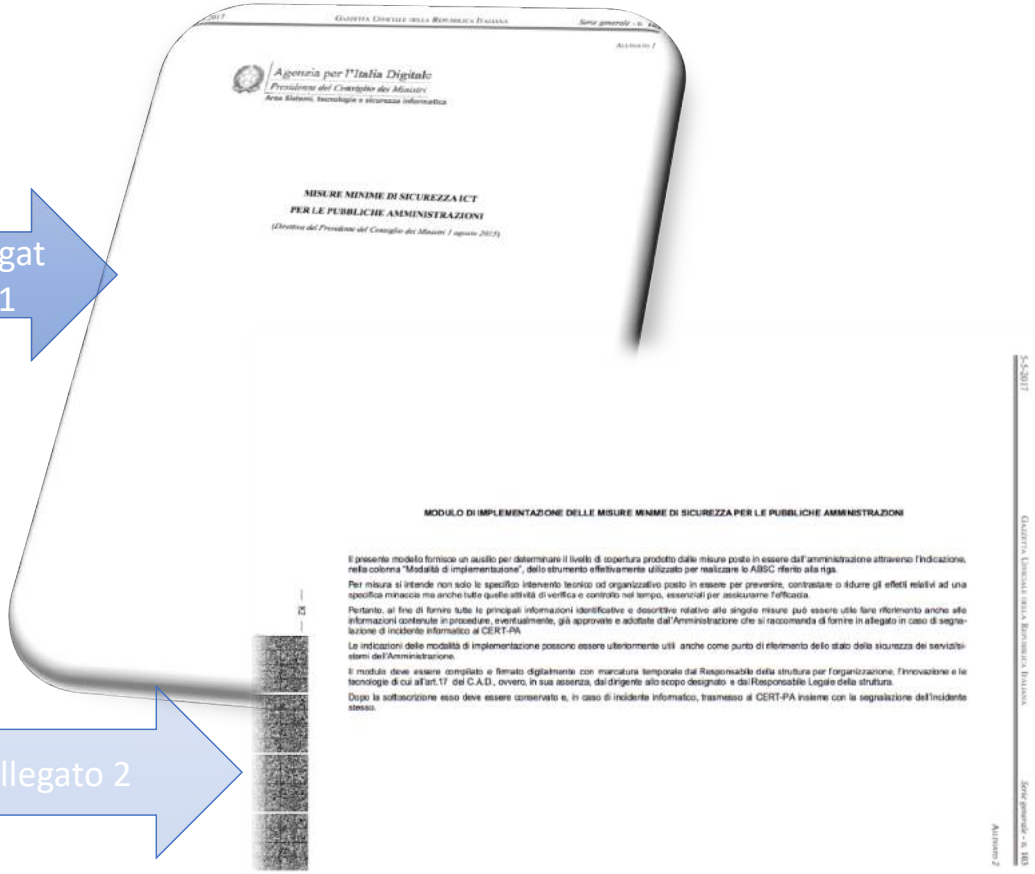
Roma, 18 aprile 2017

Il Presidente: SAMARITANI

— 65 —

Allegat o 1

Allegato 2



Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri
Area Sistemi, tecnologie e sicurezza informatica

MISURE MINIME DI SICUREZZA ICT
PER LE PUBBLICHE AMMINISTRAZIONI

(Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015)

MODULO DI IMPLEMENTAZIONE DELLE MISURE MINIME DI SICUREZZA PER LE PUBBLICHE AMMINISTRAZIONI

Il presente modello fornisce un ausilio per determinare il livello di copertura prodotto dalle misure poste in essere dall'amministrazione attraverso l'indicazione, nella colonna "Modalità di implementazione", dello strumento effettivamente utilizzato per realizzare lo ABSC riferito alla riga.

Per misura si intende non solo lo specifico intervento tecnico od organizzativo posto in essere per prevenire, contrastare o ridurre gli effetti relativi ad una specifica minaccia ma anche tutte quelle attività di verifica e controllo nel tempo, essenziali per assicurarne l'efficacia.

Pertanto, al fine di fornire tutte le principali informazioni identificative e descrittive relative alla singola misure può essere utile fare riferimento anche alle informazioni contenute in procedure, eventualmente, già approvate e adottate dall'Amministrazione che si raccomanda di fornire in allegato in caso di segnalazione di incidente informatico al CERT-PA.

Le indicazioni delle modalità di implementazione possono essere ulteriormente utili anche come punto di riferimento dello stato della sicurezza dei servizi/sistemi dell'Amministrazione.

Il modulo deve essere compilato e firmato digitalmente con marcatura temporale dal Responsabile della struttura per l'organizzazione, l'innovazione e le tecnologie di cui all'art.17 del C.A.D., ovvero, in sua assenza, dal dirigente allo scopo designato o dal Responsabile Legale della struttura.

Dopo la sottoscrizione esso deve essere conservato e, in caso di incidente informatico, trasmesso al CERT-PA insieme con la segnalazione dell'incidente stesso.

CIRCOLARI

AGENZIA PER L'ITALIA DIGITALE

CIRCOLARE 18 aprile 2017, n. **2/2017**.

Sostituzione della 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)».

Premessa.

L'art. 14-*bis* del decreto legislativo 7 marzo 2005, n. 82, di seguito C.A.D., al comma 2, lettera *a)*, tra le funzioni attribuite all'AgID, prevede, tra l'altro, l'emanazione di regole, standard e guide tecniche, nonché di vigilanza e controllo sul rispetto delle norme di cui al medesimo C.A.D., anche attraverso l'adozione di atti amministrativi generali, in materia di sicurezza informatica.

La direttiva del 1° agosto 2015 del Presidente del Consiglio dei ministri impone l'adozione di standard minimi di prevenzione e reazione ad eventi cibernetici. Al fine di agevolare tale processo, individua nell'Agenzia per l'Italia digitale l'organismo che dovrà rendere prontamente disponibili gli indicatori degli standard di riferimento, in linea con quelli posseduti dai maggiori partner del nostro Paese e dalle organizzazioni internazionali di cui l'Italia è parte.

La presente circolare sostituisce la circolare AgID n. 1/2017 del 17 marzo 2017 (pubblicata nella *Gazzetta Ufficiale* n. 79 del 4 aprile 2017).

Art. 1.

Scopo

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

Le misure minime di cui al comma precedente sono contenute nell'allegato 1, che costituisce parte integrante della presente circolare.

Art. 2.

Amministrazioni destinatarie

Destinatari della presente circolare sono i soggetti di cui all'art. 2, comma 2 del C.A.D.

Art. 3.

Attuazione delle misure minime

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 della attuazione delle misure minime di cui all'art. 1.

Art. 4.

Modulo di implementazione delle MMS-PA

Le modalità con cui ciascuna misura è implementata presso l'amministrazione debbono essere sinteticamente riportate nel modulo di implementazione di cui all'allegato 2, anch'esso parte integrante della presente circolare.

Il modulo di implementazione dovrà essere firmato digitalmente con marcatura temporale dal soggetto di cui all'art. 3 e dal responsabile legale della struttura. Dopo la sottoscrizione esso deve essere conservato e, in caso di incidente informatico, trasmesso al CERT-PA insieme con la segnalazione dell'incidente stesso.

Art. 5.

Tempi di attuazione

Entro il 31 dicembre 2017 le amministrazioni dovranno attuare gli adempimenti di cui agli articoli precedenti.

Roma, 18 aprile 2017

1.3 RIFERIMENTI

	ID	Descrizione
[D.1]	Direttiva 1 agosto 2015	Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015
[D.2]	SANS 20	CIS Critical Security Controls for Effective Cyber Defense - versione 6.0 di ottobre 2015
[D.3]	Cyber Security Report	La Sapienza - 2015 Italian Cyber Security Report del CIS -

1.4 ACRONIMI

Acronimo	Descrizione
ABSC	Agid Basic Security Control(s)
CCSC	Center for Critical Security Control
CSC	Critical Security Control
FNSC	Framework Nazionale di Sicurezza Cibernetica
NSC	Nucleo di Sicurezza Cibernetica

What is SANS?

SANS is the most trusted and by far the largest source for information security training in the world. We offer training through several delivery methods - live & virtual, classroom-style, online at your own pace or webcast with live instruction, guided study with a local mentor, or privately at your workplace where even your most remote colleagues can join in via Simulcast. Our computer security courses are developed by industry leaders in numerous fields including cyber security training, network security, forensics, audit, security leadership, and application security. Courses are taught by real-world practitioners who are the best at ensuring you not only learn the material, but that you can apply it immediately when you return to the office. All of SANS security courses are also offered at a government customer's desired location. In addition to top-notch training, we offer certification via GIAC, an affiliate of the SANS Institute, a certification body featuring over 20 hands-on, technical certifications in information security, and optional Master's Degree programs through SANS Technology Institute graduate school, as well as numerous free security resources including newsletters, whitepapers and webcasts.

https://www.sans.org/

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

Gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso

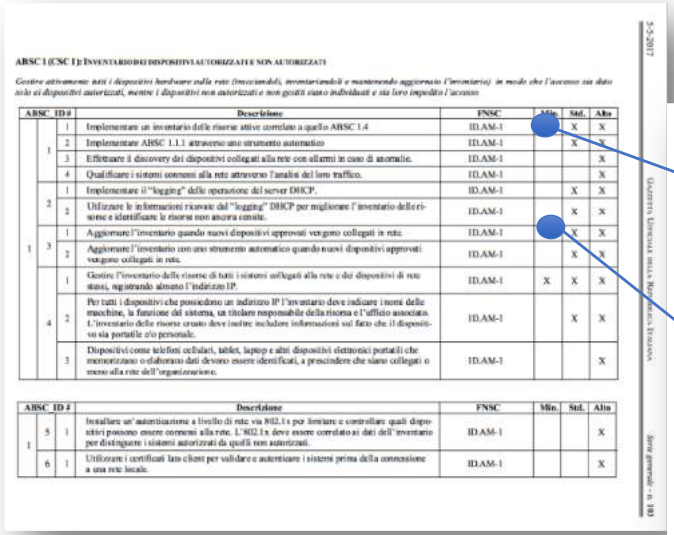
ABSC_ID #			Descrizione	FNSC	Min.	Std.	Alto
1	1	1	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	ID.AM-1	X	X	X
		2	Implementare ABSC 1.1.1 attraverso uno strumento automatico	ID.AM-1		X	X
		3	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	ID.AM-1			X
		4	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	ID.AM-1			X
	2	1	Implementare il "logging" delle operazione del server DHCP.	ID.AM-1		X	X
		2	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	ID.AM-1		X	X
	3	1	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	ID.AM-1	X	X	X
		2	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	ID.AM-1		X	X
	4	1	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	ID.AM-1	X	X	X
		2	Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine, la funzione del sistema, un titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o personale.	ID.AM-1		X	X
		3	Dispositivi come telefoni cellulari, tablet, laptop e altri dispositivi elettronici portatili che memorizzano o elaborano dati devono essere identificati, a prescindere che siano collegati o meno alla rete dell'organizzazione.	ID.AM-1			X

ABSC_ID #			Descrizione	FNSC	Min.	Std.	Alto
1	5	1	Installare un'autenticazione a livello di rete via 802.1x per limitare e controllare quali dispositivi possono essere connessi alla rete. L'802.1x deve essere correlato ai dati dell'inventario per distinguere i sistemi autorizzati da quelli non autorizzati.	ID.AM-1			X
	6	1	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	ID.AM-1			X

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

Gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso

ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
1	1	1	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4		M
		2	Implementare ABSC 1.1.1 attraverso uno strumento automatico		S
		3	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.		A
		4	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.		A
	2	1	Implementare il "logging" delle operazione del server DHCP.		S
		2	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.		S
	3	1	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.		M
		2	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.		S



ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

Gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso

ABSC_ID #			Descrizione	FNSC	Min.	Std.	Alto
1	1	1	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	ID.AM-1		X	X
		2	Implementare ABSC 1.1.1 attraverso uno strumento automatico	ID.AM-1		X	X
		3	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	ID.AM-1			X
		4	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	ID.AM-1			X
	2	1	Implementare il "logging" delle operazione del server DHCP.	ID.AM-1		X	X
		2	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	ID.AM-1		X	X
	3	1	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	ID.AM-1		X	X
		2	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	ID.AM-1		X	X
	4	1	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	ID.AM-1	X	X	X
		2	Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine, la funzione del sistema, un titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o personale.	ID.AM-1		X	X
		3	Dispositivi come telefoni cellulari, tablet, laptop e altri dispositivi elettronici portatili che memorizzano o elaborano dati devono essere identificati, a prescindere che siano collegati o meno alla rete dell'organizzazione.	ID.AM-1			X

ABSC_ID #			Descrizione	FNSC	Min.	Std.	Alto
1	5	1	Installare un'autenticazione a livello di rete via 802.1x per limitare e controllare quali dispositivi possono essere connessi alla rete. L'802.1x deve essere correlato ai dati dell'inventario per distinguere i sistemi autorizzati da quelli non autorizzati.	ID.AM-1			X
	6	1	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	ID.AM-1			X

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

Gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso

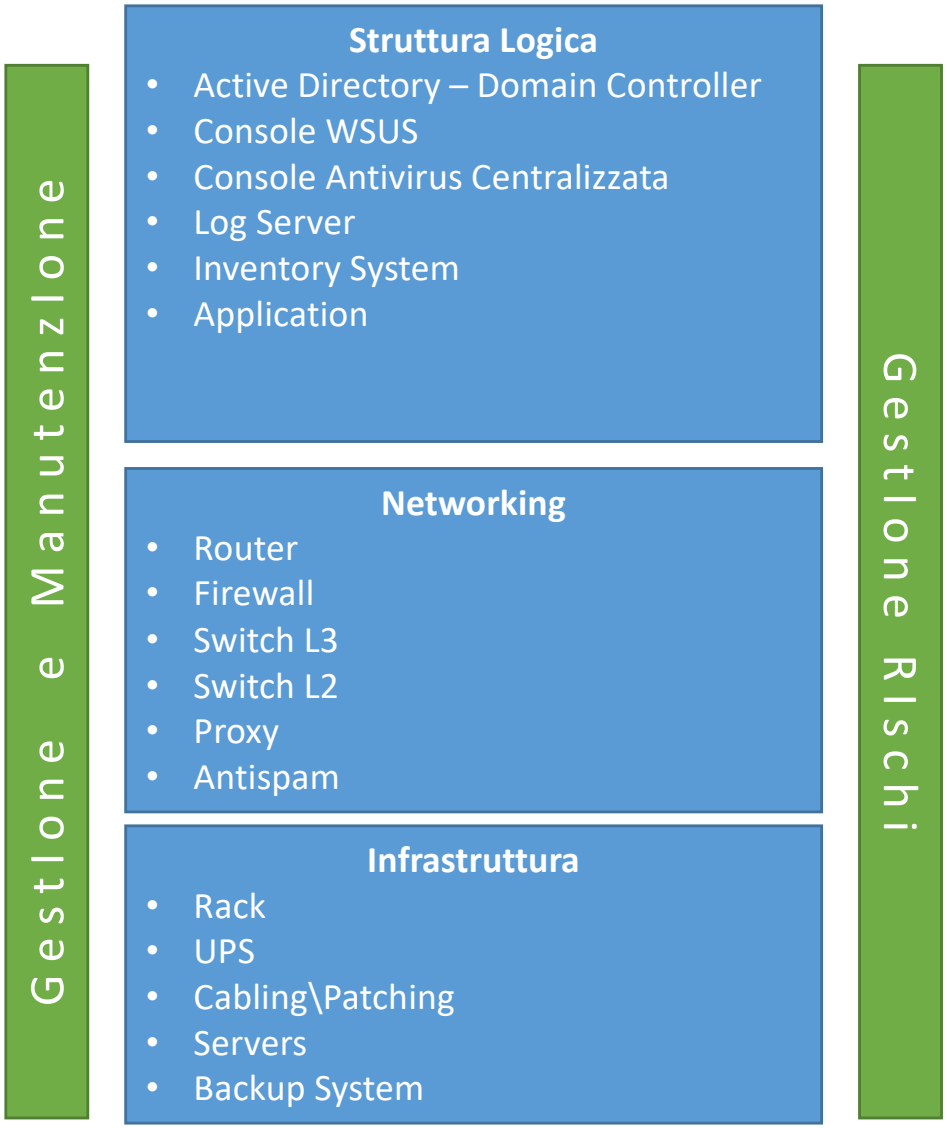
ABSC_ID #			Descrizione	Modalità di Implementazione	Liv
1	1	1	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4		M
		2	Implementare ABSC 1.1.1 attraverso uno strumento automatico		S
		3	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.		A
		4	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.		A
	2	1	Implementare il "logging" delle operazione del server DHCP.		S
		2	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.		S
	3	1	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.		M
		2	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.		S

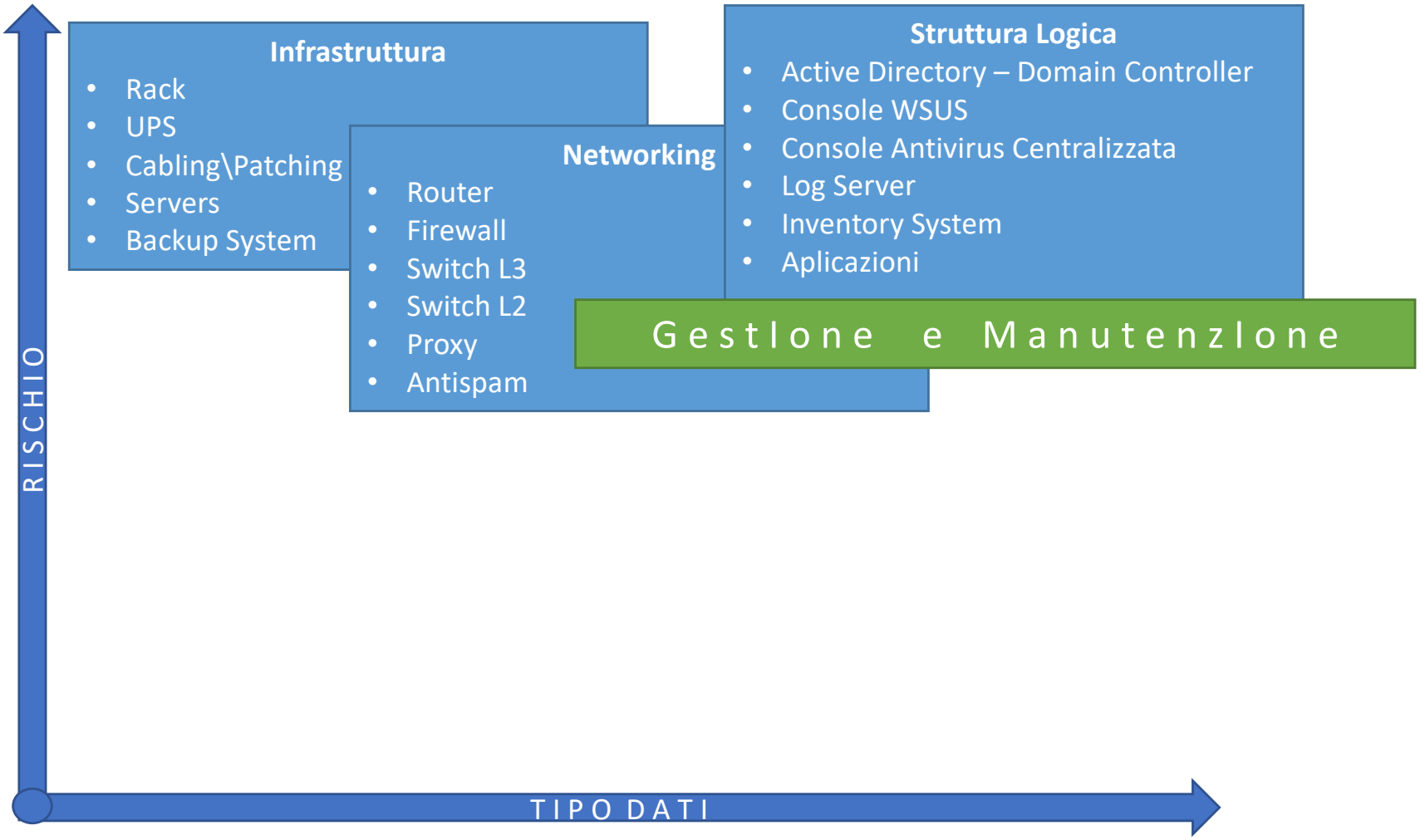
Riferimenti

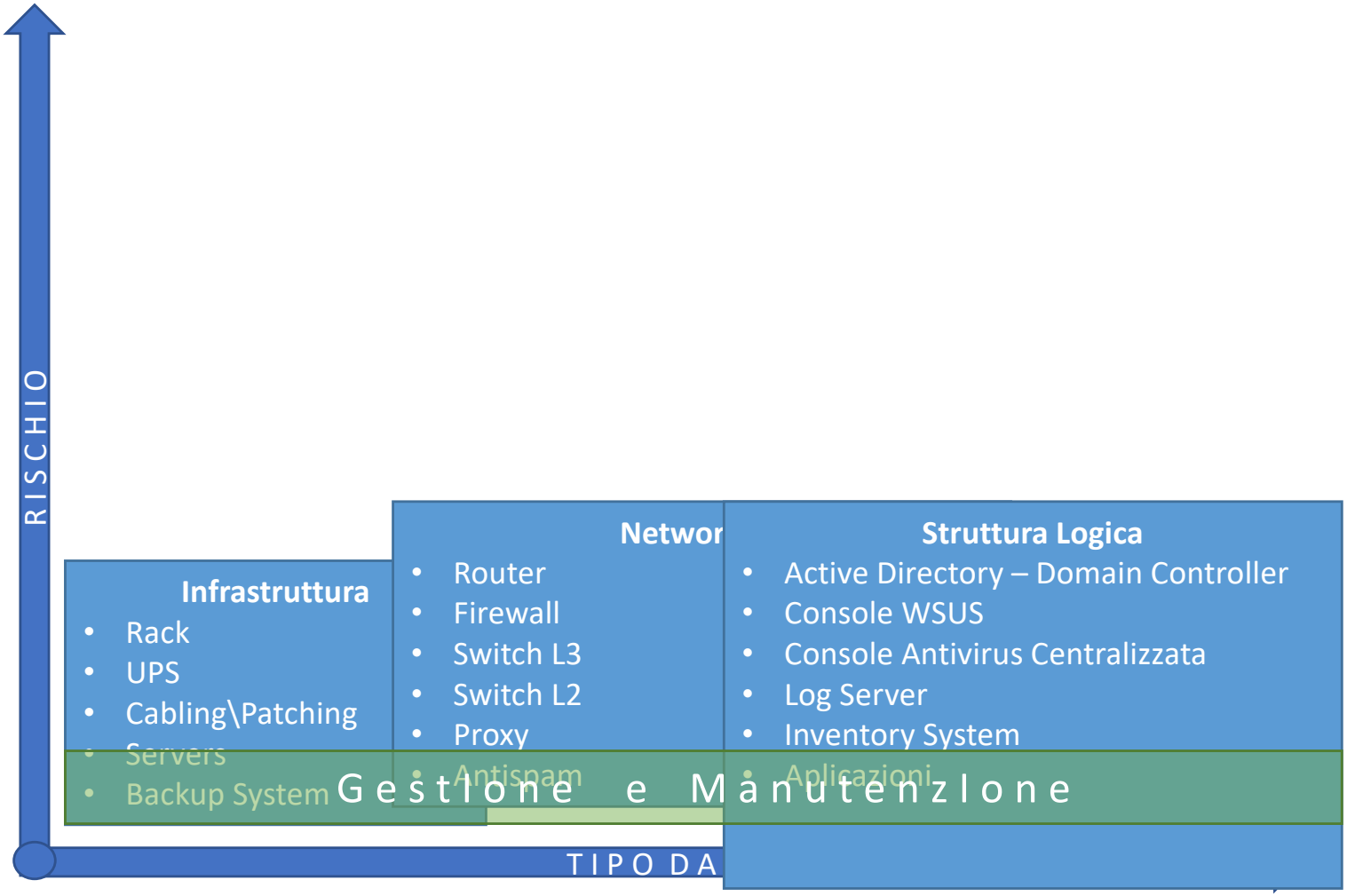
- https://www.sicurezzanazionale.gov.it/sisr.nsf/documentazione/normativa-di-riferimento/direttiva-1-agosto-2015.html
- http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/cert-pa/misure-minime-sicurezza-ict-pubbliche-amministrazioni
- https://www.cert-pa.it/documents/10184/27607/CircolareAgID_170418_n_2_2017_Mis_minime_sicurezza_ICT_PA-GU-103-050517.pdf/7ca821ea-f8cc-4310-9fad-3c6ec1ca7f85
- http://www.agid.gov.it/cad/codice-amministrazione-digitale
- https://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/pubblicato-il-nuovo-piano-nazionale-cyber.html
- http://cni-online.it/Attach/DV12627.pdf
- http://www.cni-online.it/Home/PrintDetails?id=12295
- https://www.sans.org/critical-security-controls
- https://www.sans.org/reading-room/
- https://clusit.it/

I

action

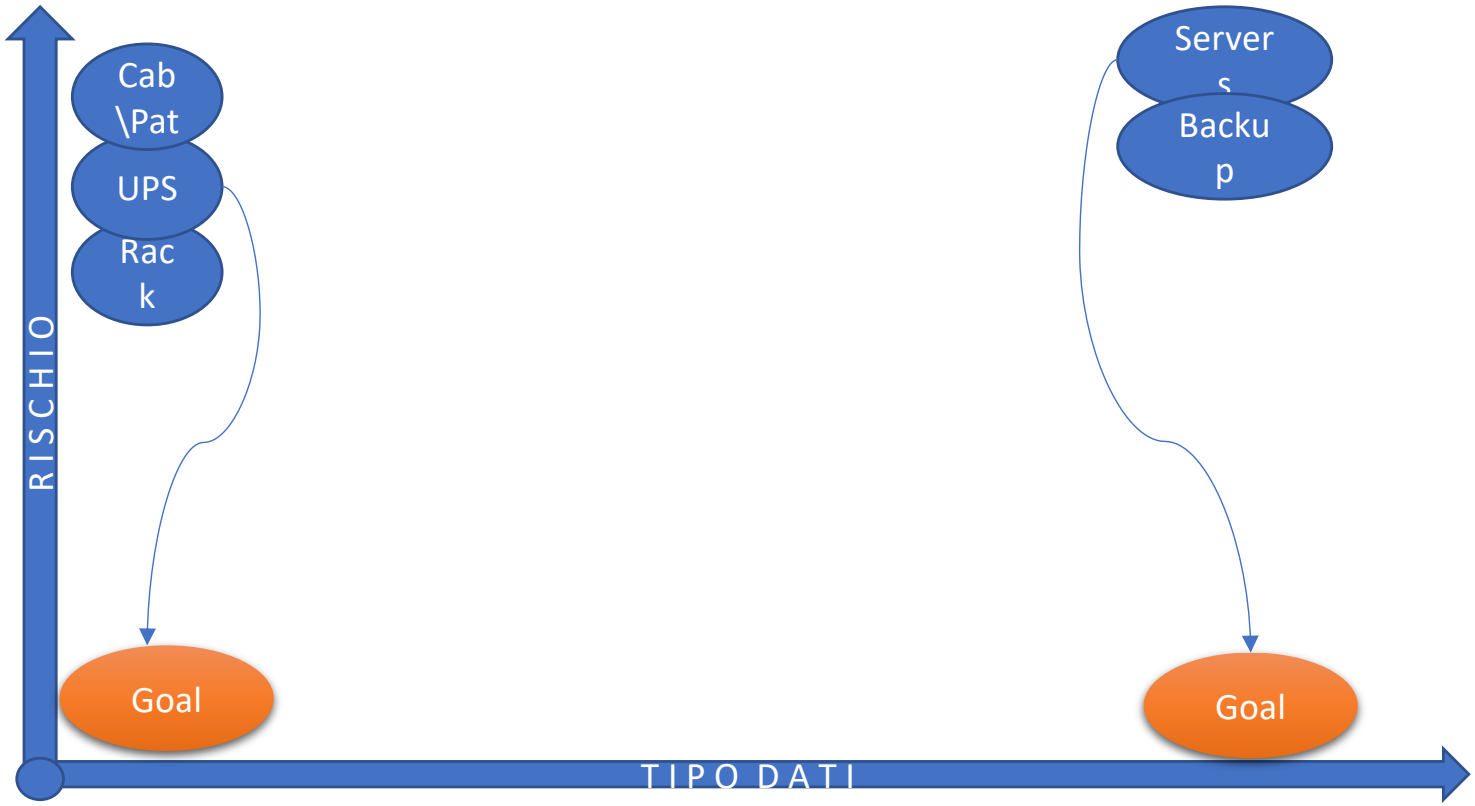

Gestione e Manutenzione
Struttura Logica
Active Directory – Domain Controller
Console WSUS
Console Antivirus Centralizzata
Log Server
Inventory System
Application
Networking
Router
Firewall
Switch L3
Switch L2
Proxy
Antispam
Infrastruttura
Rack
UPS
Cabling\Patching
Servers
Backup System
Gestione Rischi


Infrastruttura
Rack
UPS
Cabling\Patching
Servers
Backup System
Networking
Router
Firewall
Switch L3
Switch L2
Proxy
Antispam
Struttura Logica
Active Directory – Domain Controller
Console WSUS
Console Antivirus Centralizzata
Log Server
Inventory System
Aplicazioni
Gestione e Manutenzione
RISCHIO
TIPO DATI


RISCHIO
Infrastruttura
Rack
UPS
Cabling\Patching
Servers
Backup System
Networ
Router
Firewall
Switch L3
Switch L2
Proxy
Antispam
Struttura Logica
Active Directory – Domain Controller
Console WSUS
Console Antivirus Centralizzata
Log Server
Inventory System
Aplicazioni
Gestione e Manutenzione
TIPO DA

Infrastruttura

- Rack
- UPS
- Cabling\Patching
- Servers
- Backup System



Infrastruttura

- Rack
- UPS
- Cabling\Patching
- Servers
- Backup System

Il Rack deve essere posizionato in un ambiente non accessibile a persone non autorizzate

L'UPS deve essere Online ed avere una interfaccia di rete per il management

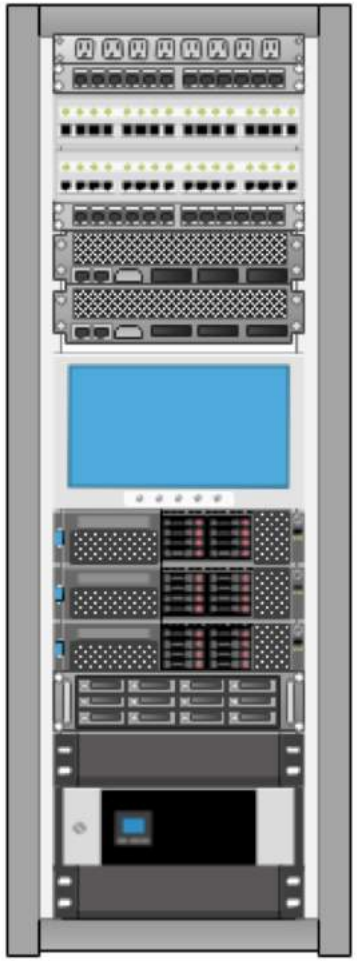
La permutazione passiva deve essere mappata in tutti I rack ed in un piano di permutazione documentato e legibile

I Servers devono essere in tecnologia raid [1,6,10 …] con sistemi di alimentazione ridondanti

Il Sistema di backup deve essere su rete distinta dalla LAN ed essere per I NAS in tecnologia RAID e per le tecnologie a nastro di tipo LTO

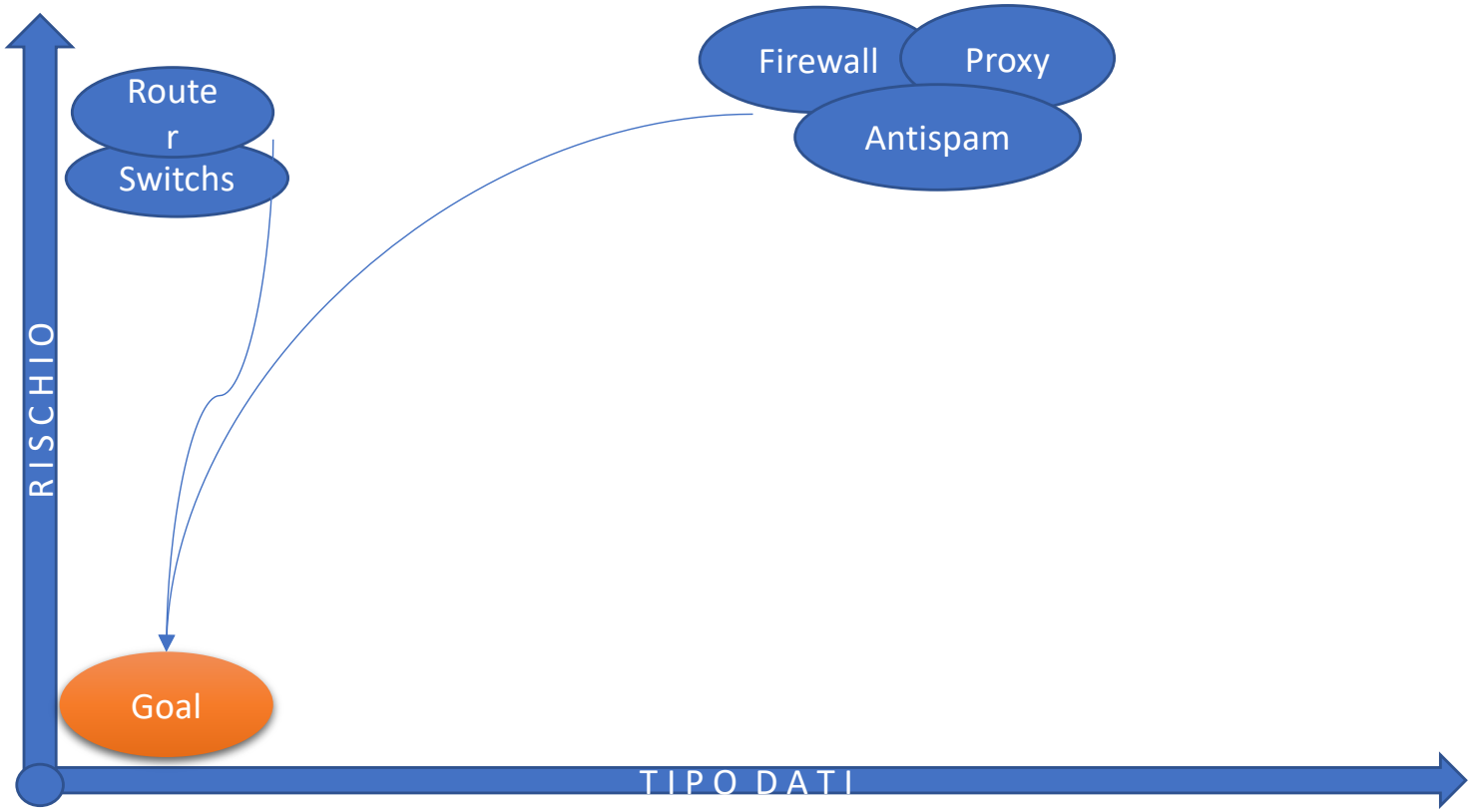
Il Rack deve essere posizionato in un ambiente non accessibile a persone non autorizzate

Tipica configurazione



Networking

- Router
- Firewall
- Switch L3
- Switch L2
- Proxy
- Antispam



Networking

- Router
- Firewall
- Switch L3
- Switch L2
- Proxy
- Antispam

IL Router se fornito dal Carrier deve essere configurato con NAT su IP. Se di proprietà è necessario disabilitare MGT remoto e L\P riservate e monitorate.

Il Firewall deve avere le funzionalità di: DDOS, IPS, IDS e network ispection. Deve essere accessibile al personale autorizzato una dashboard di analisi.

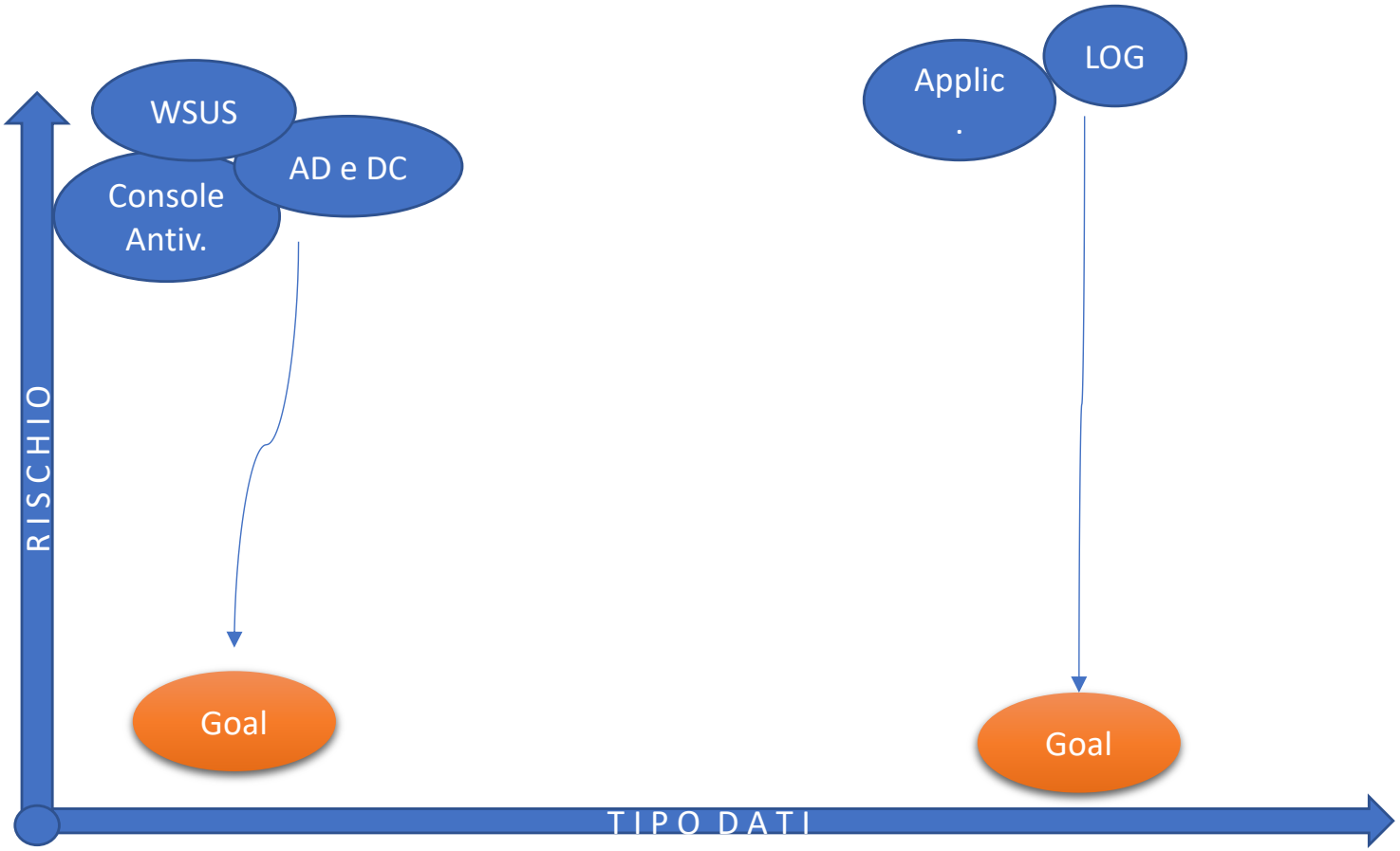
Lo switch centro stella deve avere funzionalità L3 al fine di poter effettuare routing over VLAN

Tutto il traffico web deve essere filtrato rispetto le blacklist più diffuse ed esseere configurato al fine di garantire solo la navigazione di pertinenza professionale ed eventualmente logistica del personale

Il traffico mail deve essere completamente scansionato in ingresso al fine di evitare problematiche di attacco generico e specifico verso utenze interne. Deve esistere una area di quarantena ed una di spam; il sistema di analisi dovrà avvertire l'utente che la mail è stata, eventualmente, eliminata e\o messe in area di quarantena.

Struttura Logica

- Active Directory – Domain Controller
- Console WSUS
- Console Antivirus Centralizzata
- Log Server
- Inventory System
- Applicazioni



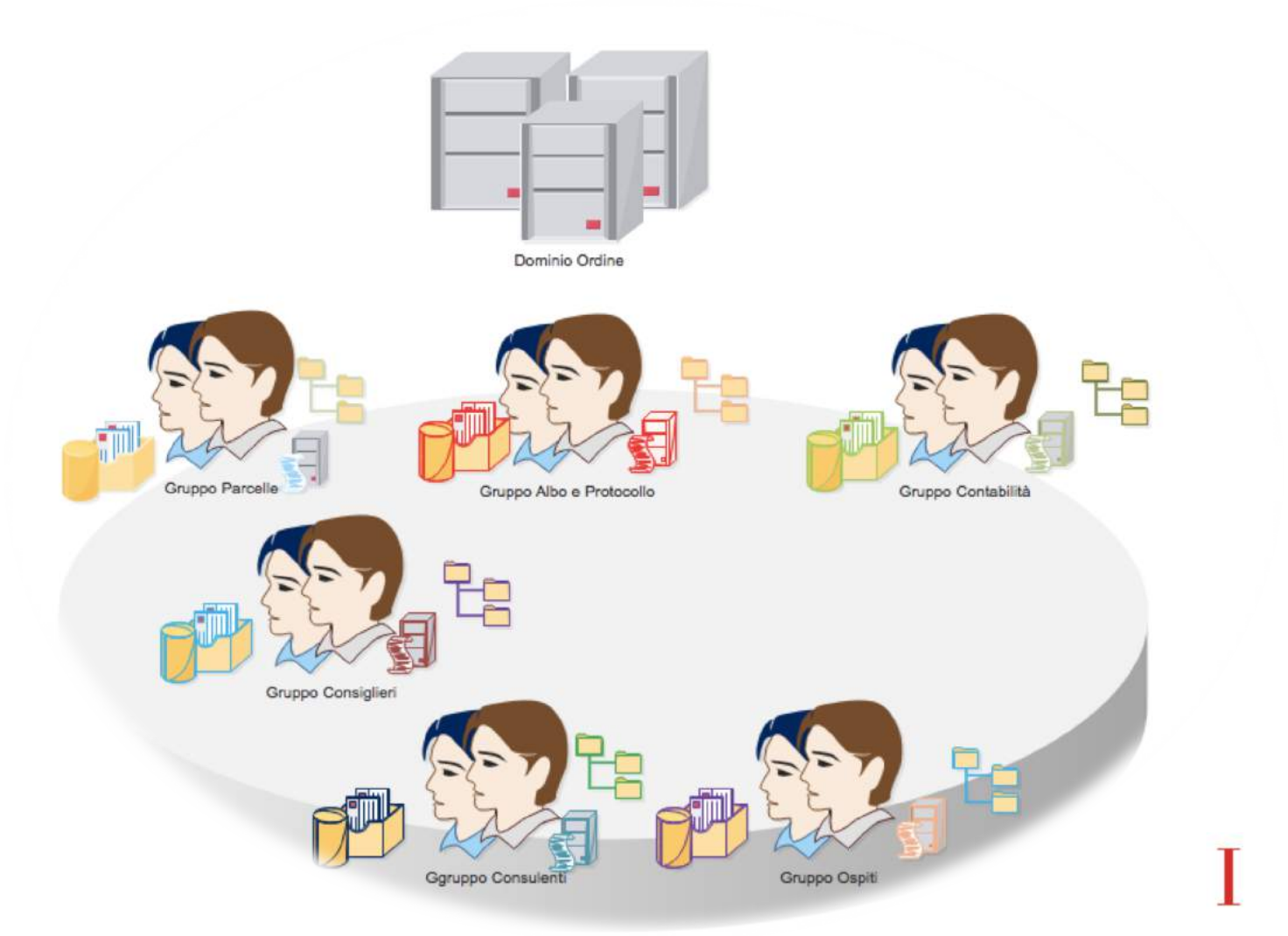
Struttura Logica

- Active Directory – Domain Controller
- Console WSUS
- Console Antivirus Centralizzata
- Log Server
- Inventory System
- Applicazioni

Deve essere attivato uno o piu server con funzionalità di Domain Controller al fine di effettuare una gestione puntuale di tutti gli accessi degli utenti secondo le indicazione dell'attuale allegato B DLgs 196\2003; in particolare le credenziali dovranno rispettare almeno questi criteri:

- Passwordcdi almeno 8 caratteri di cui Maius-Minus-Number-Spcial caracter e non essere ripetitive
- Password con max validità 90 giorni.
- Tutti I contenuti di sharing dovranno essere associati ad uno o più profili utente o Gruppo Utenti.
- Le policy di dominio dovranno non permettere installazioni di programmi se non ad utenti Domain Admin e preservare la configurazione standard dei O.S.
- …….

Deve essere attivita la funzionalità windows update server al fine di poter effettuare la validazione delle patch e delle fix dei sistemi esistenti considerando obligatorie sempre e comunque quelli di sicurezza. Dovrà esistere una daschboard di gestione dei sistemi di patching. I sistemi Linux devono essere costantemente monitorati rispetto ultime release e realtive patch e nuovi pacchetti di protezione.



CONSIGLIO NAZIONALE INGEGNERI

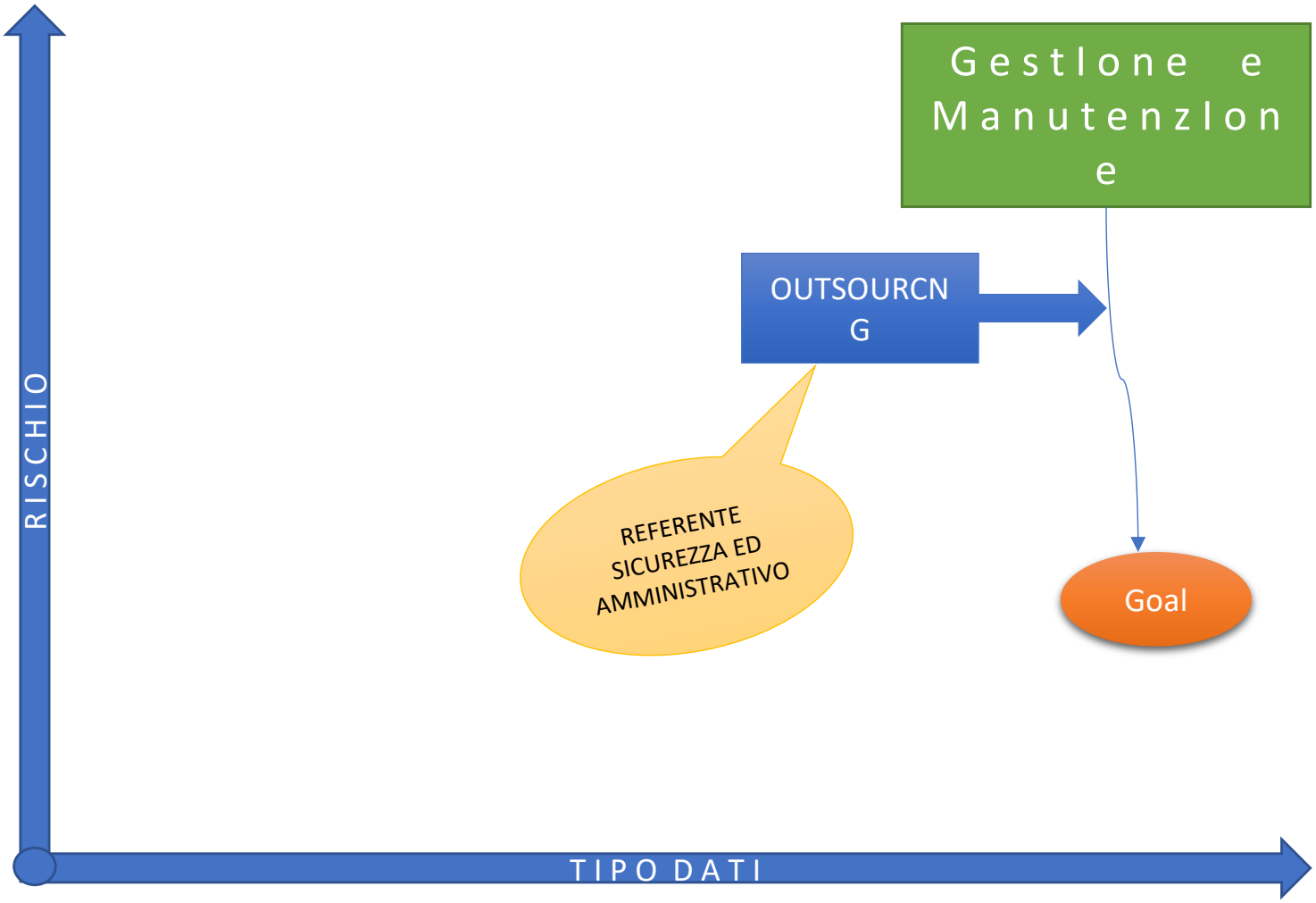
Deve essere attivata una console centralizzata di gestione antivirus che permetta la gestione delle applicazioni e delle periferiche al fine di effettuare sempre e comunque le seguenti azioni minime:

- Blocco dei driver di archiviaizone di massa (pendrive etc..) se non certificate ed autorizzate
- Scansione automatica dei file scaricati da internet o da mail
- Live protection attivato
- Sistemi di ispezione dei file e dei protocolli
- Verifica in tempo reale delle connessione aperte nella LAN
- Update automatico delle patch e fix centralizzato
- Log specifico e leggibile
- ……..

Devono essere attivite le funzionalità di log su tutti I servers possibilmente centralizzando tutto su un sistema di gestione dei log che permetta all'amminsitratore di sistema di poter intellegere tutte le attività

Devono essere presenti sistemi di inventario delle strutture LAN sia dal punto di vista hardware che software nonchè monitorare continuamente per identificare la presenza o meno di software non conosciuto o illegale.

Tutti le applicazioni devono poter\dover essere strutturate al fine di proteggere l'integrità del dato con una compliance almeno LDAP per le ACL. Inoltre le integrità dei data base e delle applicazioni devono essere garantite da opportune politiche di backup. Quando applicazione vengono esposte sul Web è necessario effettuare queste operaizoni rispettando le logiche DMZ ed in generale fare in modo da distinguere le zone di esposizione verso l'esterno da quelle di gestione interna. Qualora sia necessario una connessione esterna con la LAN interna per ragioni funzionali, sugli applicativi interni, è necessario abilitare connessioni VPN Lat to Host.


Gestlone e Manutenzlone
OUTSOURCNG
REFERENTE SICUREZZA ED AMMINISTRATIVO
Goal
RISCHIO
TIPO DATI

Art. 2.

Amministrazioni destinatarie

Destinatari della presente circolare sono i soggetti di cui all'art. 2, comma 2 del C.A.D.

Art. 3.

Attuazione delle misure minime

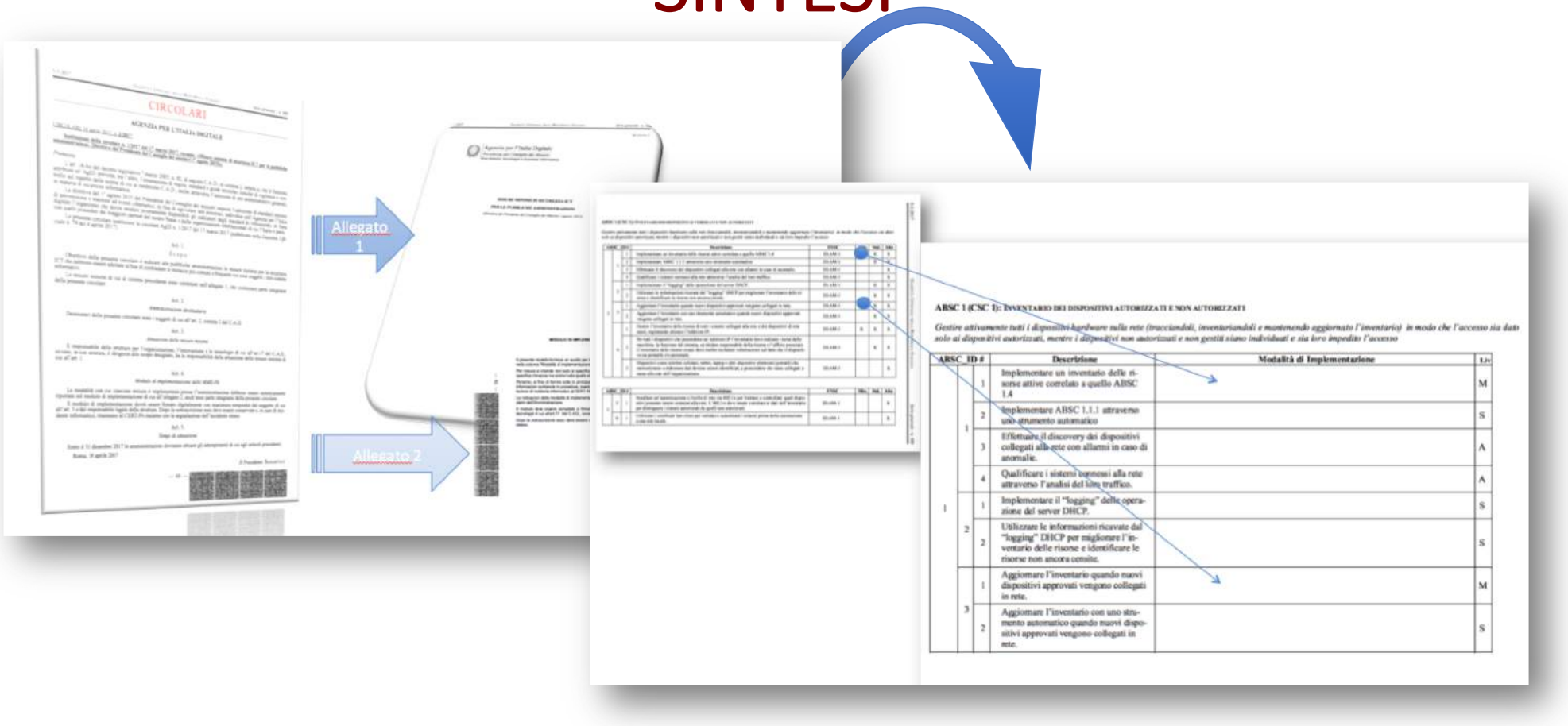
Il responsabile della struttura per l'organizzazione, l'innovazione e le tecnologie di cui all'art.17 del C.A.D., ovvero, in sua assenza, il dirigente allo scopo designato, ha la responsabilità della attuazione delle misure minime di cui all'art. 1.

Gestione e Manutenzione

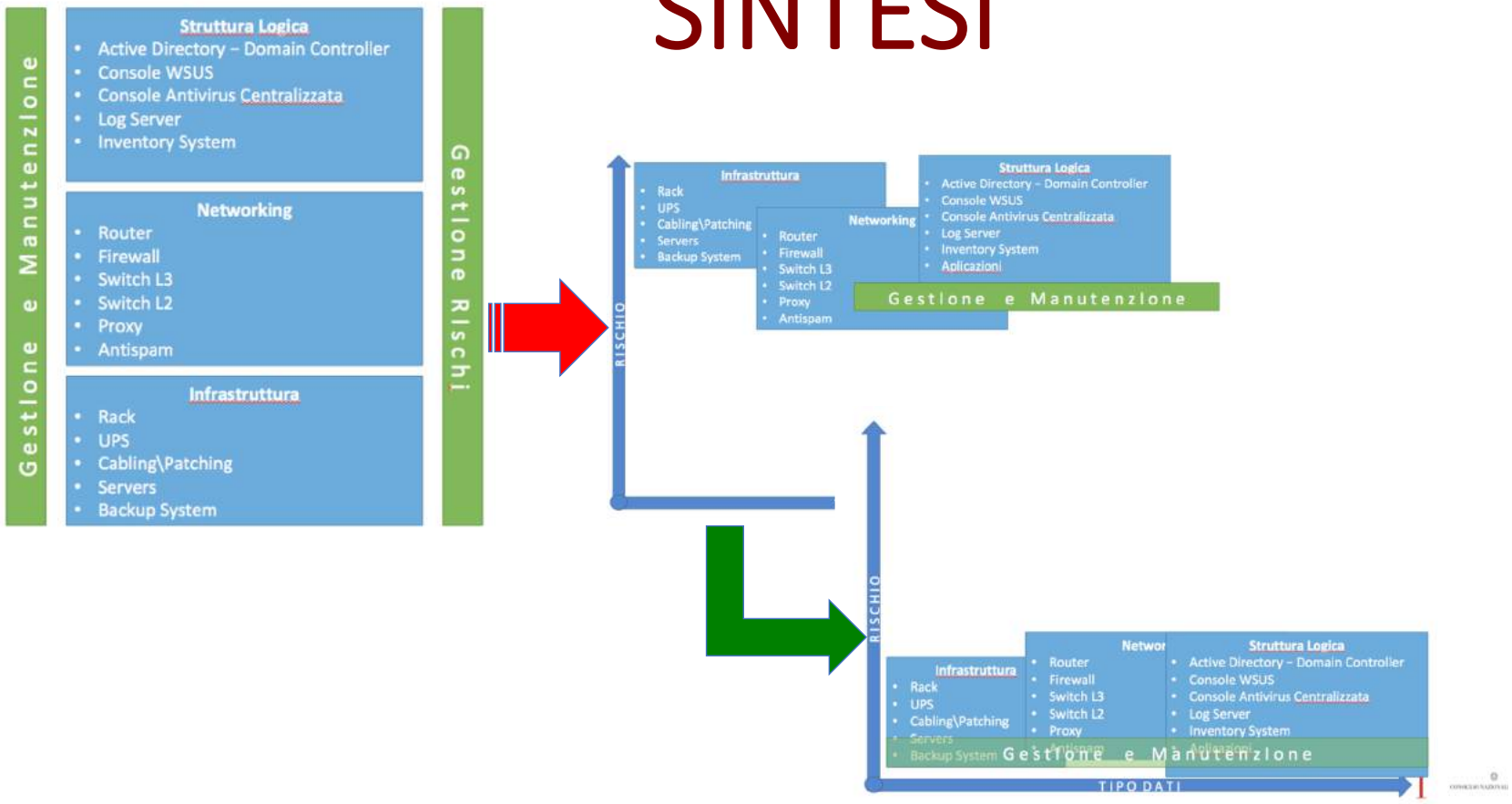
REFERENTE SICUREZZA ED AMMINISTRATIVO

SINTESI

SINTESI


CIRCOLARI
Allegato 1
Allegato 2
ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI
Gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso
ABSC_ID #
Descrizione
Modalità di Implementazione
Liv
1 1 1 Implementare un inventario delle risorse attive correlato a quello ABSC 1.4 M
1 1 2 Implementare ABSC 1.1.1 attraverso uno strumento automatico S
1 1 3 Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie. A
1 1 4 Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico. A
1 2 1 Implementare il "logging" delle operazione del server DHCP. S
1 2 2 Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite. S
1 3 1 Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete. M
1 3 2 Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete. S

SINTESI


Gestione e Manutenzione
Struttura Logica
Active Directory – Domain Controller
Console WSUS
Console Antivirus Centralizzata
Log Server
Inventory System
Networking
Router
Firewall
Switch L3
Switch L2
Proxy
Antispam
Infrastruttura
Rack
UPS
Cabling\Patching
Servers
Backup System
Gestione Rischi
RISCHIO
Aplicazioni
TIPO DATI

SINTESI

ABSC	ID #		Descrizione	FNSC	Mi	Ste	Alt
1	1	1	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	ID.AM-1	X	X	X
	3	1	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	ID.AM-1	X	X	X
	4	1	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	ID.AM-1	X	X	X

ABSC	ID #		Descrizione	FNSC	Mi	Ste	Alt
2	1	1	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di si- stema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'istallazione di software non compreso nell'elenco.	ID.AM-2	X	X	X
	3	1	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	ID.AM-2	X	X	X

ABSC	ID #		Descrizione	FNSC	Min	Ste	Alto
3	1	1	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	PR.IP-1	X	X	X
	2	1	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di si- stemi usati dall'organizzazione.	PR.IP-1	X	X	X
		2	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzan- do la configurazione standard.	PR.IP-2 RC.RP-1	X	X	X
	3	1	Le immagini d'installazione devono essere memorizzate offline.	PR.IP-2	X	X	X
	4	1	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).	PR.AC-3 PR.MA-2	X	X	X

SINTESI

ABSC	ID #		Descrizione	FNSC	Mi	St	Al
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 si- stema report con indicazioni delle vulnerabilità più critiche.	ID.RA-1 DE.CM-8	X	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

ABSC	ID #		Descrizione	FNSC	Mi	St	Al
4	5	1	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema opera- tivo 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
	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 ra- gionevole rischio.	PR.IP-12 RS.MI-3	X	X	X
	8	1	Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabi- lità , 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 ri- schio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.	PR.IP-12	X	X	X

SINTESI

ABSC	ID	#	Descrizione	FNSC	M	St	Alt
5	1	1	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	PR.AC-4 PR.PT-3	X	X	X
		2	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	PR.AC-4 PR.PT-3	X	X	X
	2	1	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	ID.AM-6 PR.AT-2 DE.CM-3	X	X	X
	3	1	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.	PR.IP-1	X	X	X

ABSC	ID	#	Descrizione	FNSC	M	St	Alt
5	7	1	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).	PR.AC-1 PR.AT-2	X	X	X
		3	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	PR.AC-1 PR.AT-2	X	X	X
		4	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	PR.AC-1	X	X	X
5	10	1	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministra- tori, alle quali debbono corrispondere credenziali diverse.	ID.AM-6	X	X	X
		2	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconduci- bili ad una sola persona.	ID.AM-6	X	X	X
		3	Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.	ID.AM-6 PR.AT-2	X	X	X
	11	1	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	PR.AC-1 PR.AT-2	X	X	X
		2	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	PR.AC-1 PR.AC-2	X	X	X

SINTESI

ABSC_ID #			Descrizione	FNSC	Min.	Std.	Alto
8	1	1	Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.	DE.CM-4 DE.CM-5	X	X	X
		2	Installare su tutti i dispositivi firewall ed IPS personali.	DE.CM-1	X	X	X
	3	1	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	PR.PT-3 DE.CM-7	X	X	X

ABSC_ID #			Descrizione	FNSC	Min.	Std.	Alto
8	7	1	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	PR.PT-2	X	X	X
		2	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	PR.AT-1 DE.CM-4	X	X	X
		3	Disattivare l'apertura automatica dei messaggi di posta elettronica.	PR.AT-1 DE.CM-4	X	X	X
		4	Disattivare l'anteprima automatica dei contenuti dei file.	PR.AT-1 DE.CM-4	X	X	X
	8	1	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	PR.PT-2 DE.CM-4	X	X	X
	9	1	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destina- tario, prevedendo anche l'impiego di strumenti antispam.	DE.CM-1 DE.CM-4	X	X	X
		2	Filtrare il contenuto del traffico web.	DE.CM-1 DE.CM-4	X	X	X
		3	Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente ne- cessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab).	DE.CM-1 DE.CM-4	X	X	X

SINTESI

ABSC_ID	#		Descrizione	FNSC		St	Alt
10	1	1	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni stretta- mente necessarie per il completo ripristino del sistema.	PR.IP-4	X	X	X
	3	1	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud. .	PR.DS-6	X	X	X
	4	1	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente ac- cessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.	PR.AC-2 PR.IP-4 PR.IP-5 PR.IP-9	X	X	X

ABSC_ID	#		Descrizione	FNSC	Min.	Std.	Alto
13	1	1	Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica	ID.AM-5	X	X	X
	8	1	Bloccare il traffico da e verso url presenti in una blacklist.	ID.-AM3 PR.DS-5 DE.CM-1	X	X	X

Criteri di valutazione

Criteri generali hardware	Rischio
• data acquisto minore di 3 anni	medio basso
• data acquisto maggiore di 3 anni	medio alto
• manutenzione attiva	medio basso
• manuntezione non attiva	medio ato
• gestione attiva	basso
• gestione non attiva	alto

Criteri generali dati	Rischio
• dati anagrafici pubblici	medio basso
• dati anagrafici non pubblici	medio
• dati contabili interni	medio
• dati giuridici	medio alto
• dati sanitari	medio alto
• dati marketing	medio
• dati strategici	medio

Criteri generali software\applicazione	Rischio
data acquisto minore di 3 anni	medio basso
data acquisto maggiore di 3 anni	medio alto
manutenzione attiva	medio basso
manuntezione non attiva	medio ato
gestione attiva	basso
gestione non attiva	alto
tecnologia base dati obsoleta	medio alto
tecnoloiga base dati non obsoleta	medio basso
tecnologia applicazione obsoleta	medio
tecnologia applicazione non obsoleta	basso
documentazione tecnica e manualistica utente presente	basso
documentazione tecnica e manualistica utente non presente	alto
politica di backup presente	basso
politica di backup non presente	alto

Applicazione

- data base: tecnologia e tipologia
- acl data base
- applicazione: tecnologia e tipolgia
- acl applicazione
- tipo di dati trattati
- processo di appartenenza
- personale interno coinvolto
- personale esterno coinvolto
- interazione utenza
- manutenzione attiva
- manutenzione non attiva
- gestione attiva
- gestione non attiva
- numero licenza
- validità licenza: da data a data
- identificazione puntuale delle installazioni

- identificazione dei server di pertinenza

Backup

elenco path in backup

- frequenza
- tempo di mantenimento
- localizzazione backup a caldo
- localizzazione backup a freddo
- frequenza
- tempo di mantenimento

elenco data base e applicazioni in backup

- frequenza
- tempo di mantenimento
- localizzazione backup a caldo
- localizzazione backup a freddo
- frequenza
- tempo di mantenimento

elenco snapshot effettuati e in backup

- localizzazione
- frequenza
- tempo di mantenimento
- localizzazione backup a caldo
- localizzazione backup a freddo

Priorità e passi operativi

- Creare organigramma funzionale nell'Ordine di riferimento
- Designare il responsabile del sistema informatico
- Designare l'amministratore di sistema
- Designare il responsabile dei dati e gli incaricati
- Designare il DPO e comunicarlo al Garante
- Identificare la tipologia di dati trattati
- Acquisire le informative dagli associati al trattamento dei dati per le finalità precipue
- Acquisire le informative dagli associati al trattamento dei dati per finalità diverse da quelle istituzionali
- Acquisire il consenso al trattamento dei dati da parte dei dipendenti, dei collaboratori e dei fornitori
- Formazione strutturata per dipendenti e collaboratori
- Definire il registro del trattamento dei dati
- Impostare il piano di gestione del rischio associato al trattamento dei dati
- Manutenere con frequenza almeno trimestrale quanto sopra elencato

Modello di comunicazione al Garante per la designazione del DPO

- Facsimile

Software per la compilazione del Privacy Impact Assessment [PIA]

Software Download

Registro Trattamenti

Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:						
l nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati	le finalità del trattamento	una descrizione delle categorie di interessati e delle categorie di dati personali	le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali	ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate	ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati	ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1. 2.

Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente			
il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;	le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento	ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate	ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.