CONSIGLIO NAZIONALE INGEGNERI

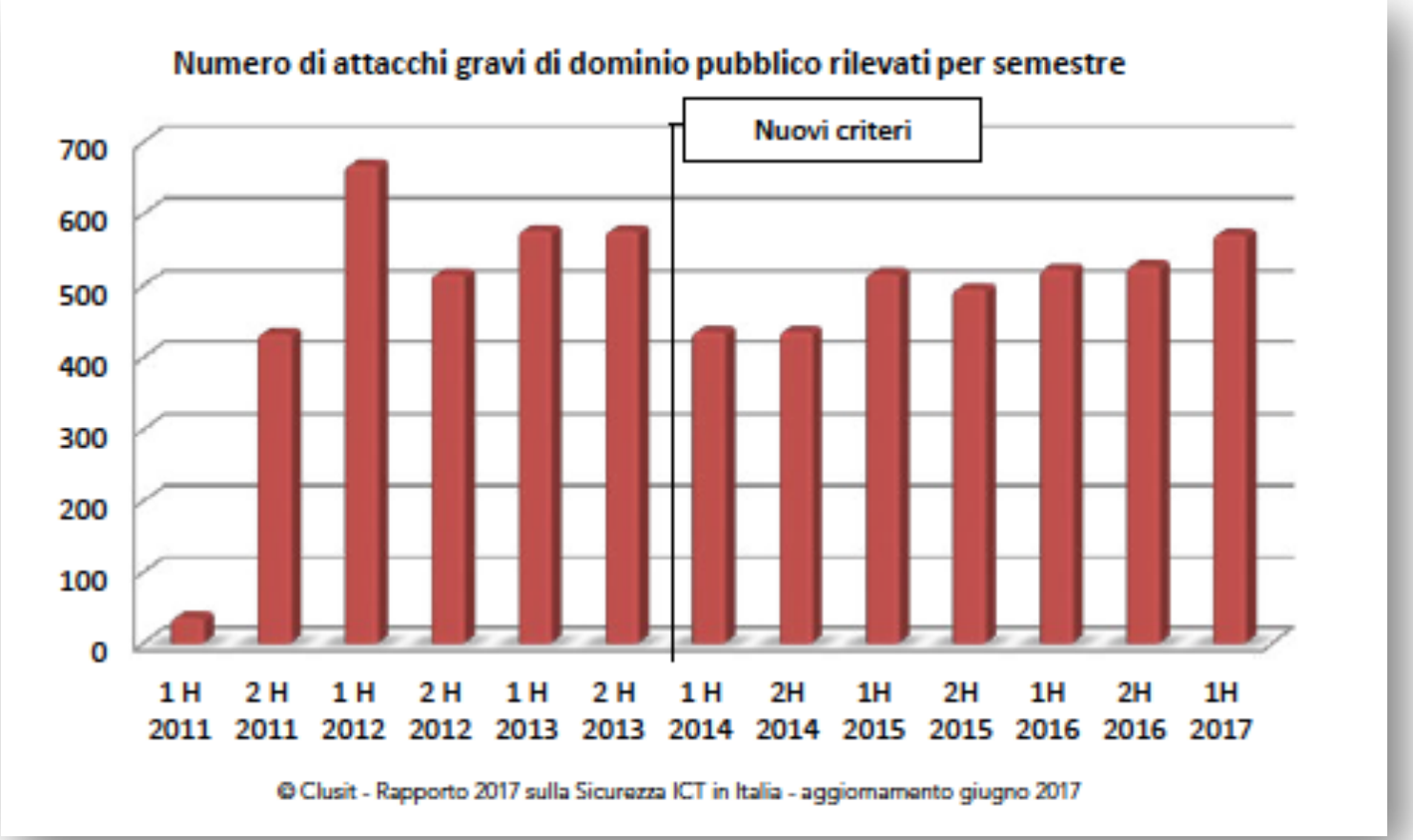
# Adempimenti in materia di sicurezza informatica: Misure minime di sicurezza ICT per le pubbliche amministrazioni.

## Circolare Agid n°2 del 18 Aprile 2017

Ing Biagio Garofalo
direzionetecnica@cni-online.it
14 dicembre 2017
CNI – Sala Conferenze

CONSIGLIO NAZIONALE INGEGNERI

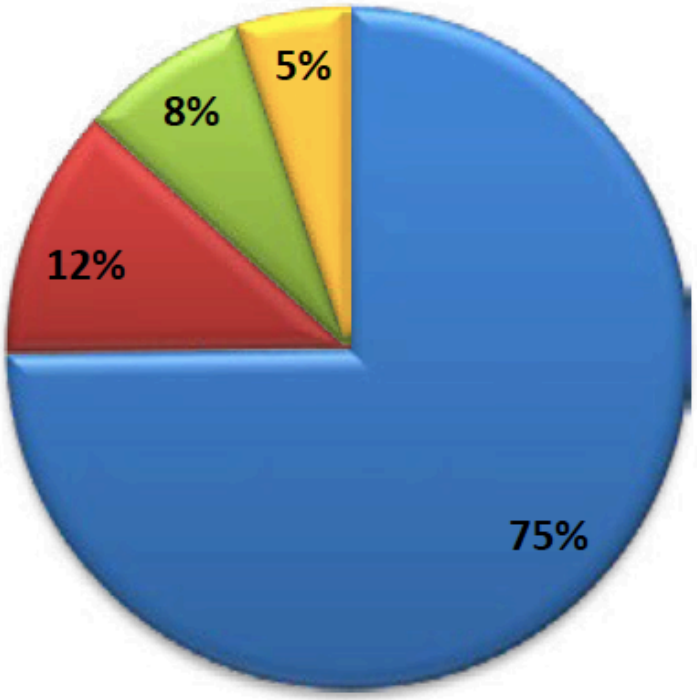

dreambox
support
juantech
password
123456
/bin/busybox
54321
ubnt
system
root
7ujMko0admin
user
vizxv
default
admin
system\x00
1234
888888
pass
xc3511
guest
12345
sh\x00
1111
666666
anko
xmhdipc
admin1
23 root
webmaster
redmine
admin
nagios
Admin\x00
service
888888
thomas
ubnt
Administrator
support
666666
shell\x00
user
minecraft
mother
enable\x00
test
ts3
bin
backup
tech
enable
root
root\x00
pi
ftpuser
sh
mysql
default
ftp
oracle
23 admin
cisco
administrator
guest
sh\x00
git
usuario
supervisor
Admin
vnc
teamspeak
postgres
apache
7up -r 7up -g 93.190.142.201;chmod


Numero di attacchi gravi di dominio pubblico rilevati per semestre
Nuovi criteri
700
600
500
400
300
200
100
0
1 H 2011
2 H 2011
1 H 2012
2 H 2012
1 H 2013
2 H 2013
1 H 2014
2H 2014
1H 2015
2H 2015
1H 2016
2H 2016
1H 2017
© Clusit - Rapporto 2017 sulla Sicurezza ICT in Italia - aggiornamento giugno 2017

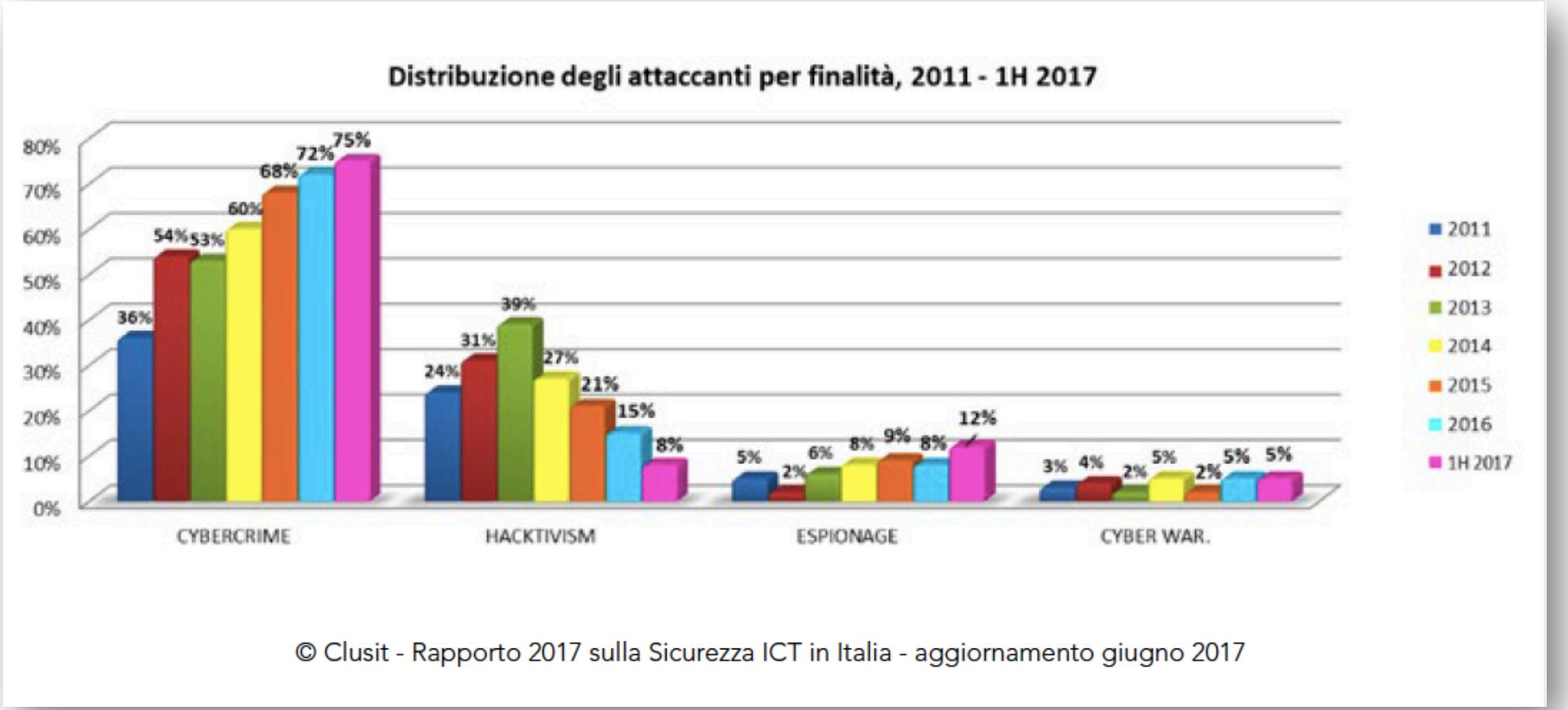
## Distribuzione degli attaccanti per tipologia e trend evolutivi

| 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% | ↗ |

## Tipologia e distribuzione degli attaccanti - 1H 2017

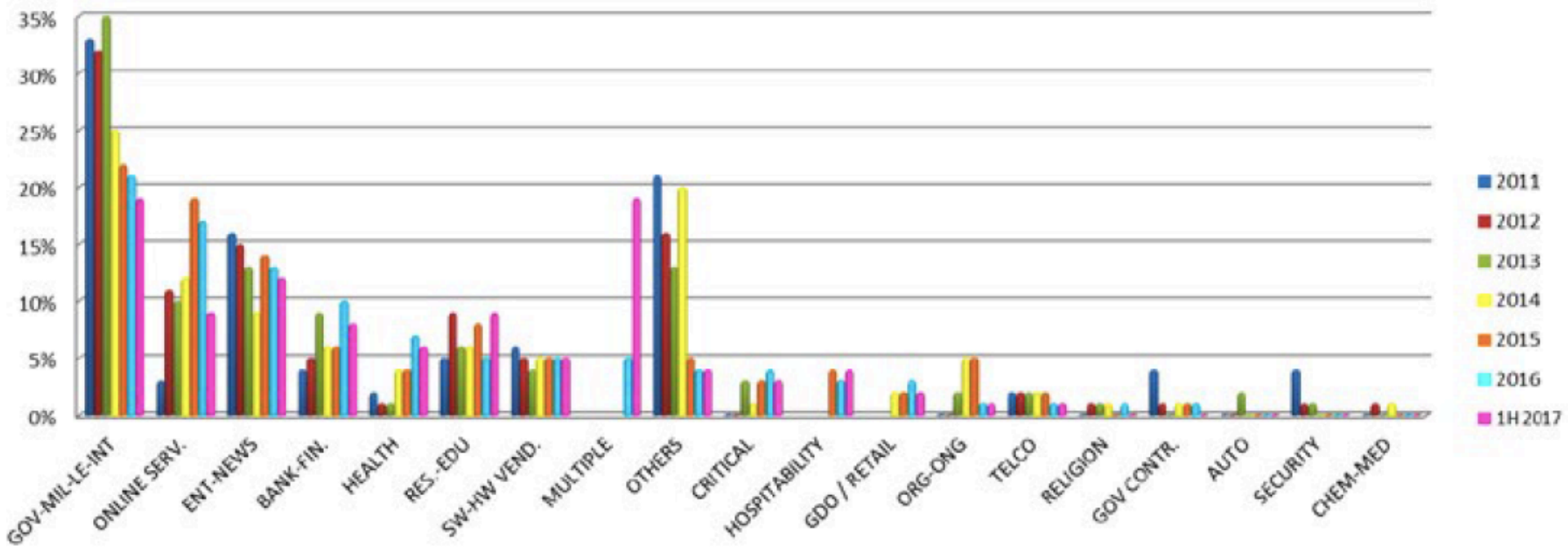



© Clusit - Rapporto 2017 sulla Sicurezza ICT in Italia - aggiornamento giugno 2017




© 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



FIGURA 3 – Rischio di minacce in aumento

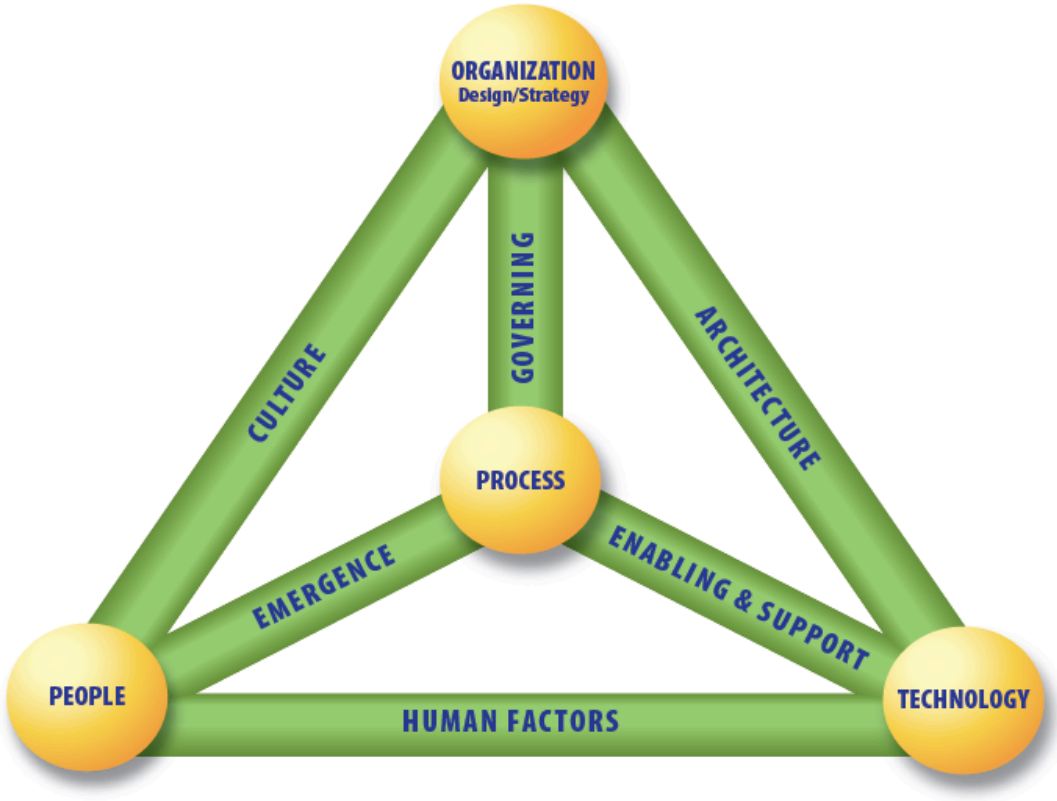



AFCEA - Ebook Cyber Security
https://www.afcea.org

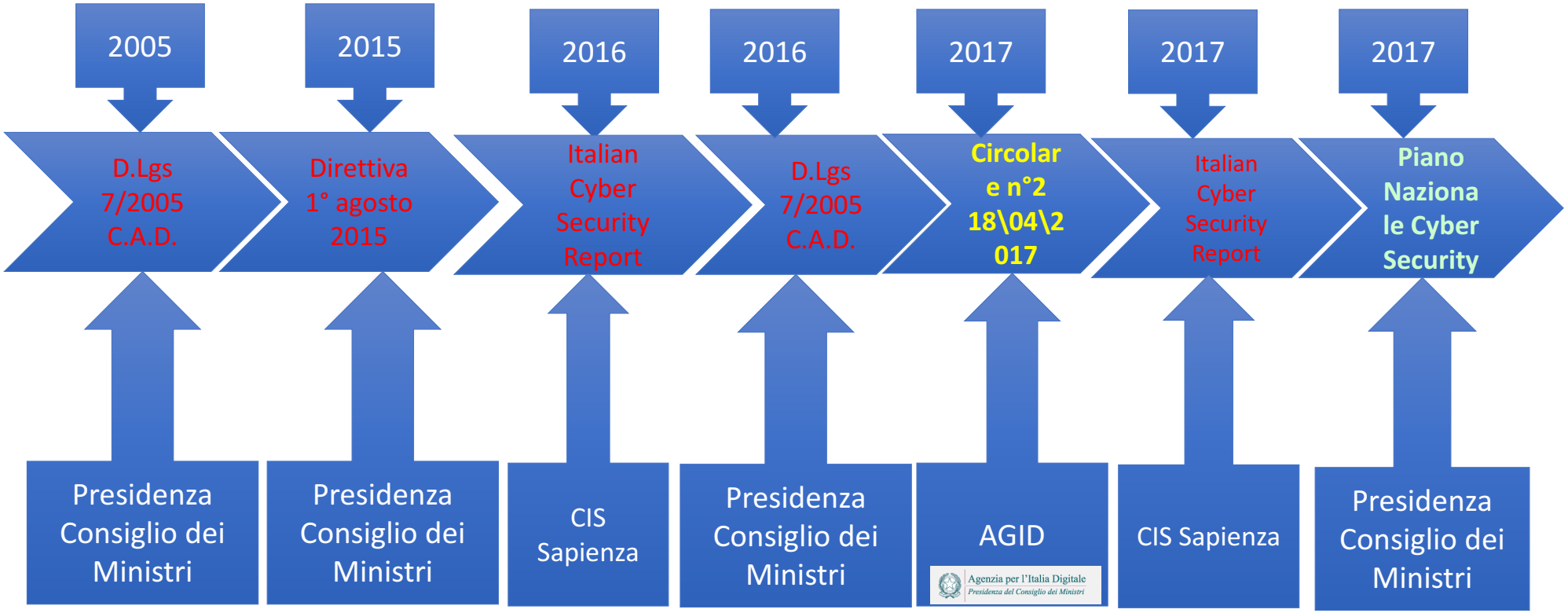
ISACA®

https://www.isaca.org

# Business Model for Information Security




CONSIGLIO NAZIONALE INGEGNERI


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 7/2005 C.A.D.
Presidenza Consiglio dei Ministri
2017
Circolare n°2 18\04\2017
AGID
Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri
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…….



# 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:

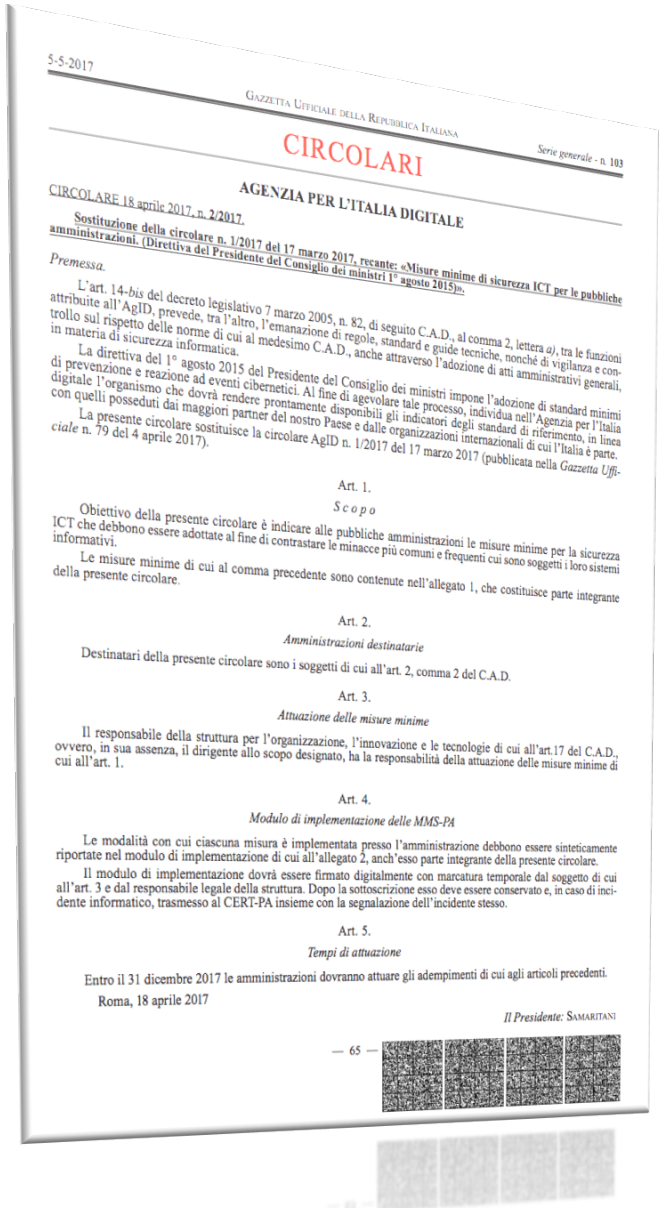
- il potenziamento delle capacità di difesa delle infrastrutture critiche nazionali e degli attori di rilevanza strategica per il sistema Paese;
- il miglioramento delle capacità tecnologiche, operative e di analisi degli attori istituzionali interessati;
- l'incentivazione della cooperazione tra istituzioni 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.

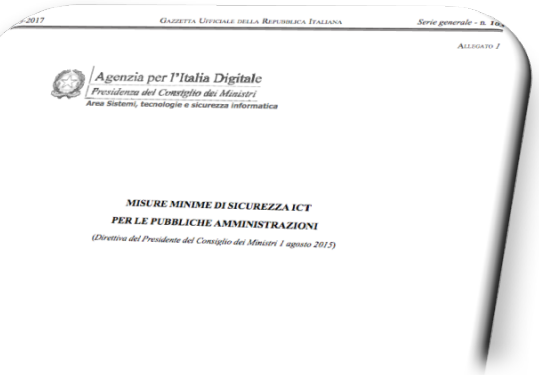
Roma, 18 aprile 2017

*Il Presidente:* SAMARITANI

— 65 —

Allegato 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 alle singole 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 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.



ALLEGATO

CONSIGLIO NAZIONALE INGEGNERI

# 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.

*S c o p o*

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*

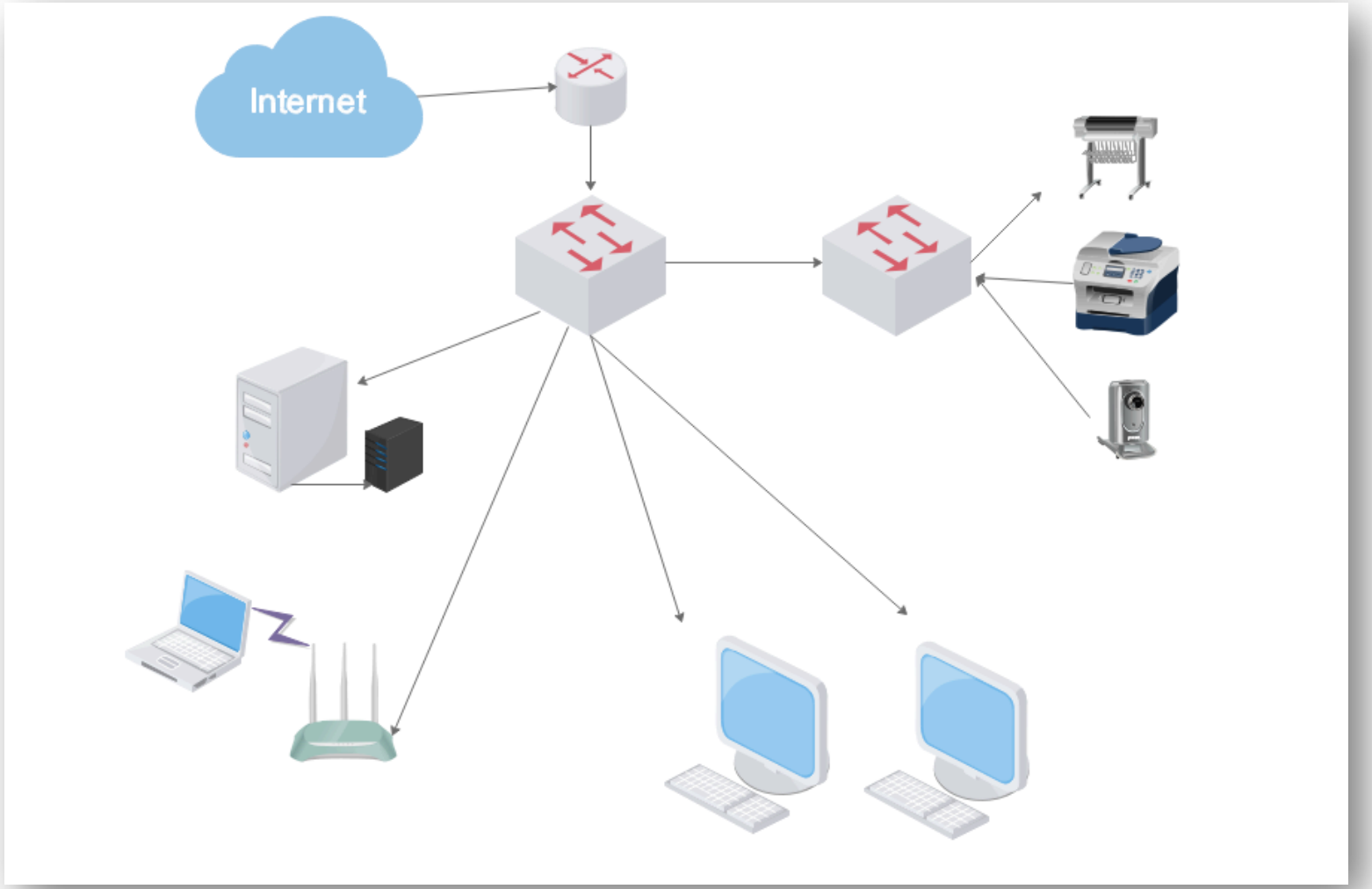
| ABSC_ID # | | | Descrizione | Modalità di Implementazione | Liv |
|---|---|---|---|---|---|
| 1 | 1 | 1 | Implementare un inventario delle risorse attive correlato a quello ABSC 1.4 | | M |
| | | 2 | Implementare ABSC 1.1.1 attraverso uno strumento automatico | | S |
| | | 3 | Effettuare il discovery 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 |

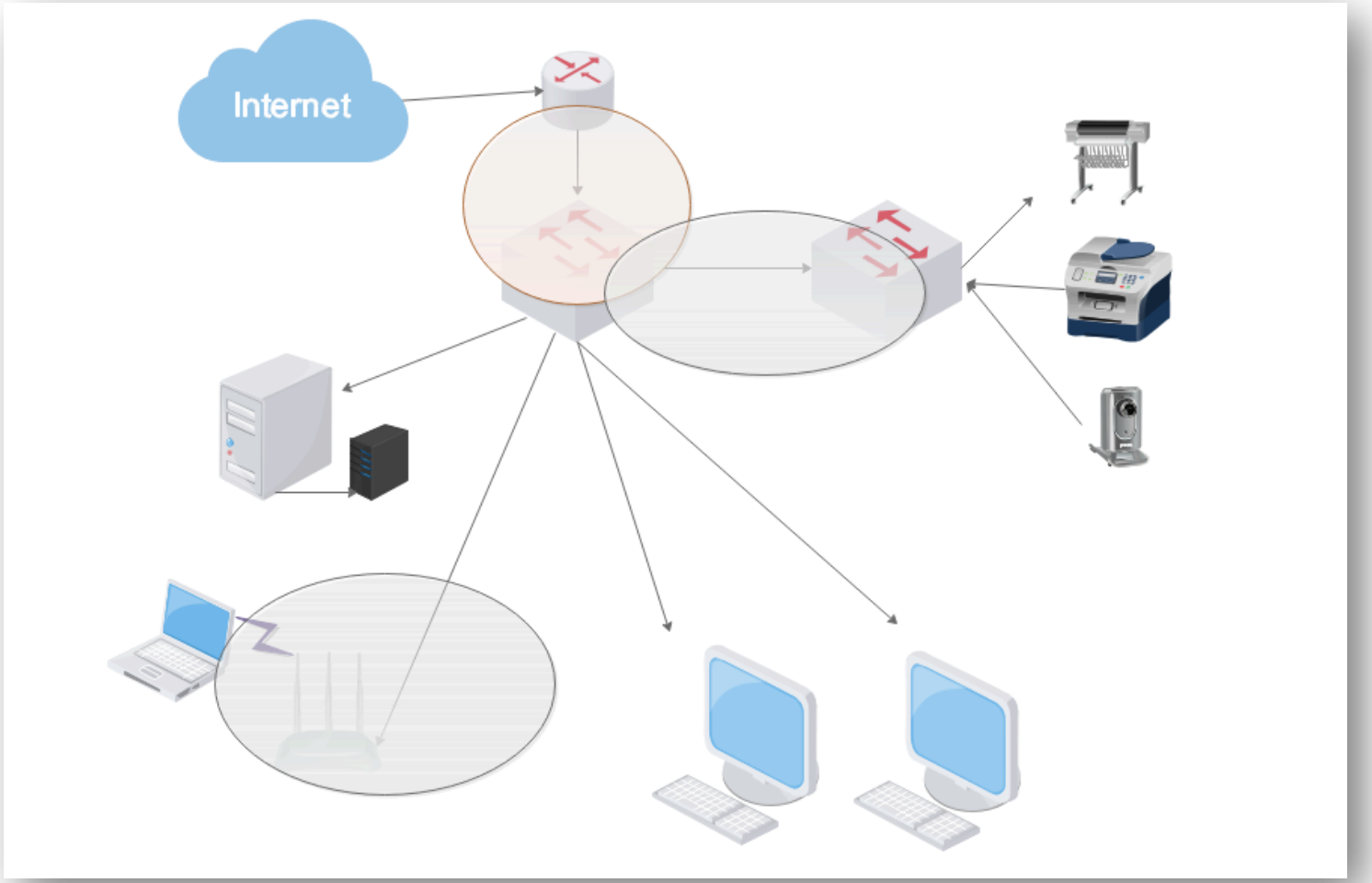
5-5-2017 GAZZETTA UFFICIALE DELLA REPUBBLICA ITALIANA Serie generale - n. 103

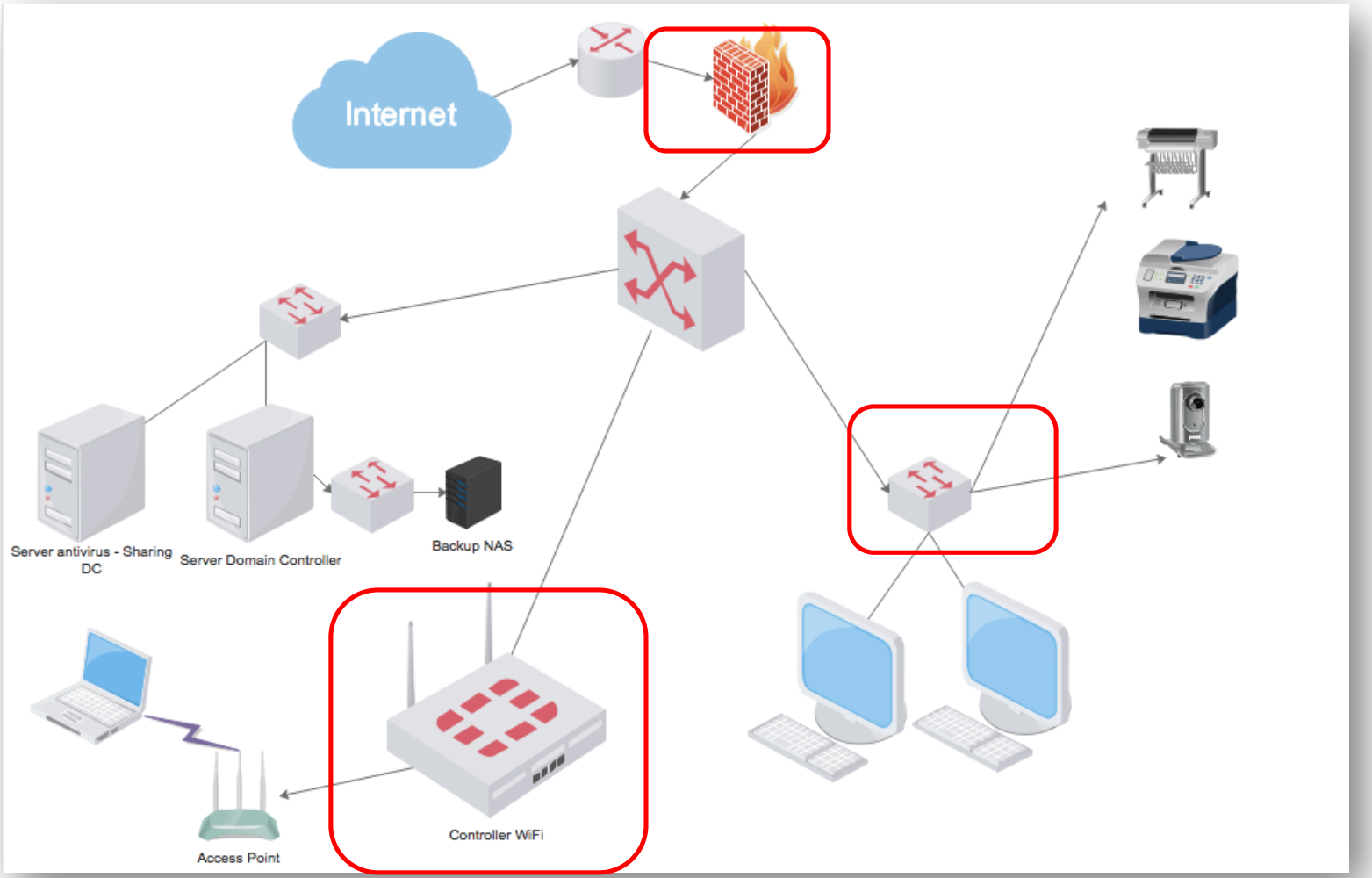
# *Riferimenti*

- 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/

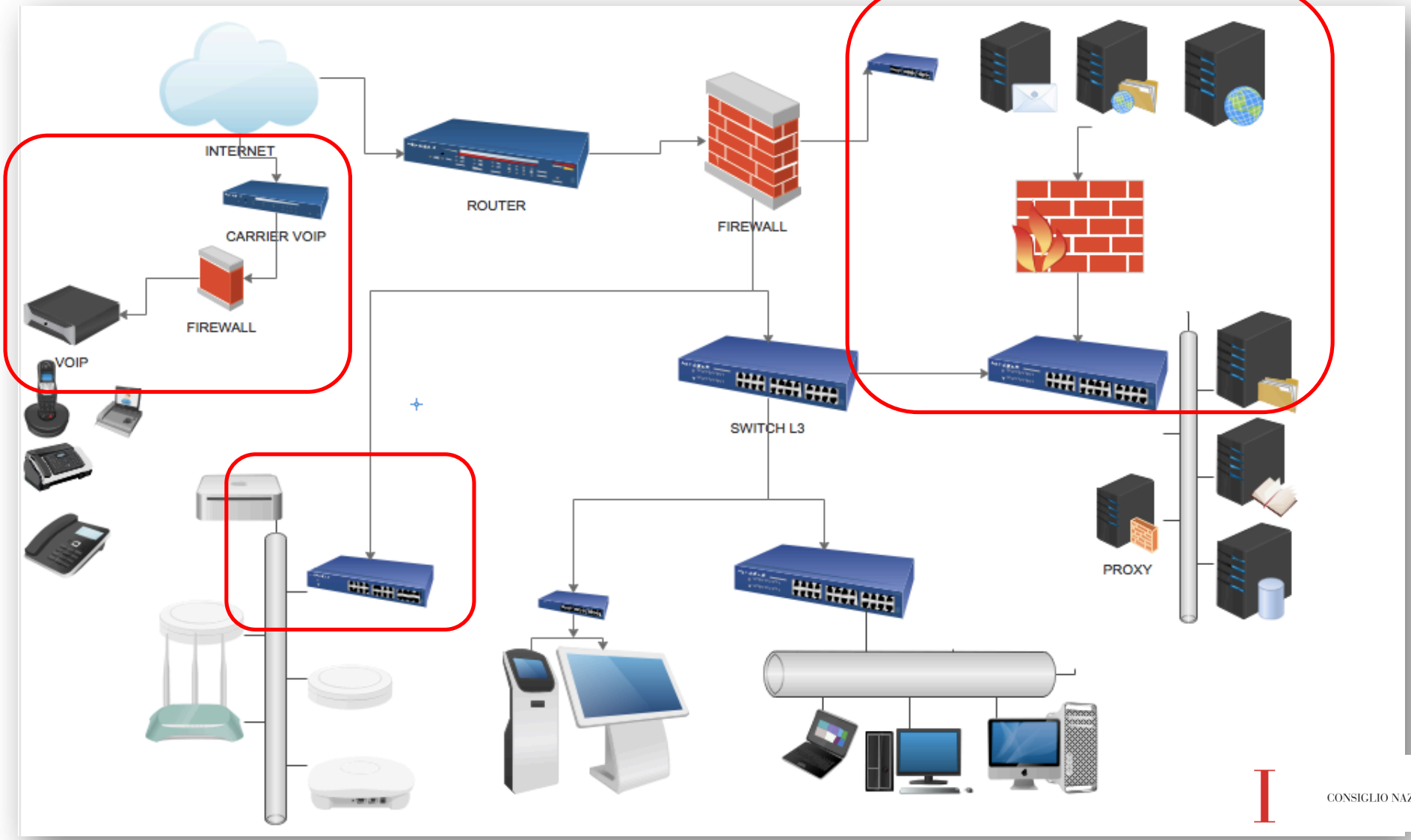
# action


Internet

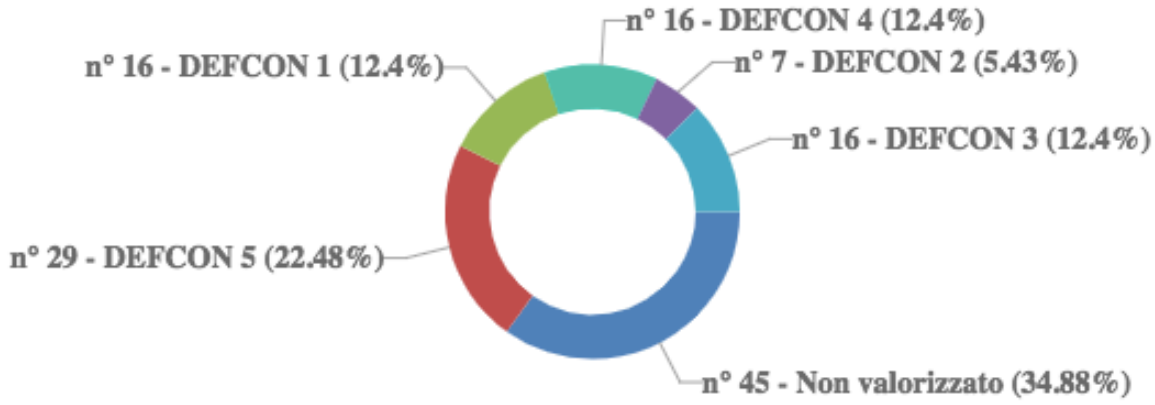

Internet


Internet
Server antivirus - Sharing DC
Server Domain Controller
Backup NAS
Controller WiFi
Access Point

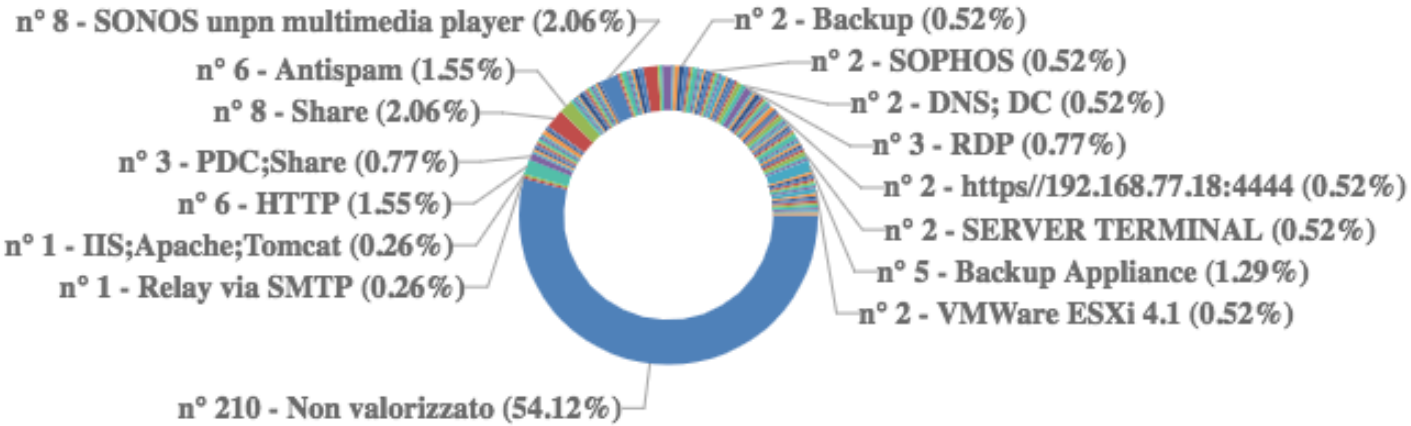
# SISTEMI PIU’ COMPLESSI


INTERNET
ROUTER
FIREWALL
CARRIER VOIP
FIREWALL
VOIP
SWITCH L3
PROXY

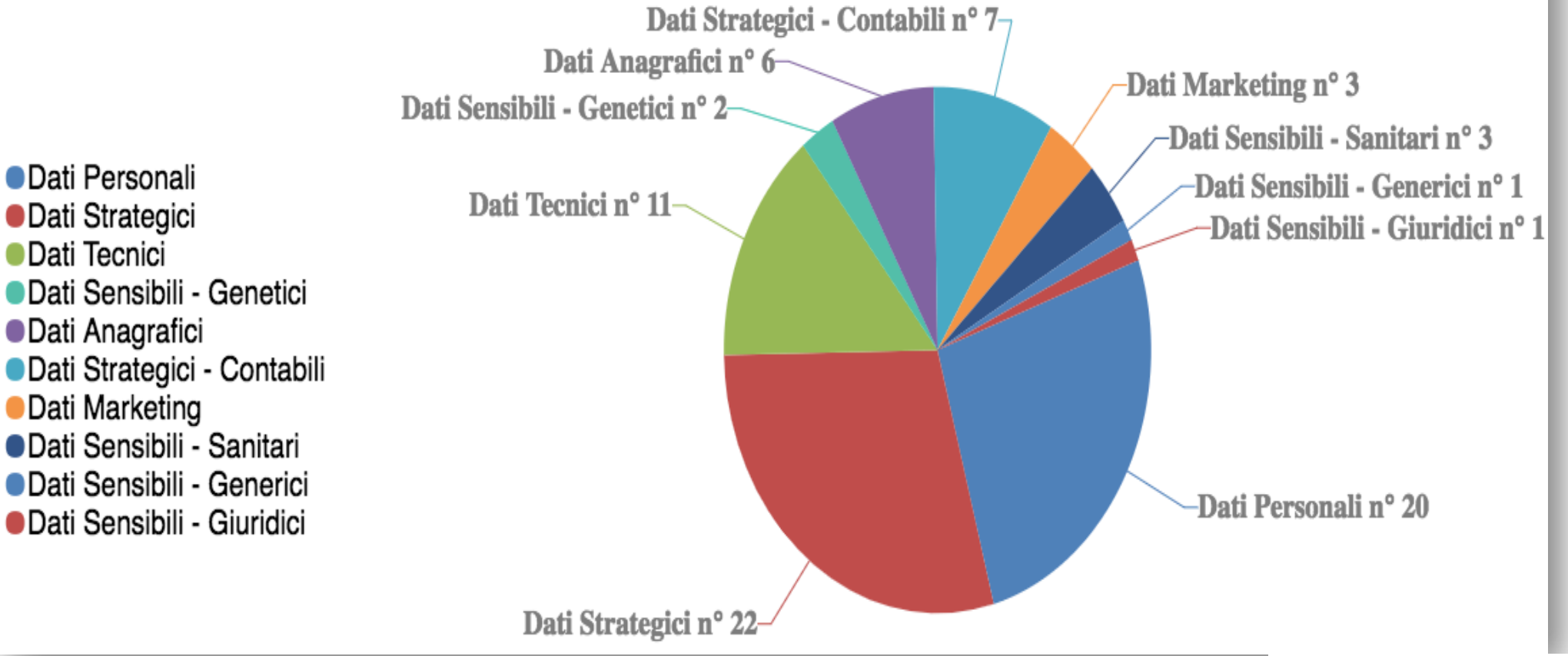
## Customer Scores ( --- )




## Customer services ( --- )



# Customer Data types



# Elementi necessari per adempiere ai requisiti minimi e in alcuni casi standard

Gestione e Manutenzione

**Struttura Logica**

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

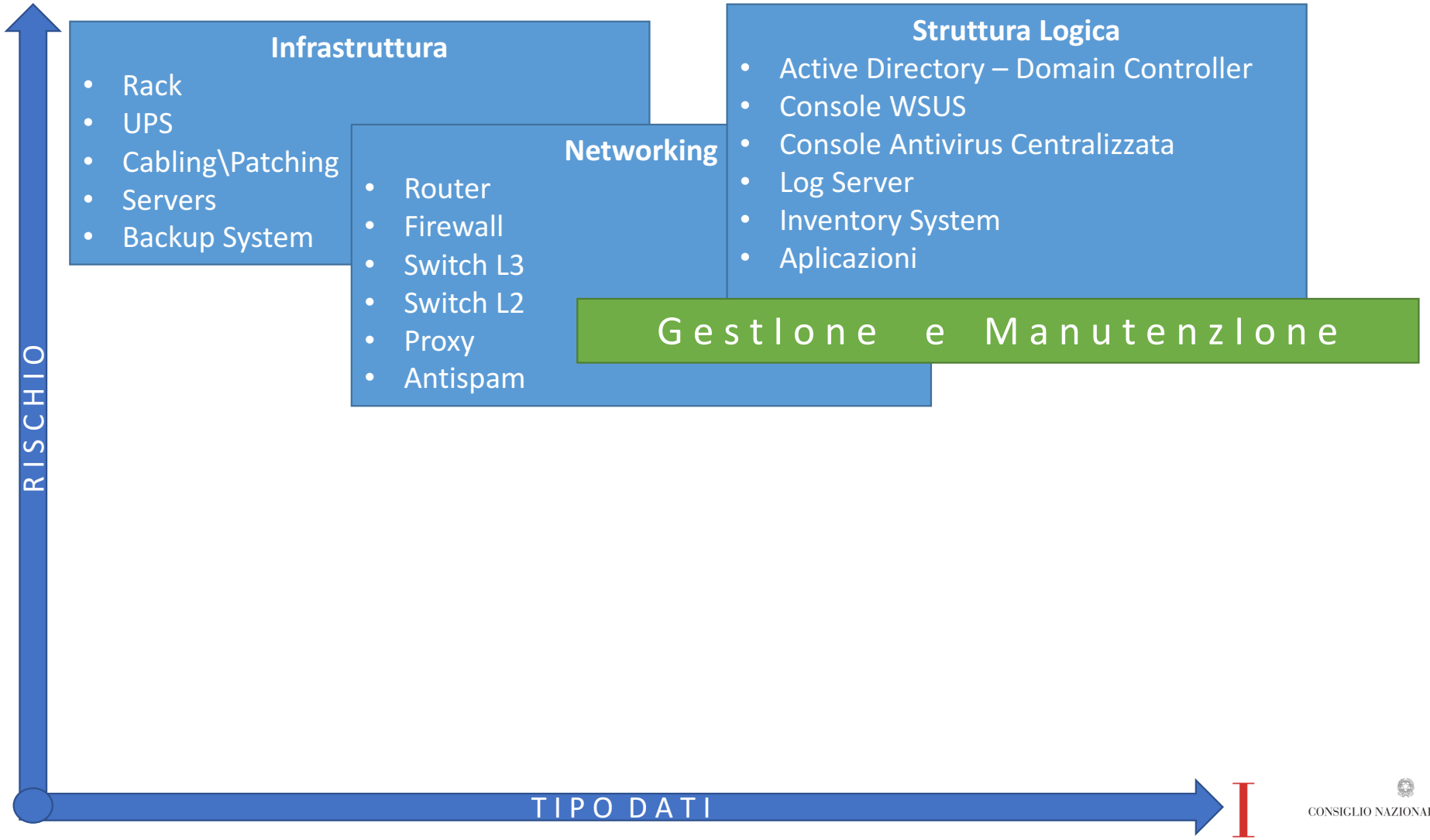
**Networking**

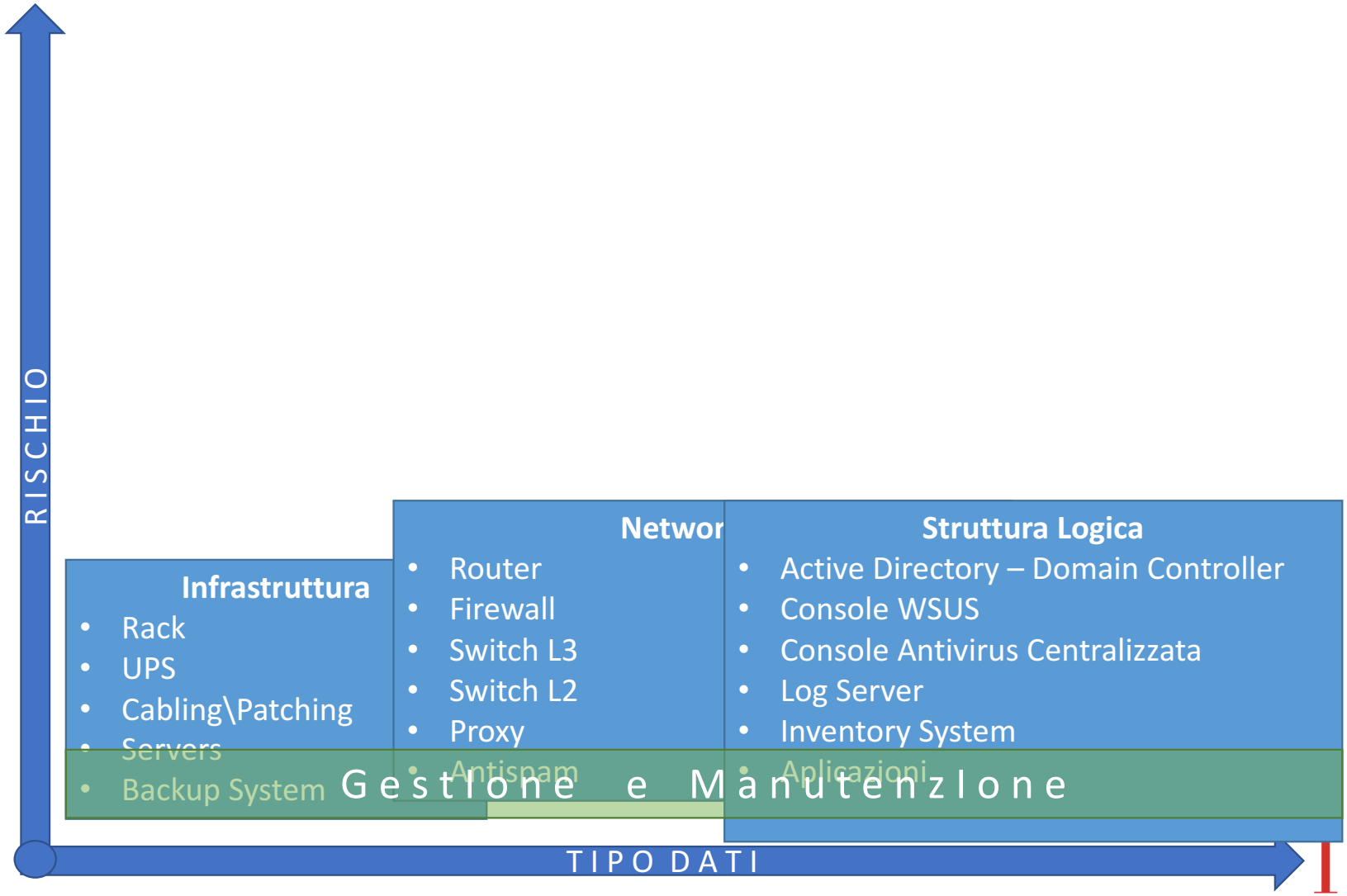
- Router
- Firewall
- Switch L3
- Switch L2
- Proxy
- Antispam

**Infrastruttura**

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

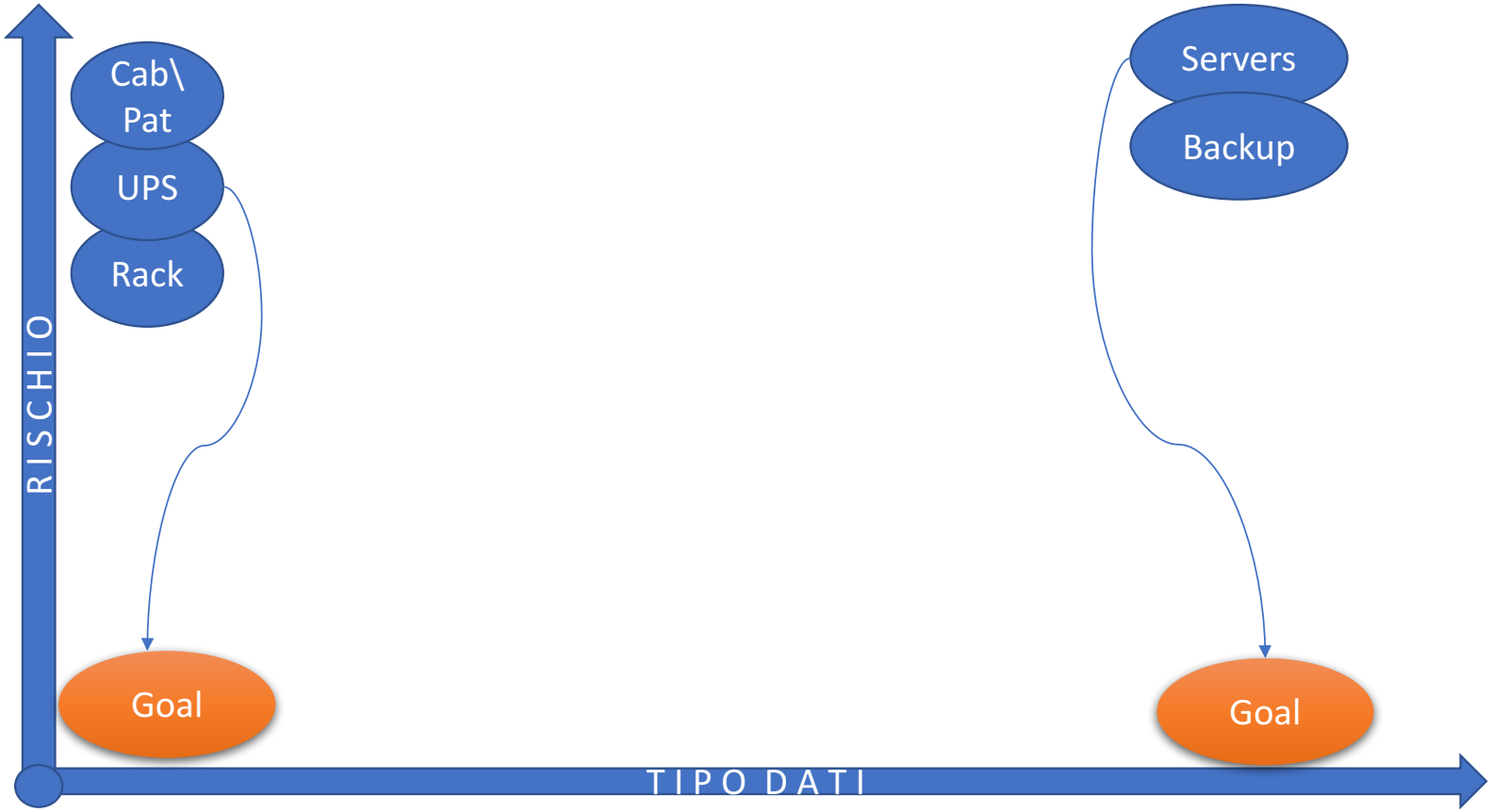
Gestione Rischi


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
Applicazioni
Gestione e Manutenzione
TIPO DATI

**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

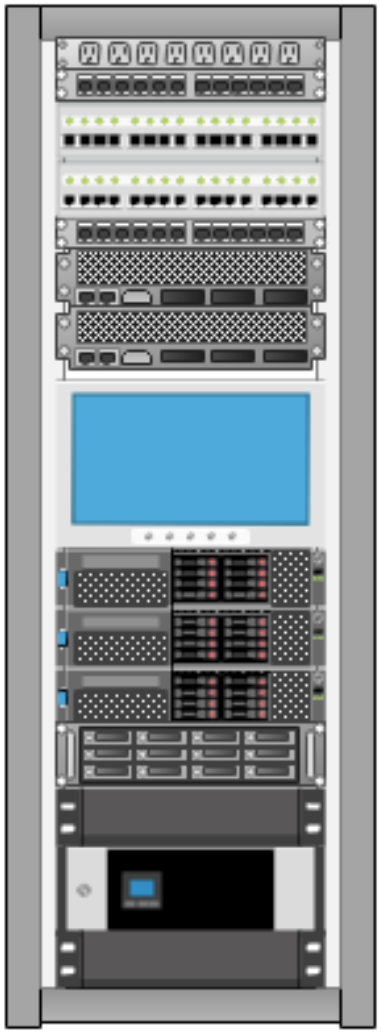
La permutazione passiva deve essere mappata in tutti I rack ed in un piano di permutazione documentato e legibile

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



Power Strip
Patch Panel

Patch Panel

Router

Firewall

Domain Controller

Console Antivirus e files Sharinf -DC

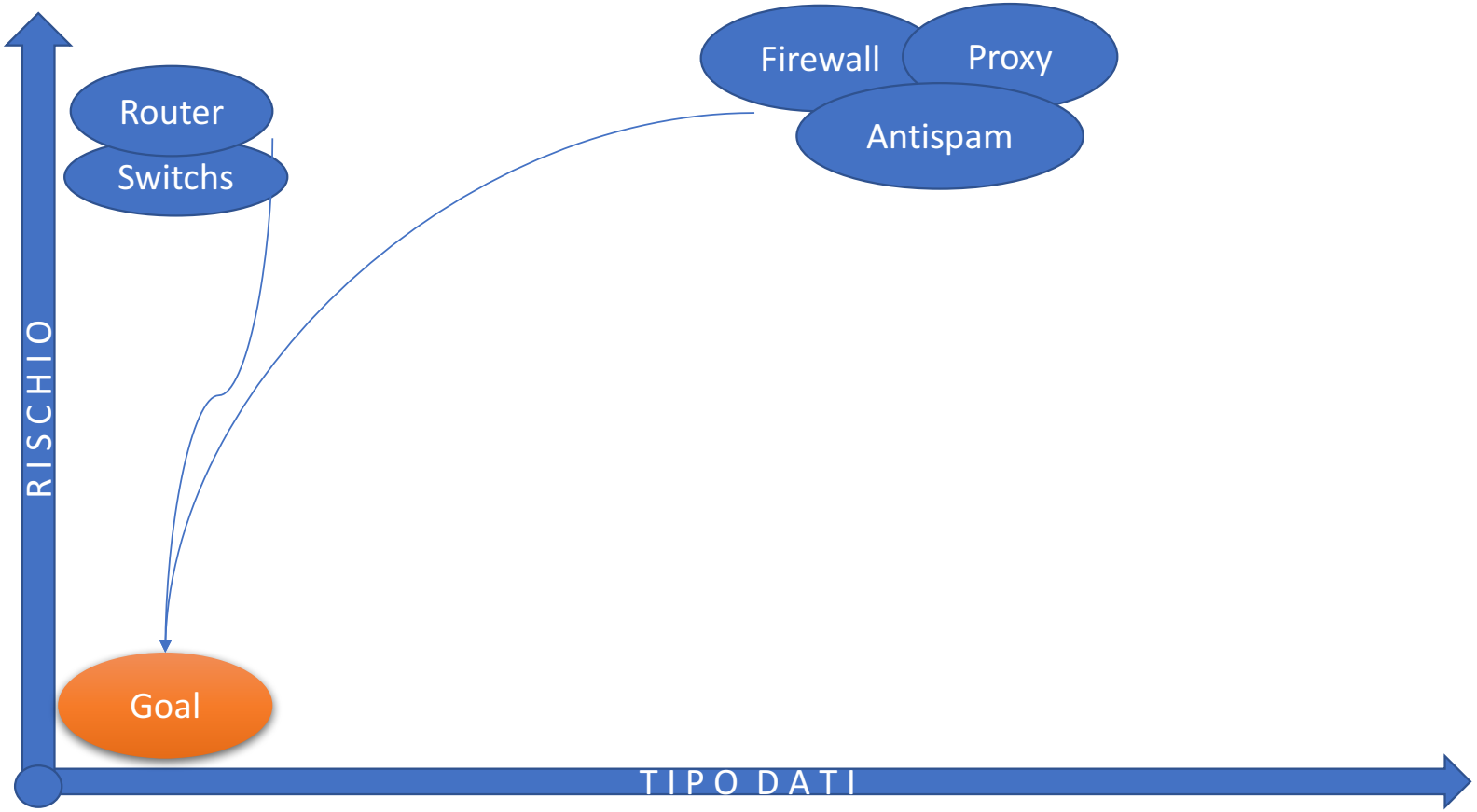
Data Base e Applicazioni

NAS - Backup

UPS OnLine - Eth0

**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.

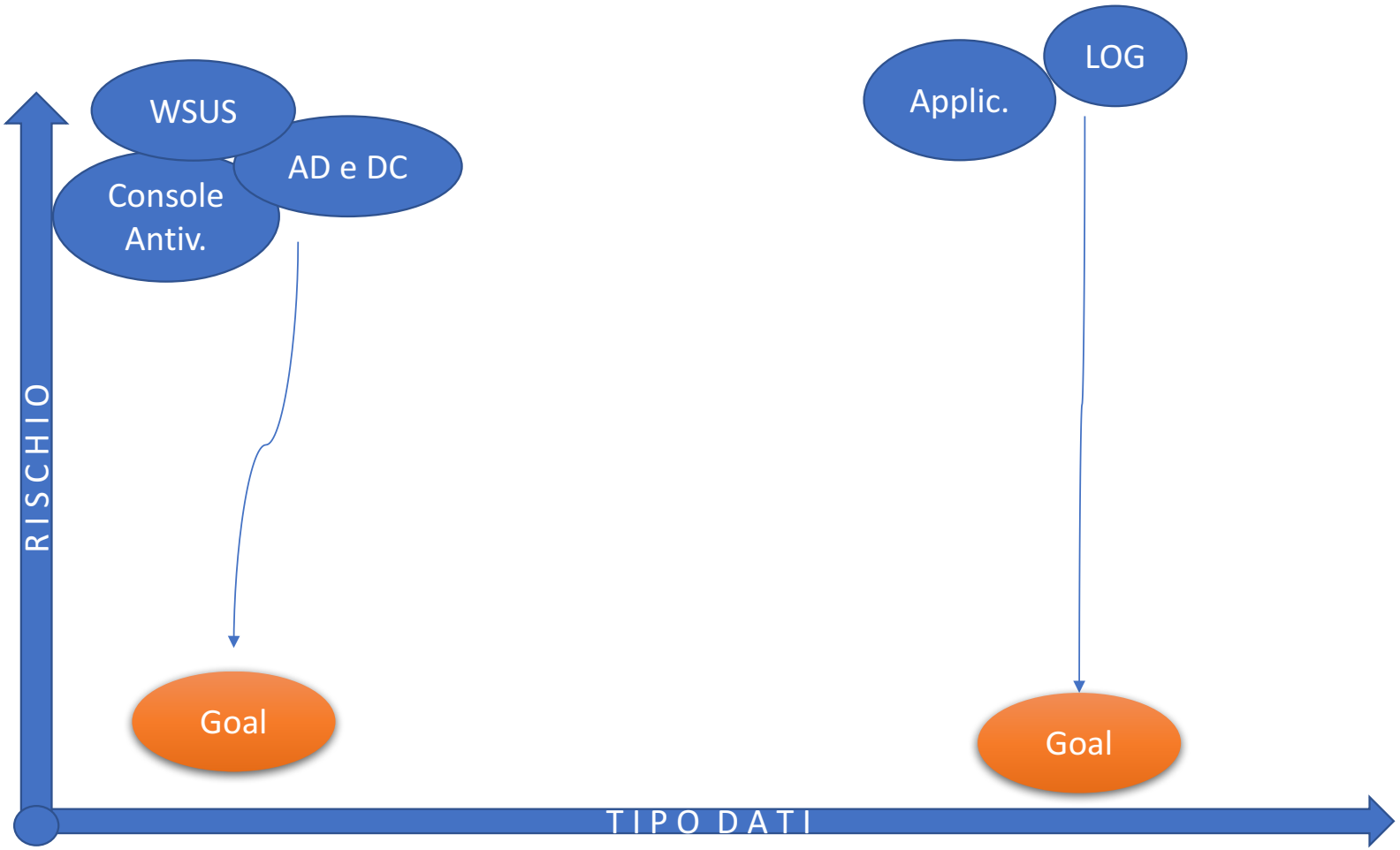
Lo switch centro stella deve avere funzionalità L3 al fine di poter effettuare routing over VLAN

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



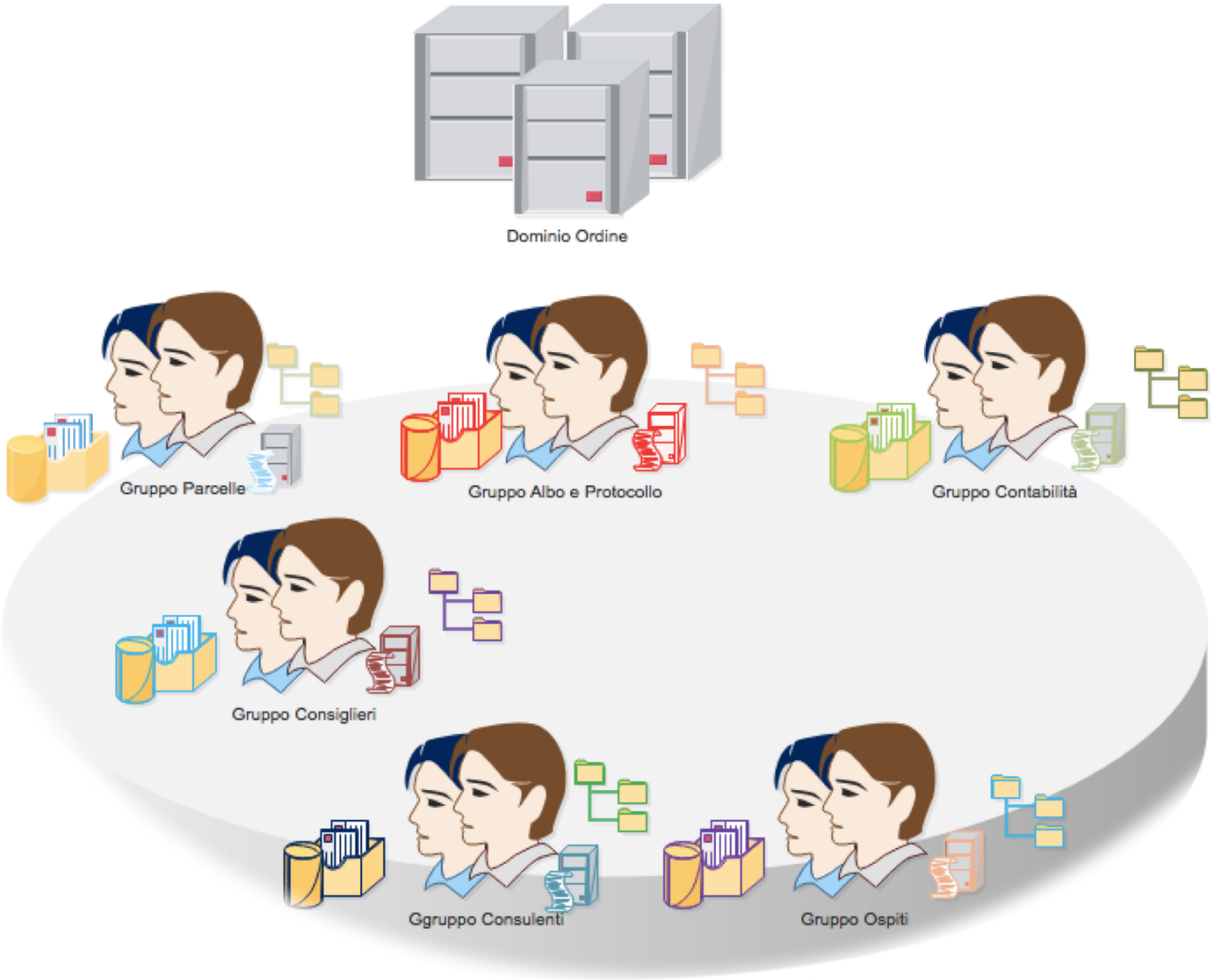
**Struttura Logica**

- 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.


Dominio Ordine
Gruppo Parcelle
Gruppo Albo e Protocollo
Gruppo Contabilità
Gruppo Consiglieri
Ggruppo Consulenti
Gruppo Ospiti

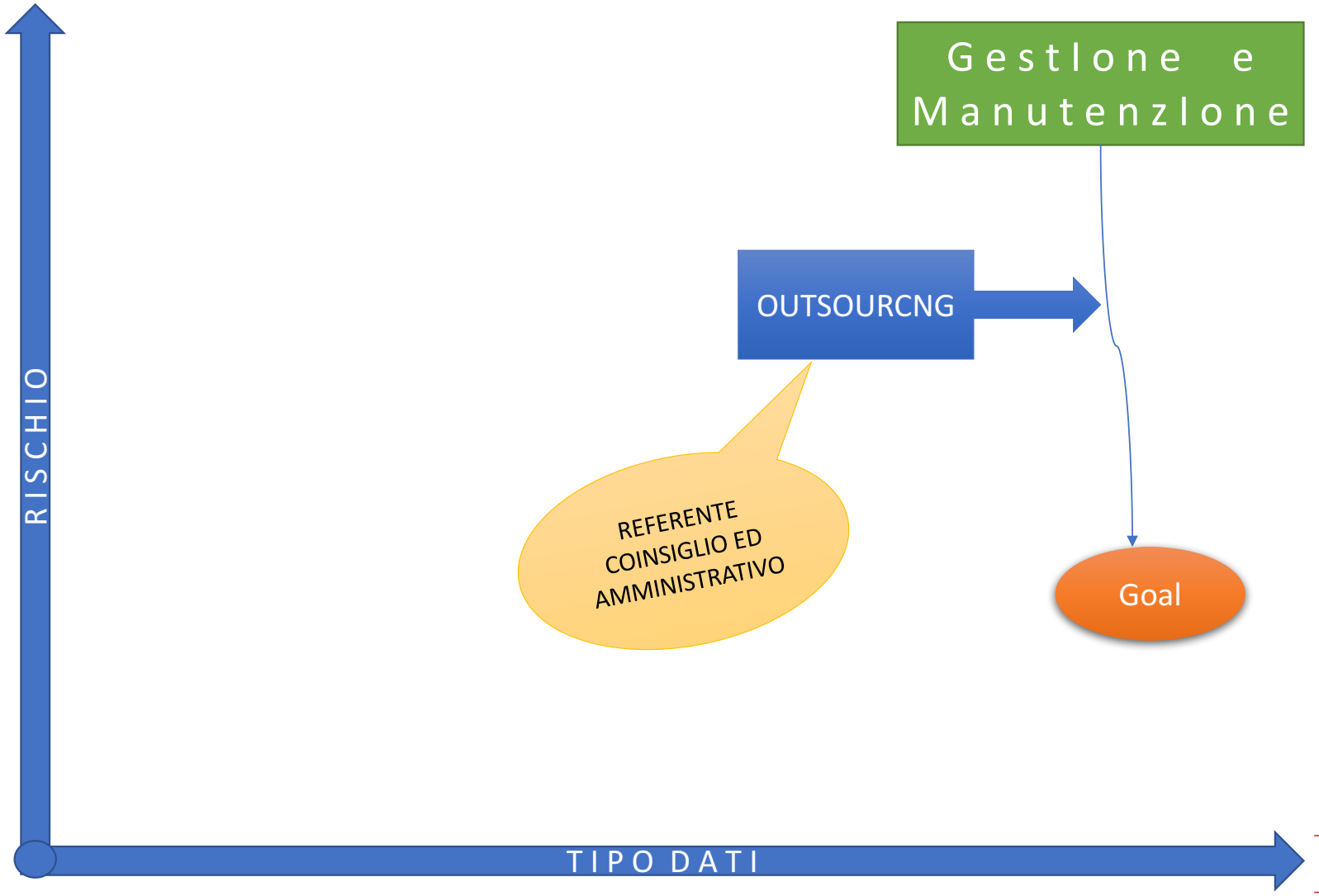
Deve essere attivata una console centralizzata di gestione antivirus che permetta la gestione delle applicazioni  e delle periferiche al fine di effettuare sempre e comunque le seguenti azioni minime:

- 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 COINSIGLIO 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*

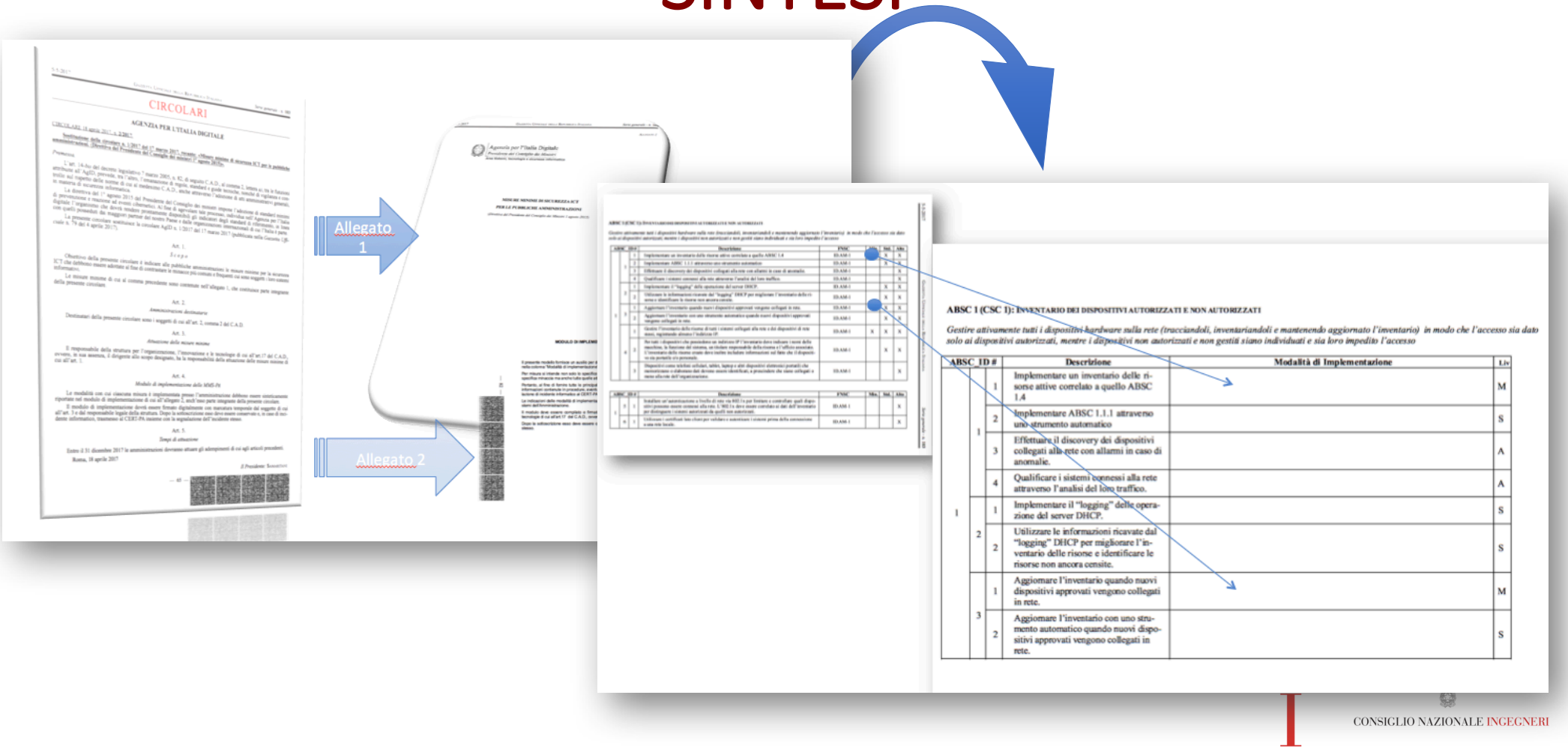
Il responsabile della struttura per l'organizzazione, l'innovazione e le tecnologie di cui all'art.17 del C.A.D., ovvero, in sua assenza, il dirigente allo scopo designato, ha la responsabilità della attuazione delle misure minime di cui all'art. 1.

Gestione e Manutenzione

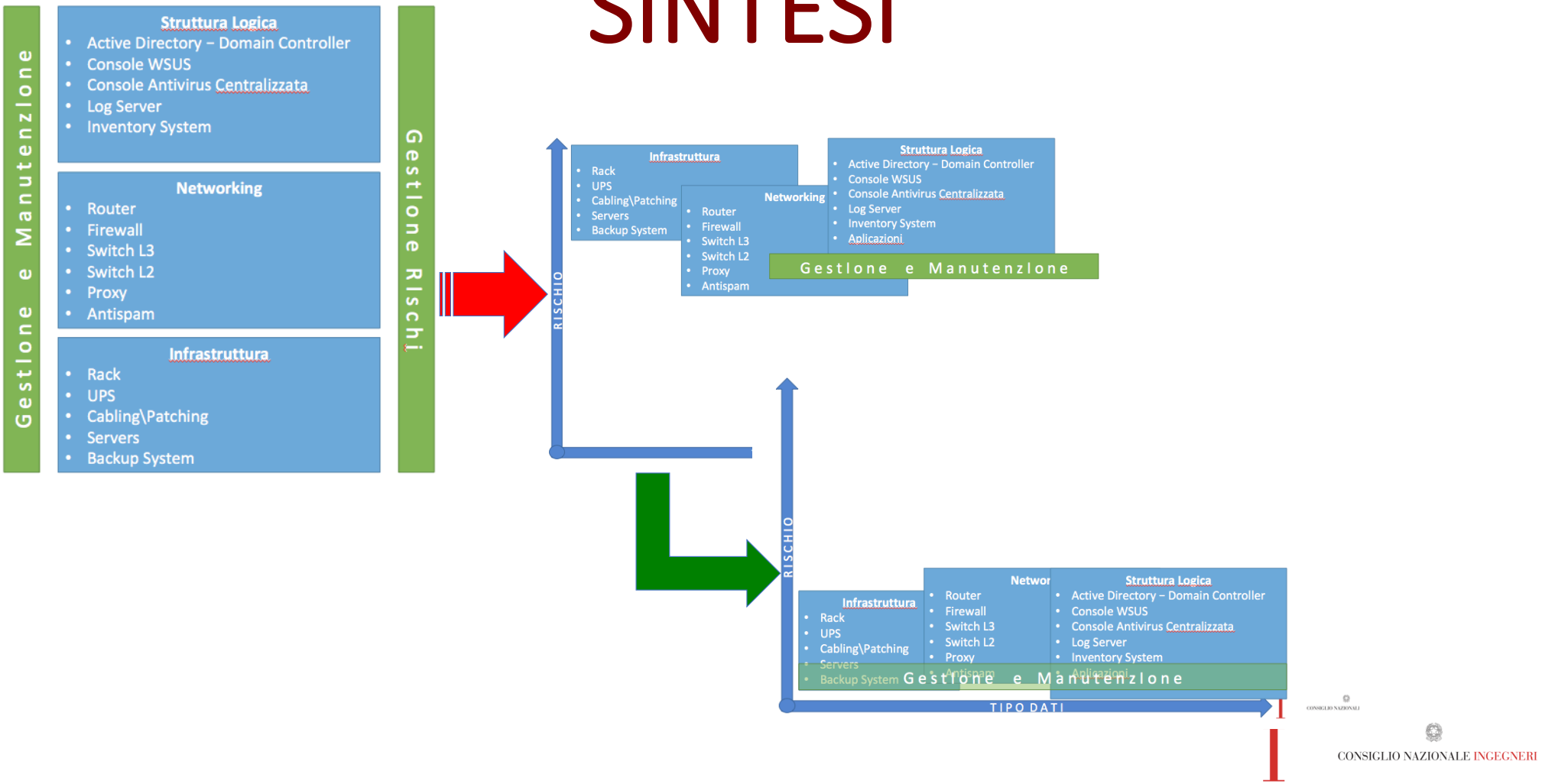
REFERENTE COINSIGLIO ED AMMINISTRATIVO

# SINTESI

# SINTESI


CIRCOLARI
AGENZIA PER L'ITALIA DIGITALE
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




CONSIGLIO NAZIONALE INGEGNERI

# SINTESI

| ABSC | ID # | | Descrizione | FNSC | Mi | Sto | Alto |
|---|---|---|---|---|---|---|---|
| 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 | Sto | Alto |
|---|---|---|---|---|---|---|---|
| 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 | Sto | 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 | | S( | 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 | |

## 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

CONSIGLIO NAZIONALE INGEGNERI

Biagio Garofalo
direzionetecnica@cni-online.it
+39 393 9505301