PROGRAMMA OPERATIVO COMPLEMENTARE

Agenzia per la Coesione Territoriale

Presidenza del Consiglio dei Ministri
Dipartimento della Funzione Pubblica

FORMEZ
AL SERVIZIO DELLA PA

FAST
PICCOLI
COMUNI

AMBITO A

VERSO LA TRANSIZIONE DIGITALE

Sicurezza delle Informazioni

David Harris

21/03/2024


Ransomware criptolocker contro le aziende sanitarie di Modena: “Servizi essenziali garantiti ma molti rallentamenti”. Cosa è successo
PIERMARIO BOCCELLATO — 30 NOVEMBRE 2023 — ITALIA

8.12.2023

CRONACA

Massiccio attacco di hacker russi a enti pubblici italiani, chiesto un riscatto

L'attacco informatico ha colpito negli ultimi giorni una società che fornisce servizi a 1.300 enti.

CYBERSECURITYITALIA

Home Italia Europa Mondo Rubriche Report Eventi Video

Attacco ransomware contro i sistemi informatici della Regione Basilicata. ACN invia pool operativo

MASSIMO CANORRO – 30 GENNAIO 2024 – ITALIA

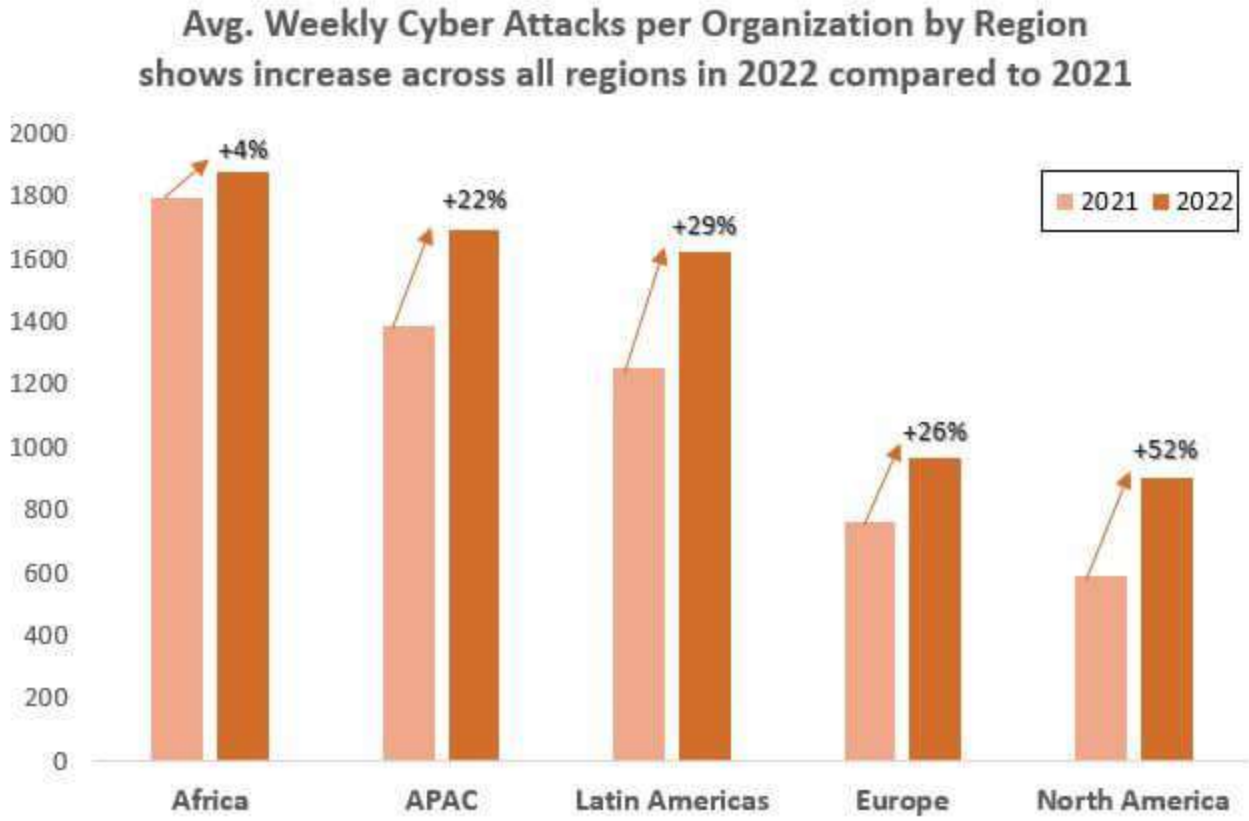
Sferrato un attacco ransomware, con richiesta di riscatto,

Crescita immensa degli attacchi informatici a livello mondiale – stato 2022

- Gli attacchi informatici a livello globale sono aumentati del 125% nel 2021 rispetto al 2020

https://aag-it.com/the-latest-cyber-crime-statistics/#:~:text=The%20growing%20cost%20of%20cyber%20crime&text=The%20average%20cost%20of%20a%20cyber%20breach%20in%202022%20was,in%202022%20was%20%244.35%20million.

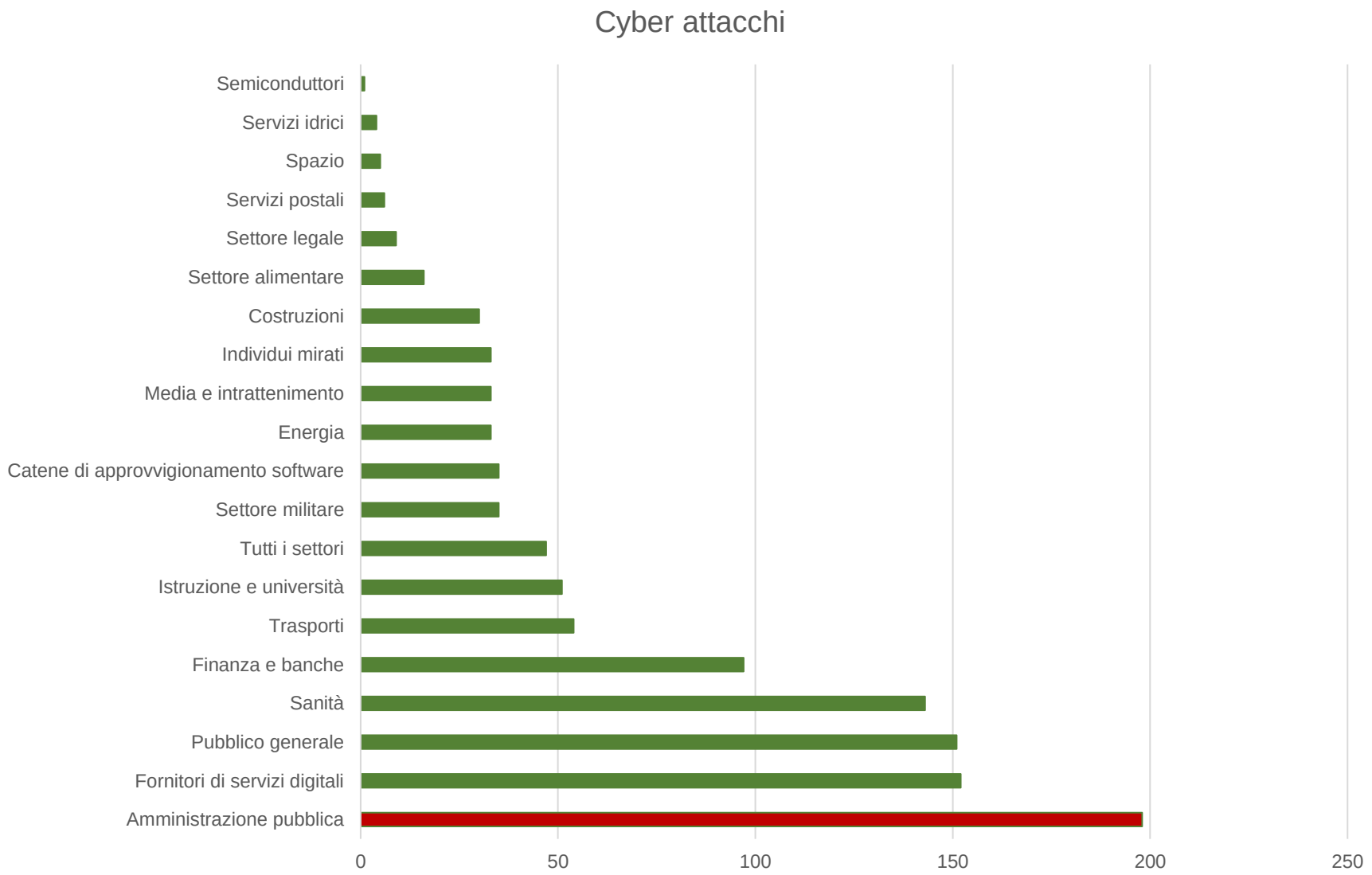
- Gli attacchi informatici sono in aumento in tutto il mondo, con il 38% in più di attacchi informatici a settimana sulle reti aziendali nel 2022, rispetto al 2021



Fonte: Checkpoint - https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks/

Lo scenario Italiano

In 2022 la PA era il settore più colpito dai cyber attacchi



Fonte: elaborazione openpolis su dati agenzia europea di cybersicurezza (Enisa) - 18.3.22
https://www.openpolis.it/numeri/la-pubblica-amministrazione-e-il-settore-piu-colpito-dai-cyber-attacchi/

Stato 2022

Rapporto Clusit 2023

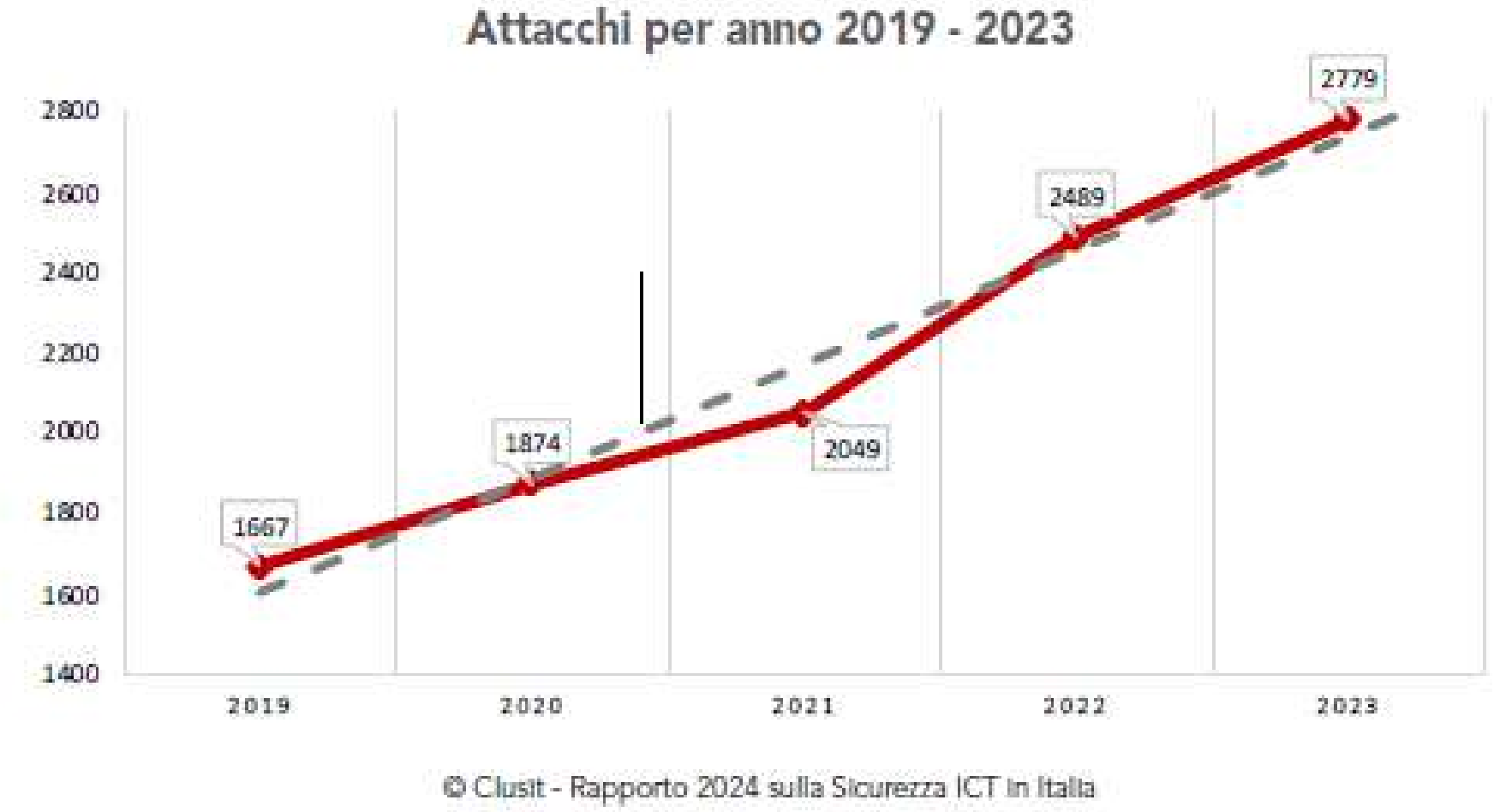
Hacktivism

Corrado Giustozzi di Agid e Clusit ha spiegato: *"Lo scenario in cui viviamo è caratterizzato da pressioni legate al conflitto russo ucraino… … è cresciuto in modo importante l'hacktivism dal 2022, perché il settore pubblico è il preferito dagli attivisti che intendono dimostrare il supporto agli attori dei conflitti"*

https://www.cybersecurity360.it/news/cyber-security-litalia-attaccata-quattro-volte-piu-del-resto-del-mondo-i-dati-semestrali-clusit/

Nel primo semestre del 2023 si è visto un incremento del 30% negli attacchi classificati come "Hacktivism": in Italia, rappresenta una quota molto superiore rispetto alla media globale del 6,9% nel 2022.

Nel 2023 le cose sono peggiorate



Nel 2023, gli attacchi classificati come “critici” o “gravi” rappresentano ormai oltre l’81% del totale (erano il 47% nel 2019)

Nel 2023 le cose sono peggiorate

- **Il periodo che va dal 2018 al primo semestre del 2023 ha visto una crescita esponenziale degli attacchi informatici in Italia**

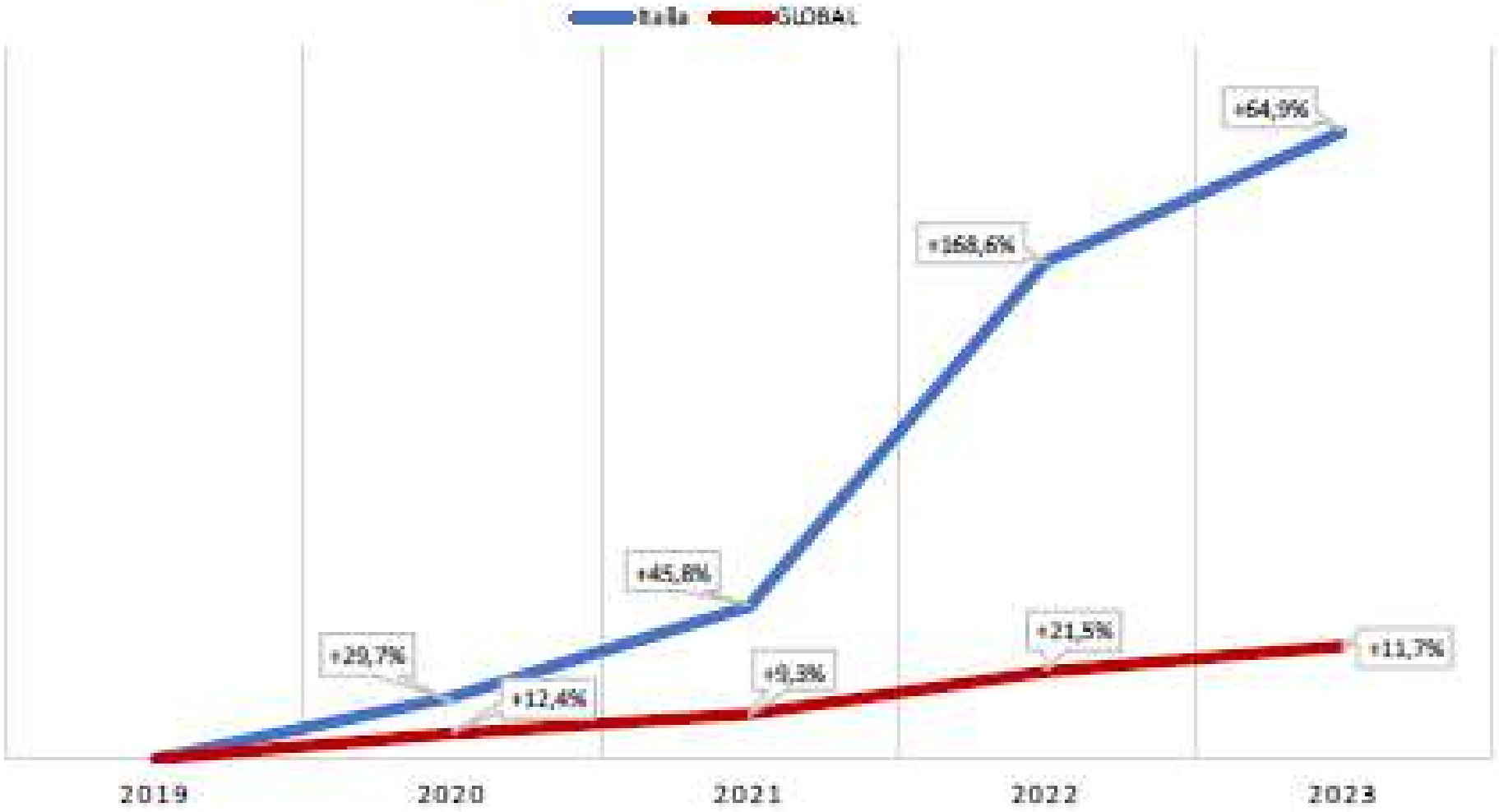
- La percentuale di crescita è del 40% nel primo semestre del 2023 rispetto all'anno precedente, attestandosi a quattro volte la media globale

- **L'Italia è diventata un obiettivo primario per gli attacchi informatici, rappresentando il 9,6% del totale globale di vittime**

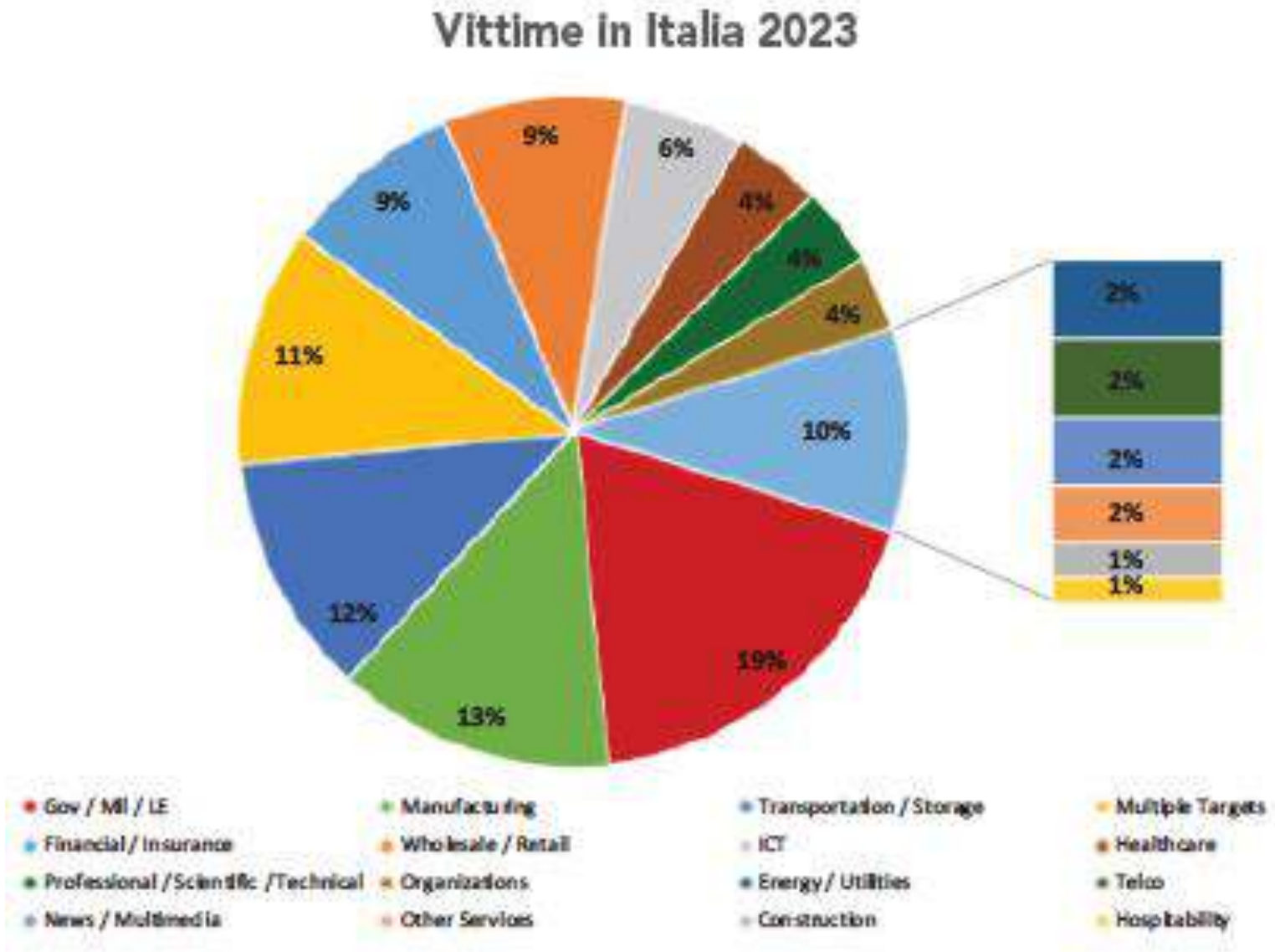
- Gli attacchi gravi o gravissimi rappresentano il 78,5% del totale

«Rapporto Clusit 2023»

Confronto crescita % Italia Vs Global

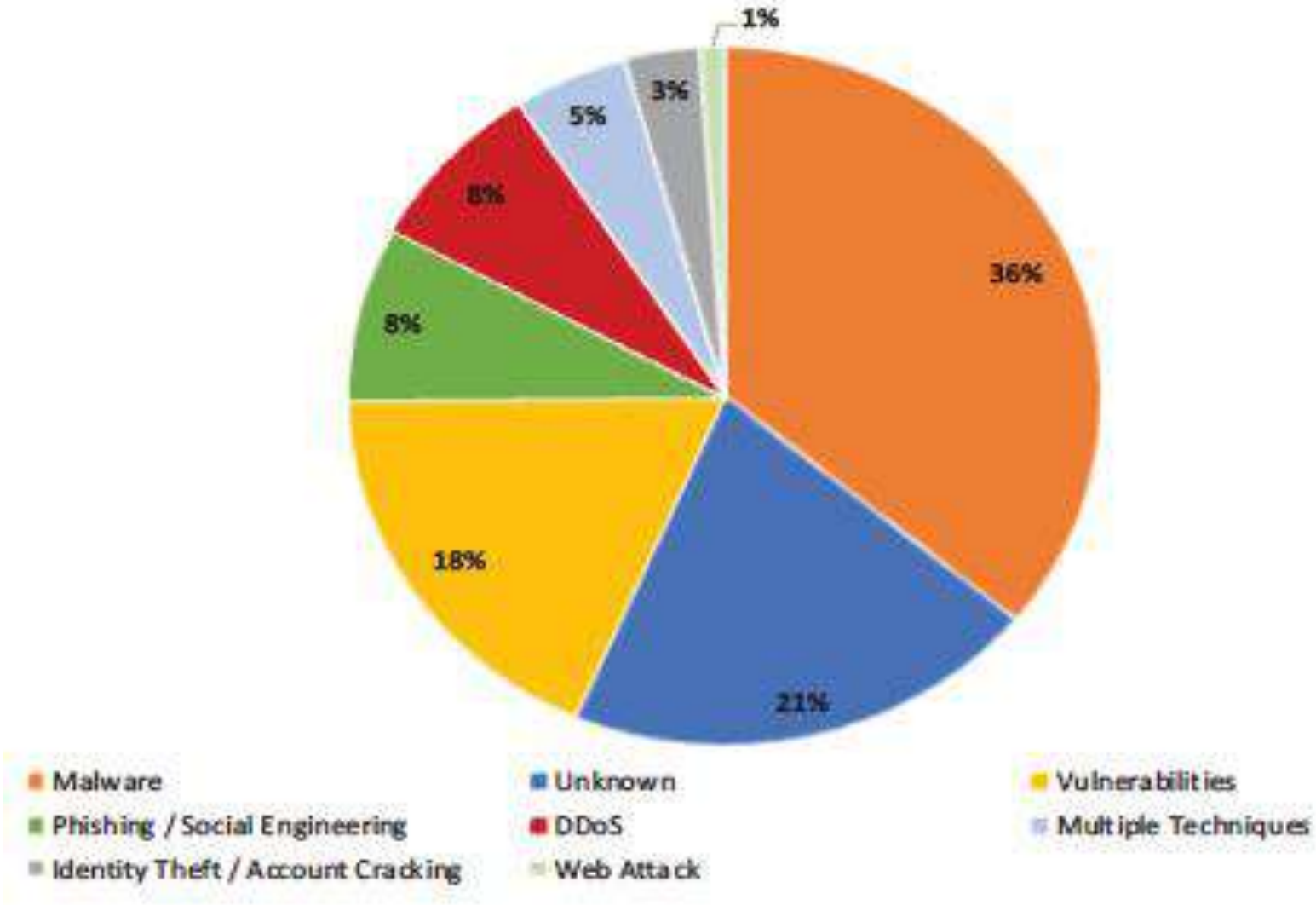


© ClusIt - Rapporto 2024 sulla Sicurezza ICT in Italia



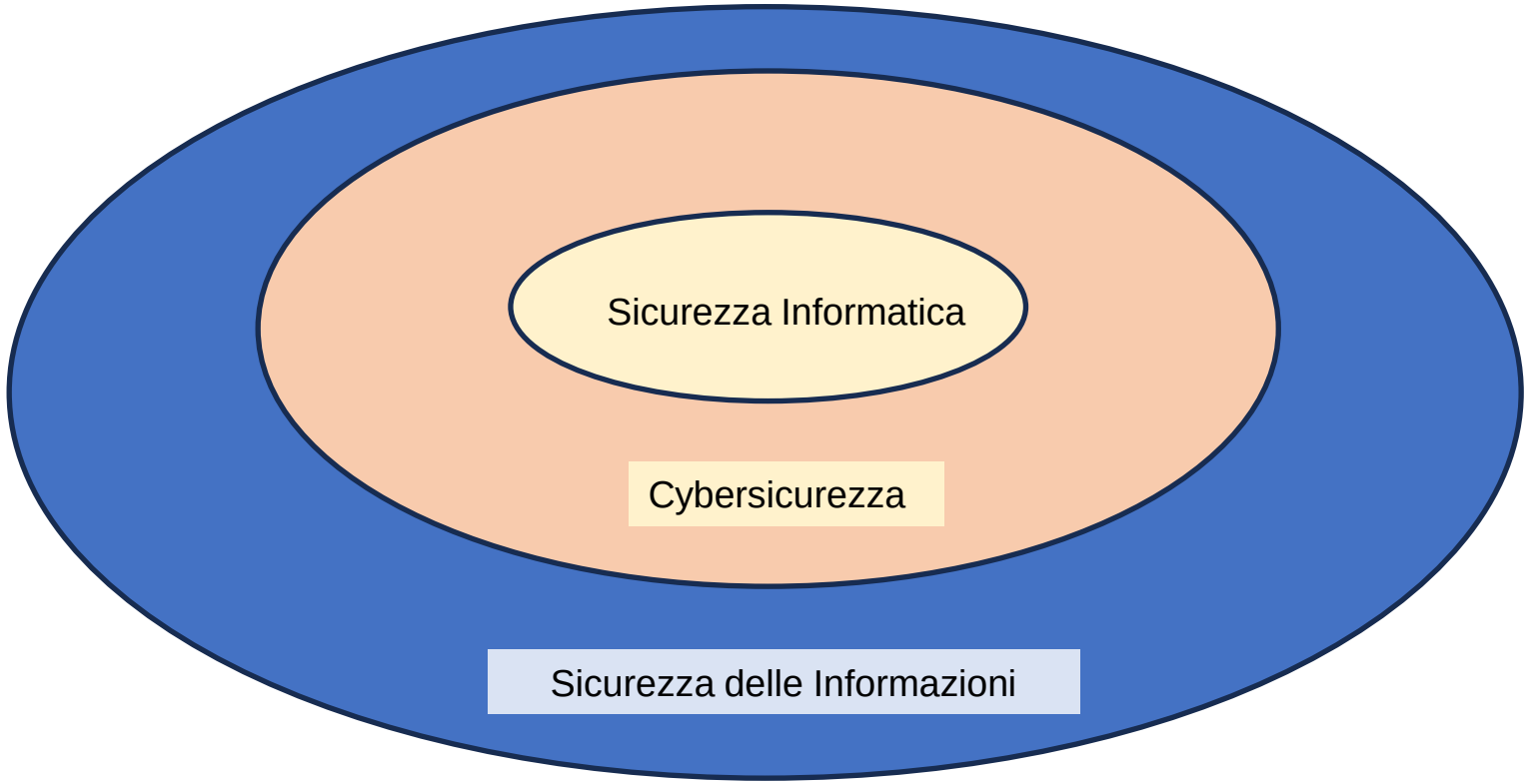
© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia

Distribuzione delle tecniche 2023



© ClusIt - Rapporto 2024 sulla Sicurezza ICT in Italia

Nel contesto delle crescenti minacce digitali emergono chiare necessità di riflessione e azione per mitigare gli impatti negativi sulla sicurezza delle informazioni in Italia.



La **Sicurezza delle Informazioni** estende la sicurezza al livello fisico, ai dati, all'organizzazione, ai processi e alle persone.

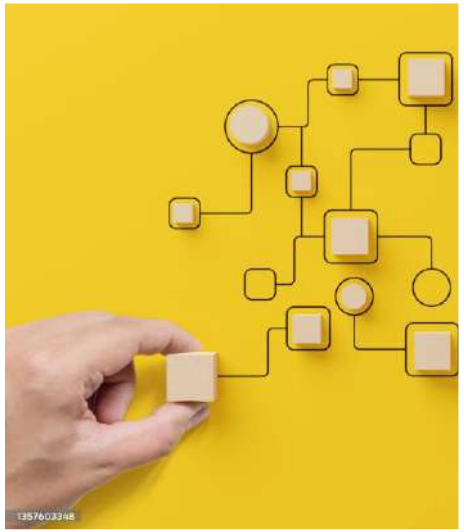
La **Sicurezza Informatica** è la protezione dei sistemi IT contro danni e rischi. Ciò vale per singoli file su computer come per interi data center e comprende database, software, applicazioni, server e dispositivi.

La **Cybersicurezza** estende la sicurezza informatica al cyber spazio complessivo. Ciò include controlli di accesso, crittografia, gestione dei diritti, firewall, proxy, gestione delle vulnerabilità e molto altro; si concentra sulle attività criminali agevolate specificamente attraverso Internet.

Le fasi di sicurezza

- Prevenzione/Protezione
- Rilevamento
- Risposta

I Pilastri

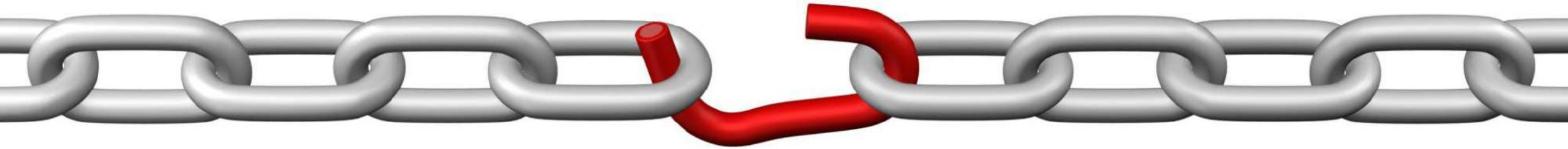


Le Persone

I processi

I dati

Una catena non è più forte dell'anello più debole



Non si possono eliminare i rischi né avere sicurezza perfetta (costi proibitivi, attacchi sempre più sofisticati, ecc.).

Ma si può e si deve cercare di mitigare i rischi.

Ad esempio la MMS 4.8.1 impone di «*Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità, del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).*»

Mitigazione del rischio: cosa costituisce un Sistema Informatico sicuro?

Un computer chiuso in un caveau, senza connessione di rete né connessione elettrica, e anche in questo caso dovresti preoccuparti di chi può accedere al caveau.

La sicurezza implica sempre dei compromessi

5 passi per valutare costi – benefici (il modello di Bruce Schneier)

1. Quali risorse stai cercando di proteggere?
2. Quali sono i rischi contro questi asset?
3. In che misura la soluzione di sicurezza mitiga i rischi?
4. Quali altri rischi comporta la soluzione di sicurezza?
5. Quali compromessi richiede la soluzione di sicurezza?

Esempio: le password

- Le password compromesse sono coinvolte in circa l'80% delle violazioni

Forrester Research - https://www.forrester.com/report/The-Forrester-Wave-Privileged-Identity-Management-Q4-2018/RES141474

- L'82% di tutte le violazioni dei dati sono dovute a errori umani evitabili, come password facilmente indovinabili

https://www.verizon.com/business/resources/reports/dbir/

Regole tipiche per le password

- Non devono contenere il nome dell'account dell'utente o parti del nome completo dell'utente che superino due caratteri consecutivi
- Devono avere almeno 8 caratteri di lunghezza
- Devono contenere almeno tre delle seguenti quattro categorie:
- Caratteri maiuscoli inglesi (dalla A alla Z)
- Caratteri minuscoli inglesi (dalla a alla z)
- Numeri (da 0 a 9)
- Caratteri non alfabetici (ad esempio, !, $, #, %)
- Devono essere cambiate almeno ogni 180 giorni
- Le vecchie password non possono essere riutilizzate prima di sei modifiche

Esempio: le password

Io: Cos'è la password del Wi-Fi?
Barista: Prima deve comprare da bere
Io: Si certo. Mi dia una birra. Quanto costa?
Barista: €10
Io: Ok, ecco i soldi. E adesso cos'è la password del Wi-Fi?
Barista: Prima deve comprare da bere. Tutto minuscolo e senza spazi

Esempio: Password. Applichiamo il modello di Schneier

1. **Quali risorse stai cercando di proteggere?**

   - impedire l'accesso non autorizzato ai dati.
   - impedire l'uso non autorizzato delle tue risorse, con possibili implicazioni legali.
   - evitare danni alla tua rete.
   - …

Esempio: Password. Applichiamo il modello di Schneier

2. Quali sono i rischi contro questi asset?

Il rischio è che i criminali possano mettere le mani su questi dati.

Dal punto di vista dell'amministrazione, tuttavia, il rischio è ciò che potrebbe succedere a loro se ciò accadesse.

Ciò li porterà a ricevere sanzioni pecuniarie?

Il sindaco sarà trascinato davanti al giudice?

Il funzionario riceverà una valutazione delle performance negativa?

Esempio: Password. Applichiamo il modello di Schneier

3. **In che misura la soluzione di sicurezza mitiga i rischi?**

Costringere le persone a cambiare frequentemente la propria password sarà una misura significativamente efficace per impedire l'accesso non autorizzato?

Esempio: Password. Applichiamo il modello di Schneier

4. **Quali altri rischi comporta la soluzione di sicurezza?**

Poiché tutte le misure di sicurezza richiedono una varietà di risorse (e il tempo e l'attenzione delle persone sono una di quelle risorse), enfatizzare una misura di sicurezza può sottrarre risorse a misure più efficaci che non ricevono sufficiente attenzione.

Rischi derivanti dal modo in cui le persone agiscono in risposta a questa politica.

Esempio: Password. Applichiamo il modello di Schneier

5. Quali compromessi richiede la soluzione di sicurezza?

Questa politica ha un impatto notevole:

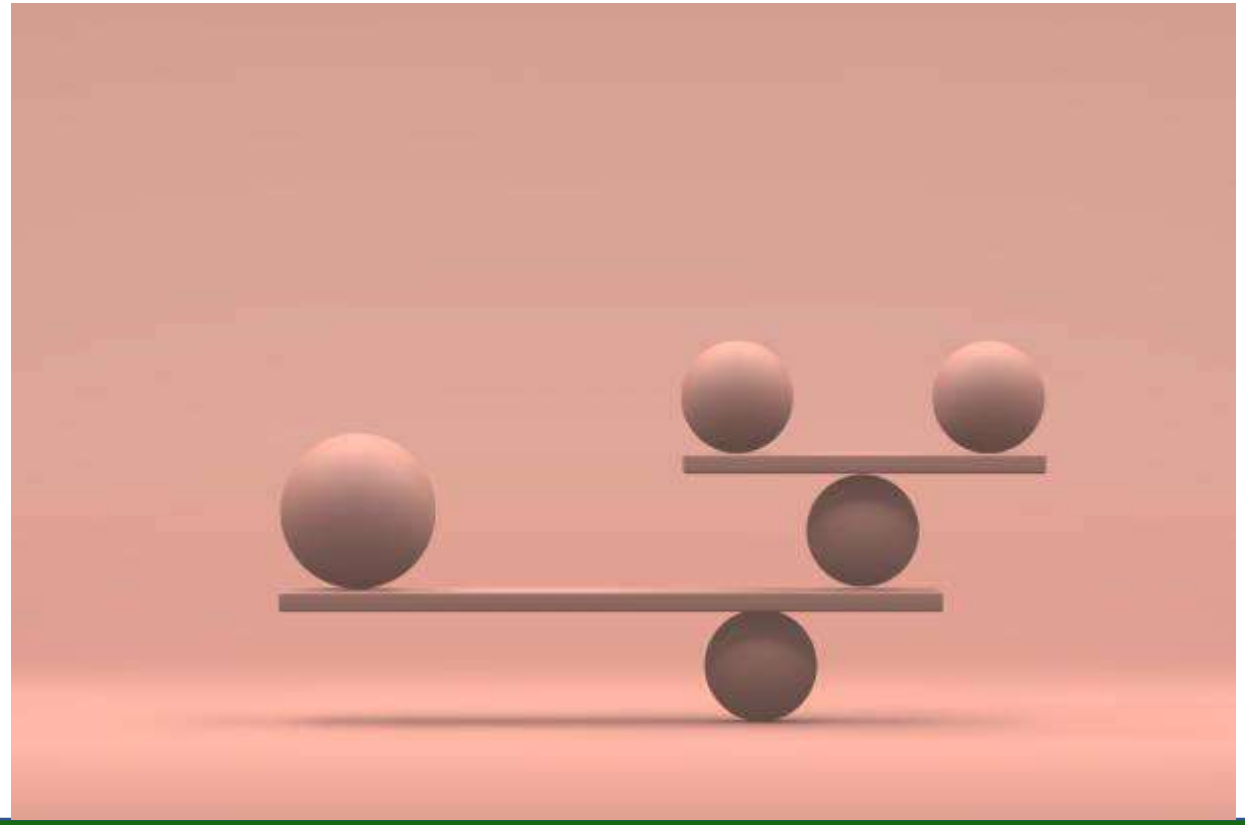
- Le persone cercano delle password facile;
- Il reparto IT è visto con una certa ostilità,
- L' Help Desk IT riceve molte chiamate da persone che non possono accedere perché hanno dimenticato la password, che è una conseguenza naturale del costringere le persone a continuare a cambiarla.

Tutto questo per una soluzione che in realtà serve a poco.

Esempio: Password - Cosa significa tutto questo in ultima analisi?

Considerare attentamente quali misure valga effettivamente la pena adottare

Valutare alternative



Come si indovina le password

- Il cracking delle password (chiamato anche hacking delle password) è un vettore di attacco che coinvolge gli hacker che tentano di decifrare o determinare una password utilizzando un software specifico.

- Un cracker di password recupera le password utilizzando varie tecniche. Le più semplici (e comuni):

  - Usare un elenco di parole (password comuni)

  - Forza bruta in cui vengono controllate tutte le combinazioni possibili

Come si indovina le password – spesso le ns regole facilitano il processo

I frequenti cambi di password innescano la nostra pigrizia, quindi “password” diventa “password1” e “password2”.

Ogni cracker di password è a conoscenza di queste cattive pratiche relative alle password.

Anche sostituire le lettere con numeri e simboli è una pratica prevedibile. Ad esempio, 3 per E, 4 per A e @ per a, zero per O, 1 per I…. Gli strumenti di cracking delle password preparano per queste variazioni comuni.

Gli aggressori cercano di apprendere informazioni di base sulla complessità della password, come la lunghezza minima e massima della password, nonché la complessità della password. Ad esempio, la password contiene lettere maiuscole e minuscole, numeri, simboli o una combinazione? Gli aggressori sono anche interessati a conoscere le restrizioni sulle password. Questi parametri potrebbero essere:

- Iniziare con una lettera maiuscola
- Non iniziare con un numero
- Richiedere un numero minimo di un particolare tipo di carattere

Le tipiche regole (limitando la ripetizione dei caratteri, almeno un simbolo e un numero…) riducono il numero di combinazioni che l’aggressore deve prendere in considerazione e, quindi, minano l’efficacia della password.

Cracking delle password sui sistemi Windows

- In Windows, sono consentiti l'utilizzo di 96 caratteri per le password:

  A – Z
  a - z
  0 – 9
  @ # $ % ^ & * - _ ! + = [ ] { } | \ : ' , . ? / ` ~ " ( ) ; < >
  Blank space

- Per una password composta da 2 caratteri ci sono 96 * 96 diverse possibilità (9.216)
- Ogni carattere in più moltiplica per 96 il numero di possibilità

Una password lunga = una password più sicura

- Per un password composta da 8 caratteri le possibilità sono 7.213.895.789.838.336

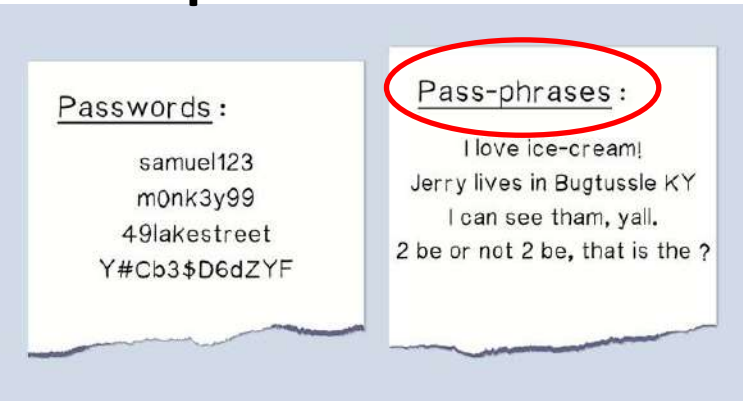
Ma una password lunga potrebbe essere difficile da ricordare.

La soluzione è un pass-phrase (sino a 127 carattere):

- Esempio: *Sono un consulente del Formez.* - 31 caratteri - le possibilità sono 2,8 * 10^61 (in confronto, ci sono «solo» 1,3 * 10^50 atomi in questo mondo)

Valutare alternative

qualcosa che sai



qualcosa che hai: cellulare, token, autenticatore app

qualcosa che sei

Standard di riferimento

ISO 31000: GESTIONE DEL RISCHIO - PRINCIPI E LINEE GUIDA
Standard che fornisce una serie completa di principi e linee guida per aiutare le organizzazioni ad eseguire l'analisi e la valutazione dei rischi.

IRAM 2 (ISF): METODOLOGIA DI SECURITY RISK ASSESSMENT
Metodologia di valutazione dei rischi mediante analisi e valutazione di minacce, vulnerabilità e impatti

ISO 27001: SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI
Standard utilizzato per arricchire il framework di controlli in ambito information security

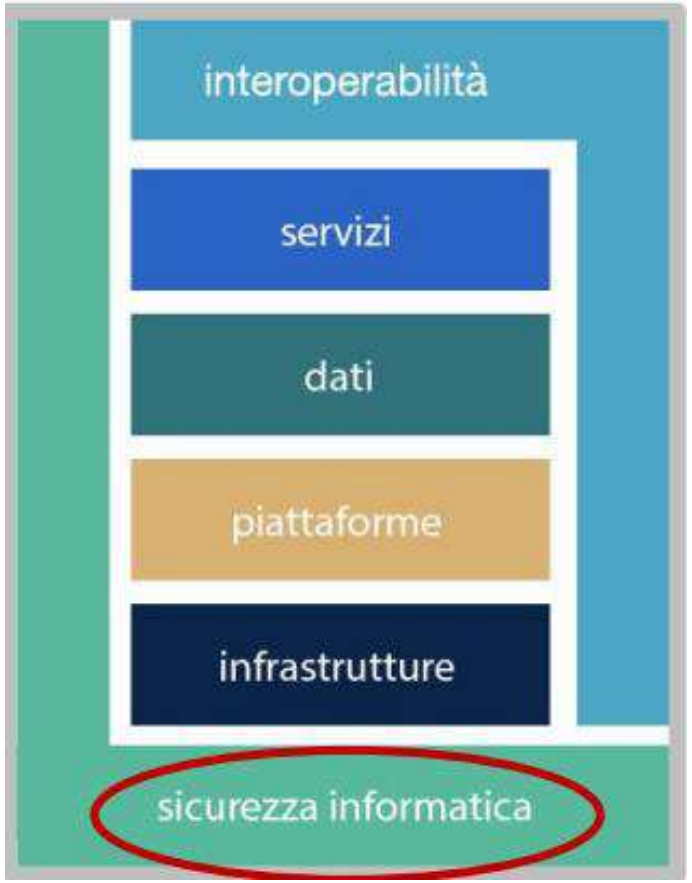
NIST
Insieme di pubblicazioni utilizzate per arricchire il framework di controlli in ambito information security

MISURE MINIME DI SICUREZZA ICT PER LE PA
Misure per valutare e migliorare il livello di sicurezza informatica della PA, al fine di contrastare le minacce informatiche più frequenti

Quadro Normativo (parziale) in Italia

- DPCM n. 81/2021 ha definito le modalità per la notifica nel caso di incidenti dovuti ad attacchi informatici;
- DL n. 82/2021 ha definito l'architettura nazionale di cybersicurezza e ha istituito l'Agenzia per la cybersicurezza nazionale;
- il PNRR comprende la cybersecurity nella Missione 1 e le destina. 620 milioni di euro;
- DPCM 16 settembre 2021 ha definito i termini e le modalità del trasferimento di funzioni, beni strumentali e documentazione dal Dipartimento delle informazioni per la sicurezza all'Agenzia per la cybersicurezza nazionale.

Architettura del PTI



PRIORITÀ		
PIATTAFORME ABILITANTI	SPID, PAGOPA, APPIO, PND, SEND (INAD)	FINANZIAMENTO PNRR
SITI ISTITUZIONALI		FINANZIAMENTO PNRR
APPLICAZIONE LINEE GUIDA AGID SUL DOCUMENTO INFORMATICO		
CLOUD E SICUREZZA INFORMATICA		FINANZIAMENTO PNRR
OPEN DATA		
COMPETENZE DIGITALI DIPENDENTI E CITTADINI		FINANZIAMENTO PNRR 1.7 REGIONE

Come FAST può aiutare i comuni

I microprogetti predisposti sono un insieme di misure tecniche ed organizzative.

- **Misure Minime di Sicurezza**

Assistere il comune nel raggiungere la conformità con le misure minime di sicurezza.

- **Capitolato per la nomina dell'Amministratore di Sistema e per l'affidamento della gestione del sistema informatico**

Supportare il Comune nella redazione del capitolato di gara allo scopo di assicurare che il servizio di assistenza e amministrazione degli strumenti locali del comune sia conforme a quanto previsto nelle Misure Minime di Sicurezza.

- **Regolamento comunale per la sicurezza delle informazioni**

Dotare il comune di un regolamento che stabilisce la politica per la sicurezza delle informazioni e regole per l'utilizzo degli strumenti ICT.

- **Realizzazione di un Piano di continuità operativa**

Assistere i comuni nell'attivare le misure di protezione organizzative e procedurali

Come aumentare il livello di protezione dei sistemi informatici

- Dal 31 dicembre 2017, come indicato nell'art. 17 del Codice dell'Amministrazione Digitale (CAD), è entrato in vigore l'obbligo per le pubbliche amministrazioni, di mantenere standard minimi di sicurezza relativi alle infrastrutture informatiche.

- Tutte le pubbliche amministrazioni sono quindi tenute a sottostare alle misure minime di sicurezza informatica elaborate da AgID.

- AgID ha fornito alla PA un vademecum per il raggiungimento di misure minime di sicurezza ICT. Si tratta delle "**Misure minime di sicurezza ICT per le pubbliche amministrazioni**".

I tre livelli di controllo nelle MMS – un insieme di misure tecniche ed organizzative

Minimo

Ogni pubblica amministrazione deve necessariamente adottare le misure di sicurezza relative a questo livello

Standard

Livello base per una sicurezza seria

Avanzato

Livello di miglioramento per una sicurezza robusta

AgID

Le Misure Minime di Sicurezza

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

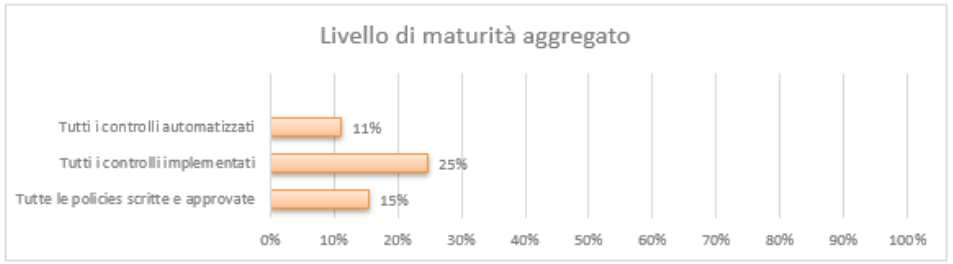
Le modalità con cui ciascuna misura è implementata presso l'amministrazione debbono essere sinteticamente riportate nel modulo di implementazione di cui all'allegato 2, anch'esso parte integrante della presente circolare.

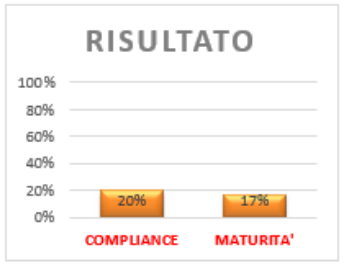
Il modulo di implementazione dovrà essere firmato digitalmente con marcatura temporale dal soggetto di cui all'art. 3 e dal responsabile legale della struttura. Dopo la sottoscrizione esso deve essere conservato e, in caso di incidente informatico, trasmesso al CERT-PA insieme con la segnalazione dell'incidente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

Otto tabelle con le singole misure (identificate con il nome AGID Basic Security Control - ABSC).

- inventario dei dispositivi autorizzati e non autorizzati
- inventario dei software autorizzati e non autorizzati
- proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, pc e server
- valutazione e correzione continua della vulnerabilità
- uso appropriato dei privilegi di amministratore
- difese contro i malware
- copie di sicurezza
- protezione dei dati

Analisi dello stato attuale

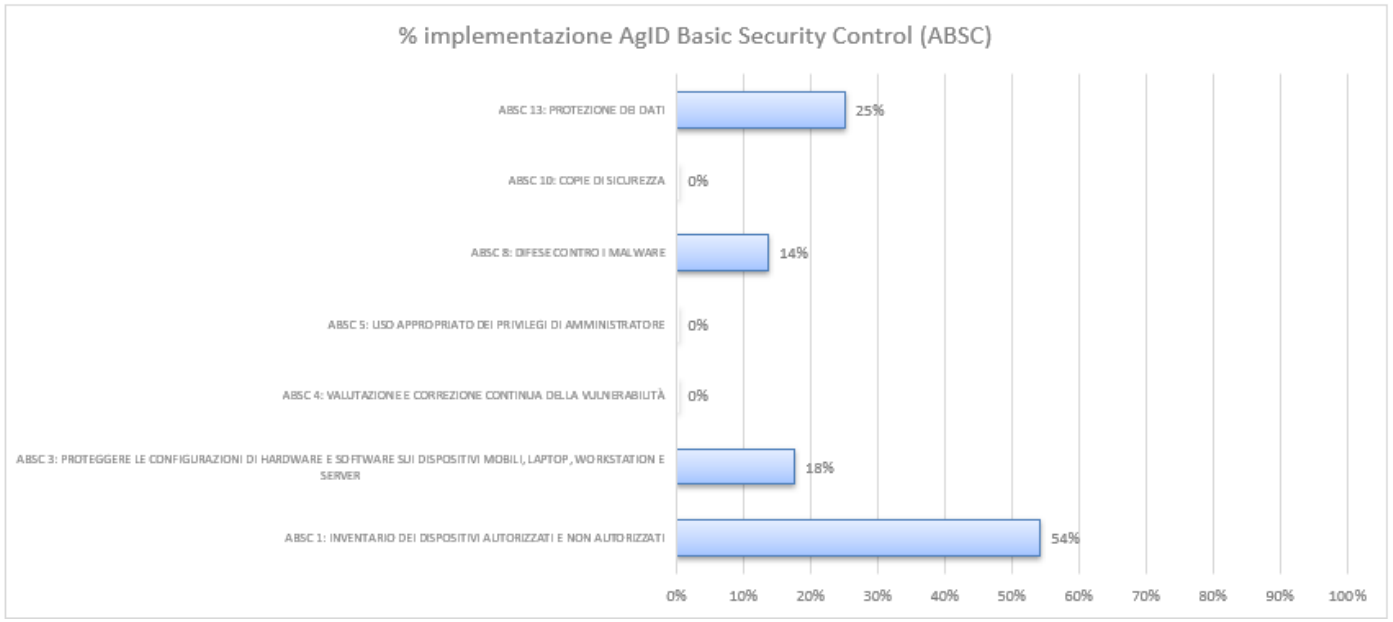




ABSC 1: INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI	54%
ABSC 2: INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI	50%
ABSC 3: PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SU	18%
ABSC 4: VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ	0%
ABSC 5: USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE	0%
ABSC 8: DIFESE CONTRO I MALWARE	14%
ABSC 10: COPIE DI SICUREZZA	0%
ABSC 13: PROTEZIONE DEI DATI	25%

DESCRIZIONE	punteggio
Tutte le policies scritte e approvate	15%
Tutti i controlli implementati	25%
Tutti i controlli automatizzati	11%
COMPLIANCE	20%
MATURITA'	17%

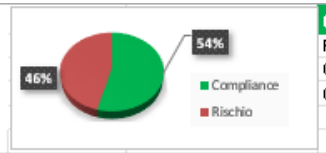
Livello di Sicurezza	Minimo



Compilazione delle MMS e sintesi per ogni ABSC

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.



Compliance	54%	Rischio	46%
Policy scritte e aprovate	50%		
Controlli implementati	58%		
Controlli automatizzati	17%	% di maturità	42%

ABSC_ID			Livello	Descrizione	Richiede una policy scritta	Policy definita (se richiesta)	Policy implementato	Controllo automatizzato	Previsione anno di implementazione	Previsione trimestre di implementazione	Modalità di implementazione
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	No	policy non necessaria	su tutti i sistemi	su tutti i sistemi	2024	1	•Censimento di tutti gli indirizzi IP in uso alla struttura; censimento dell'inventario: ciascun utente della struttura dovrà compilare un form nella qual dovrà indicare i riferimenti tecnici del o dei dispositivoli che utilizza (es. mac address ovvero modello e numero di serie), e i software (per tipologia o categoria). Etichettare i dispositivi •Acquistare e adoperare un software gestionale, quale ad esempio, la piattaforma Microsoft System Management Server che procede automaticamente ad avere un riepilogo inventariale di tutte le PdL (sia desktop che portatili) e i server windows presenti nella rete del comune. In ogni caso, l'inventario patrimoniale dei beni informatici viene mantenuto dall' ufficio preposto all' installazione nuovi dispositivi. I nuovi dispositivi prima di essere messi in esercizio sono etichettati. Dal punto di vista tecnico a tutti i pc desktop e portatili collegati in rete viene attribuito un indirizzo IP. •L'inventario patrimoniale dei beni informatici viene mantenuto aggiornato attraverso l'incarico ad una ditta esterna che a provvede ad etichettare i dispositivi acquisiti prima che vengano inseriti in rete. Dal punto di vista tecnico tutti i pc, portatili e telefoni VOIP collegati in rete sono gestiti dal DHCP. Quindi accedendo ad uno dei due server attivi è possibile verificare quali sono i dispositivi in esso registrati. Tutti i PdL (sia desktop che portatili) e i server windows sono inventariate automaticamente all'interno della piattaforma Microsoft System Management Server
	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	Si	Policy non scritta	su maggior parte sistemi	Non automatizzata	2024	2	Nel regolamento comunale è fatto divieto ai dipendenti di utilizzare / collegare alla rete dispositivi non autorizzati. Secondo quanto implementato in ABSC 1.1.1 le risposte possono essere: •È in esercizio la piattaforma Microsoft System Management Server per monitorare e gestire tutte le PdL e i server Windows. •Gli inventari di cui al ABSC 1.1.1 vengono aggiornati quando nuove risorse attive vengono collegate in rete

Cronoprogramma – attuazione delle MMS mancante

						data prevista per completare l'implementazione (se necessario)											
						2024				2025				2026			
ABSC_ID			Livello	Descrizione	Controllo già implementato (almeno in parte)	1° Trimestre	2° Trimestre	3° Trimestre	4° Trimestre	1° Trimestre	2° Trimestre	3°° Trimestre	4° Trimestre	1° Trimestre	2° Trimestre	3°° Trimestre	4° Trimestre
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4													
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.													
1	4	1	M	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.													
2	1	1	M	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.													
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.													
3	1	1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.													
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.													
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.													
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.													
3	4	1	M	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).													
4	1	1	M	Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.													
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.													
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.													
4	5	2	M	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di													
4	7	1	M	Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.													
4	8	1	M	Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità , del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).													
4	8	2	M	Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.													
5	1	1	M	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.													
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.													
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.													

Dove iniziare - i cinque controlli grazie ai quali evitare l’85% degli attacchi cyber

1. inventario e controllo delle risorse hardware
2. inventario e controllo delle risorse software
3. costante vulnerabilità management
4. uso controllato dei privilegi amministrativi
5. configurazione sicura per hardware e software su qualsiasi dispositivo aziendale

CAPITOLATO SPECIALE

PER LA NOMINA DELL'AMMINISTRATORE DI SISTEMA E L'AFFIDAMENTO DEL SERVIZIO DI ASSISTENZA, GESTIONE E MANUTENZIONE DELLA RETE, DEL SISTEMA INFORMATICO, TELEFONICO, DELLE POSTAZIONI DI LAVORO E DEI SERVER – PER MESI XX (ANNI 2024/2025/2026).

Indice

CAPITOLATO SPECIALE

PER LA NOMINA DELL'AMMINISTRATORE DI SISTEMA E L'AFFIDAMENTO DEL SERVIZIO DI ASSISTENZA, GESTIONE E MANUTENZIONE DELLA RETE, DEL SISTEMA INFORMATICO, TELEFONICO, DELLE POSTAZIONI DI LAVORO E DEI SERVER – PER MESI XX (ANNI 2024/2025/2026).

Art. 5 comma A - Attività inerenti alle Misure Minime per la Sicurezza ICT delle pubbliche amministrazioni

Le attività da svolgere sono di seguito riportate:

1) predisporre un documento, approvato del RTD, che indichi la configurazione standard e le policy di dominio con la quale tutte le postazioni PC vengono create e gestite;
2) predisporre e mantenere aggiornata la configurazione base da installare sui PC e Server;
3) verificare e garantire il corretto funzionamento dei Sistemi di autenticazione e profili utenti (password, id, profilo utente, etc.);
4) mantenere aggiornato un documento in cui indicare la lista del software autorizzato dal comune, a partire dai sistemi operativi, il software installato sulle postazioni di lavoro ad uso del personale tecnico amministrativo;
5) assicurare la continua e tempestiva installazione degli aggiornamenti del software di base dei PC e dei Server, delle basi dati, della Posta elettronica, Antivirus, ecc.;
6) implementare e mantenere aggiornato un riepilogo inventariale (hardware e software installato) di tutte le PdL (sia desktop che portatili) e i server windows presenti nella rete del comune;
7) eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato, documentando il risultato;
8) ...
9) ...

PRIORITÀ DELLE PRIORITÀ

AGID | Agenzia per l'Italia Digitale

Il Manuale contiene un capitolo «Piano di Sicurezza» Art. 3.8 «Linee Guida sulla formazione, gestione e conservazione dei documenti informatici«

Linee Guida sulla formazione, gestione e conservazione dei documenti informatici

ADOZIONE DEI MANUALI DI GESTIONE DOCUMENTALE E CONSERVAZIONE

FORMAZIONE E REVISIONE DEI PROCEDIMENTI (REINGEGNERIZZAZIONE)

FORMAZIONE AL PROTOCOLLO (PROCESSI DI SCANSIONE, CORRETTO UTILIZZO DELLA TITOLAZIONE)

FASCICOLAZIONE DIGITALE

TEMPI DA SUBITO: ENTRO IL 2024

Le MMS sono anche richiamate nelle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici (AgID)

Misure di sicurezza

… le Pubbliche Amministrazioni sono tenute ad ottemperare alle misure minime di sicurezza ICT emanate dall'AgID con circolare n. 2/2017.

In tale ottica, **il responsabile della gestione documentale…**, …in accordo con il **responsabile della conservazione… … con il responsabile per la transizione digitale** e **acquisito il parere del responsabile della protezione dei dati personali**…

predispone **il piano della sicurezza del sistema di gestione informatica dei documenti**

prevedendo opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio in materia di protezione dei dati personali, ai sensi dell'art. 32 del Regolamento UE 679/2016 (GDPR)39, anche in funzione delle tipologie di dati trattati, quali quelli riferibili alle categorie particolari di cui agli artt. 9-10 del Regolamento stesso.

Il Regolamento per la sicurezza delle informazioni

Definisce le regole (compiti e responsabilità di tutto il personale) previste per mitigare i rischi per la sicurezza delle informazioni nonché per assicurare un corretto utilizzo degli strumenti informatici messi a disposizione da parte del Comune. Prevede opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio in materia di protezione dei dati personali.

Il Regolamento per la sicurezza delle informazioni

Indice

La politica di “Scrivania pulita” e “Schermo pulito”

D.lgs. 82/2005 art. 51 (CAD)

- Scrivania pulita
  - Ove possibile, carta e supporti informatici devono essere conservati in apposite casseforti, armadi o altre forme di protezione quando non sono in uso, soprattutto al di fuori dell'orario di lavoro.
  - Le porte delle aree di ufficio devono essere chiuse a chiave quando non sono in uso o non sono vigilate.
  - Informazioni riservate, sensibili o classificate, una volta stampate, devono essere rimosse immediatamente dalle stampanti.

  Questa politica è particolarmente importante quando si tratta di documenti contenenti dati sensibili
- Schermo pulito
  - Gli utenti devono sempre “log-off”(disconnettersi), quando lasciano il computer incustodito.
  - Impostare il Blocco schermo di Windows affinché si attivi automaticamente quando non vi è alcuna attività per un breve predeterminato periodo di tempo.
  - Il Blocco schermo di Windows deve essere protetto da password per la riattivazione

Piano di continuità operativa

L'art. 64 del D.lgs. n. 179/2016 ha abrogato l'art. 50-bis del CAD ("Continuità operativa") che prevedeva:

«…le pubbliche amministrazioni predispongono i piani di emergenza in grado di assicurare la continuità delle operazioni indispensabili per il servizio e il ritorno alla normale operatività.

A tali fini, le pubbliche amministrazioni definiscono:

a) il piano di continuità operativa, che fissa gli obiettivi e i principi da perseguire, descrive le procedure per la gestione della continuità operativa, anche affidate a soggetti esterni. Il piano tiene conto delle potenziali criticità relative a risorse umane, strutturali, tecnologiche e contiene idonee misure preventive. Le amministrazioni pubbliche verificano la funzionalità del piano di continuità operativa con cadenza biennale

b) il piano di disaster recovery, che costituisce parte integrante di quello di continuità operativa di cui alla lettera a) e stabilisce le misure tecniche e organizzative per garantire il funzionamento dei centri di elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione.»

Piano di continuità operativa

Tuttavia, a ben guardare, il tema della continuità operativa è ancora presente nell'art. 51 del Codice dell'Amministrazione Digitale che al comma 1 parla di "soluzioni tecniche idonee a garantire la protezione, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati **e la continuità operativa dei sistemi** e delle infrastrutture"; inoltre, il comma 2 dice che "I documenti informatici delle pubbliche amministrazioni devono essere custoditi e controllati con modalità tali da **ridurre al minimo i rischi di distruzione, perdita**, accesso non autorizzato o non consentito o non conforme alle finalità della raccolta".

Inoltre, l'art. 32 del GDPR così recita: "… il titolare del trattamento e il responsabile del trattamento devono mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono tra l'altro, se del caso … … **la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico…»**

Rimane dunque l'imposizione di garantire la continuità dei sistemi ma le P.A. possono svilupparla e gestirla in autonomia

Piano di continuità operativa

Il Piano è diviso in due sezioni

1. I componenti del Sistema Informatico gestiti in Cloud;
    - Le clausole contrattuali
2. I componenti del Sistema informatico residente in loco

Infine, la formazione dei dipendenti è la migliore difesa dei sistemi informatici

PRIMO PIANO - 12/02/2024

Campagna phishing a tema "Helpdesk Support"

È stato rilevato il riacutizzarsi di una campagna di phishing - a tema "Helpdesk Support" - volta a carpire le credenziali utente delle potenziali vittime [...]

LEGGI DI PIÙ →

AgID - Piano triennale Informatica 2024-2026 - obiettivo 7.5

Promuovere attività legate al miglioramento della cultura *cyber* delle Amministrazioni.

Grazie per la Vostra attenzione

David Harris

dharris.sassari@gmail.com

PROGRAMMA OPERATIVO COMPLEMENTARE

Agenzia per la Coesione Territoriale

Presidenza del Consiglio dei Ministri
Dipartimento della Funzione Pubblica

FAST PICCOLI COMUNI È UN PROGETTO FINANZIATO
DAL PROGRAMMA OPERATIVO COMPLEMENTARE AL
PON "GOVERNANCE E CAPACITÀ ISTITUZIONALE" 2014-2020