ACCREDIA L'Ente Italiano di Accreditamento

Convegno di aggiornamento e studio
«Dipartimento Certificazione e Ispezione di Accredia»

"Cybersecurity act e schemi IT"

Riccardo Bianconi
ACCREDIA, Ispettore

ACCREDIA - Milano
2020 Gennaio 14

"Cybersecurity Act" e schemi IT

Aspetti Generali

- Di cosa parliamo
- Come vanno le cose

Cybersecurity

- Di che si tratta?
- Direttive e Leggi nazionali

Schemi di Certificazione

- Organizzazioni
- Persone
- Servizi
- E poi?

Aspetti Generali

- Di cosa parliamo
- Come vanno le cose

Austria, attacco informatico da Paese straniero

Dopo ok Verdi a nuovo governo.

Interferenze ancora in corso

© *ANSA/EPA*

05 Gennaio 2020

"Cybersecurity Act" e schemi IT

Così la Cina si prepara alla guerra (cyber) del futuro

Nel suo nuovo Libro Bianco della Difesa, Pechino non nasconde le ambizioni di costruire u esercito moderno e tecnologicamente avanzato, in grado di sfidare gli Usa e di essere all'avanguardia anche nel quinto dominio. Numeri e scenari

I conflitti stanno evolvendo in 'guerra intelligente', abilitata dalle possibilità offerte da un u sapiente dello spazio cibernetico. E la Cina, che oggi conta sul secondo più grande budget r (+ 7,5% nel 2019) anche se ancora molto indietro rispetto agli Stati Uniti, sta puntando mol quello che considera il dominio che più in fretta potrebbe consentirle di colmare il gap con Washington.

IL NUOVO LIBRO BIANCO DELLA DIFESA

Nel nuovo Libro Bianco della Difesa pubblicato oggi, Pechino non nasconde le sue ambizio costruire un esercito moderno e tecnologicamente avanzato, in un quadro contraddistinto da crescente uso di intelligenza artificiale, i big data, l'IoT, il cloud e il quantum computing.
Il testo è in inglese, cosa che non accade per tutti i documenti cinesi: un dettaglio simbolico che rende chiara la volontà di comunicare il messaggio soprattutto all'esterno.
E la 'missiva' non lascia spazio a fraintendimenti. La terminologia impiegata spicca per contrasto con quella utilizzata nell'ultimo paper analogo, pubblicato nel 2015, in cui Pechino sottolineava la necessità di aumentare la cooperazione sul piano militare tra le due grandi potenze mondiali. In questo, invece si accusano gli Stati Uniti di "minare la stabilità strategica globale", proprio mentre la rivalità tra Pechino e Washington si intensifica su molti fronti, compreso quello cyber, nel quale gli Usa denunciano da tempo l'espansionismo e l'aggressività del gigante asiatico.

China's National Defense in the New Era

The State Council Information Office of
the People's Republic of China

July 2019

First Edition 2019

"Cybersecurity Act" e schemi IT

UK is nearly ready to launch force to hit hostile countries with cyberattacks

The specialist unit will be dedicated solely to offensive action to combat security threats, extremism, hackers, disinformation and election interference

Kim Sengupta Defence Correspondent | 1 day ago | 105 comments

"Cybersecurity Act" e schemi IT

TECH NEWS

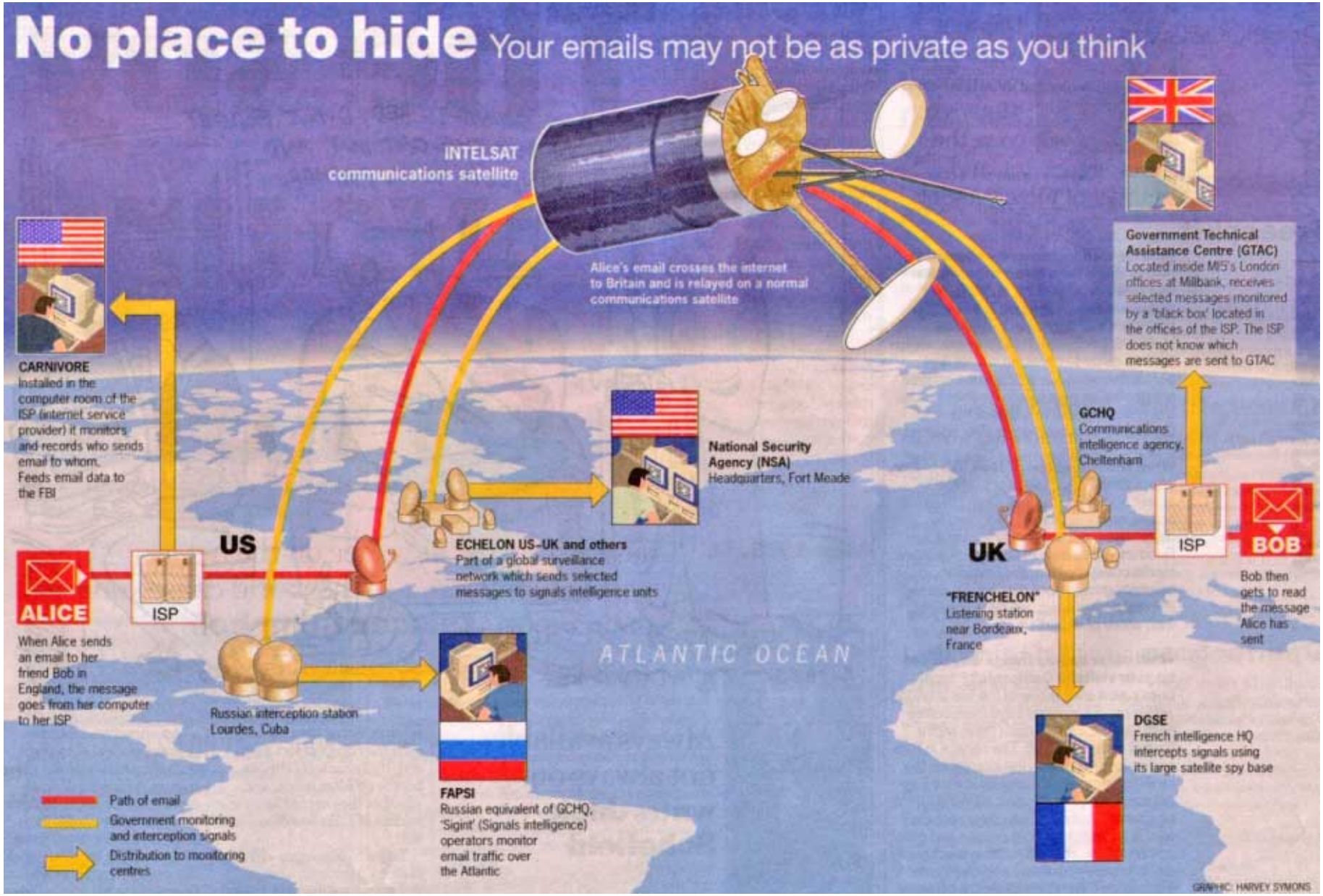
Attacchi hacker dagli Stati Uniti, l'Italia tra i Paesi più colpiti

Il gruppo hacker Shadow Broker rivela nuovi dati sull'attività della NSA. Nel nostro Paese presi di mira istituti universitari e di ricerca

C'è anche **l'Italia** nella *top 10* dei **Paesi maggiormente colpiti dagli hacker della NSA** (acronimo di *National Security Agency*), l'agenzia per la sicurezza nazionale degli Stati Uniti salita più volte agli onori della cronaca per le varie operazioni di pirateria informatica condotte a livello internazionale.

"Cybersecurity Act" e schemi IT

"Cybersecurity Act" e schemi IT



"Cybersecurity Act" e schemi IT

Cyberattacco a Libero e Virgilio Mail: rubate 1,4 milioni di password

Condividi questo articolo

L'intrusione ad opera di un hacker 24enne effettuata in un bar di Assago proprio a fianco alla sede di Italiaonline. Indagano la procura di Milano e il Garante Privacy

24 Apr 2019

Oltre un milione di credenziali di accesso alle caselle di posta elettronica di altrettanti utenti, clienti di **Libero Mail** e **Virgilio Mail**, sono finite nella mani di un **hacker** 24enne.

L'operazione sarebbe avvenuta in un bar di Assago, non lontano dagli uffici di Italiaonline. La notizia è riportata dal Corriere della Sera che racconta di un attacco veloce ed efficace, messo a punto con l'uso di un computer portatile e di una grande antenna; 1,4 milioni di dati sarebbero poi stati inviati a presunti committenti che però sono ancora ignoti. Il contatto tra il giovane hacker e i mandanti del colpo sarebbe avvenuto tramite Telegram e le due parti avrebbero concordato il pagamento in bitcoin.

L'hacker 24enne è entrato nelle rete Wifi di Italiaonline, che gestisce gli account di posta Libero e Virgilio, usando la password di un dipendente per sferrare l'attacco.

MENU | CERCA — la Repubblica — R+ | Rep: | ABBONATI

Economia&Finanza — Seguici su — Ricerca titolo

HOME | MACROECONOMIA | FINANZA | LAVORO | DIRITTI E CONSUMI | AFFARI&FINANZA | OSSERVA ITALIA | CALCOLATORI | GLOSSARIO | LISTINO | PORTAFOGLIO

Unicredit, attacco informatico: violati i dati per 3 milioni di utenti nel 2015. "Nessun accesso ai conti"

La nota della banca: "Accesso non autorizzato a nome, città, numero di telefono e indirizzo email. Non compromessi altri dati sensibili"

"Cybersecurity Act" e schemi IT

Hackers Can Silently Control Your Google Home, Alexa, Siri With Laser Light

November 05, 2019 Mohit Kumar

A team of cybersecurity researchers has discovered a clever technique to remotely inject inaudible and invisible commands into voice-controlled devices — all just by shining a laser at the targeted device instead of using spoken words.

L'AgID e gli attacchi hacker via PEC ed email da parte del malware FTCODE

Negli ultimi mesi **l'AgID, Agenzia per l'Italia Digitale**, sta fornendo una serie di indicazioni del CERT-PA, team facente parte dell'AgID, volte ad informare e fornire soluzioni di prevenzione riguardo **campagne hacker** del **malware FTCODE**. Il bollettino AgID sulla sicurezza informatica riguardanti email e PEC ha al centro questo nuovo software malevolo che a partire da settembre sta infettando diverse **PEC** e caselle **email** della Pubblica Amministrazione, aziende, professionisti italiani.

Il malware FTCODE

Alla prima versione del FTCODE, un *ransomware*, un software che cattura i dati degli utenti criptando i file e rendendoli inutilizzabili da parte dell'utente, si è aggiunta la funzione di *info-stealer* in quanto in grado di catturare i dati personali dell'utente quali password e cookie. Colpisce *sistemi Window e più recentemente Android.*

La particolare pericolosità deriva dal fatto che il mittente della mail sembra attendibile, in quanto è lo stesso con cui la vittima ha avuto una conversazione precedente via email. Gli ultimi attacchi sono infatti caratterizzati dall'invio di una *email con unico link* il cui testo è preso da una precedente conversazione con il mittente. Tale link punta a un *file compresso zip con dentro un file VBS.* Una volta scaricato e eseguito il file si innesca l'infezione, vengono criptati dati e rubate password personali.

Cyberattacks against industrial targets have doubled over the last 6 months

12,000 workstations on average will be damaged in cases of destructive malware.

Charlie Osborne for Zero Day | August 5, 2019

Aspetti Generali

- Di cosa parliamo
- Come vanno le cose

Possiamo prendere in esame i rapporti predisposti

dalla Commissariato di P.S. online – Sportello per la sicurezza degli utenti del web [riferito al 2019]

e

da Clusit – Associazione Italiana per la Sicurezza Informatica [riferito al 2019, con storicità]

"Cybersecurity Act" e schemi IT

Oltre 82.000 segnalazioni su possibili attacchi diramati alle infrastrutture critiche nazionali
[+ 30% sul 2018]

Gestiti 1.186 attacchi dei quali 243 verso siti istituzionali, 938 di aziende e PA locali.

155 Inchieste, con sequestri di piattaforme utilizzate per sorveglianza illecita e sottrazione di credenziali da grandi database pubblici.

Forte incremento episodi di Phishing, truffe in e-commerce e trading (196.000 segnalazioni)

Denunciati 4.930 casi di crimini cyber-finanziari.

Con il rapporto 2019 viene evidenziato un aumento sostanziale delle attività criminali(+ 79%) finalizzate a sottrarre denaro ad aziende e privati (esempio tramite uso di ransonware e richieste di riscatto)

Viene registrato un aumento significativo dei casi di spionaggio industriale (+ 57%) per sottrazione informazioni di business.

Pressoché raddoppiato (+ 99%) il furto di dati personali.

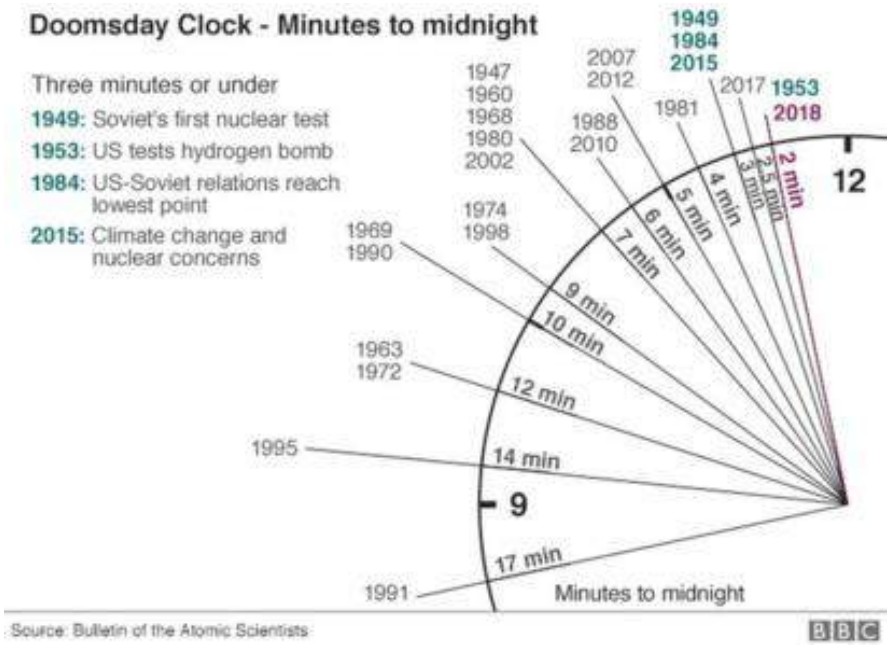
Andamento, rispetto al 2018, degli attacchi a:

PA incremento di oltre il 40%
Istituzioni finanziarie + 33%
Centri di ricerca + 55%
Infrastrutture Cloud + 37%

Nell'ultimo biennio il tasso di crescita del numero di attacchi gravi è aumentato di 10 volte rispetto al precedente. Non solo, la "Severity" media di questi attacchi è contestualmente peggiorata, agendo da moltiplicatore dei danni.

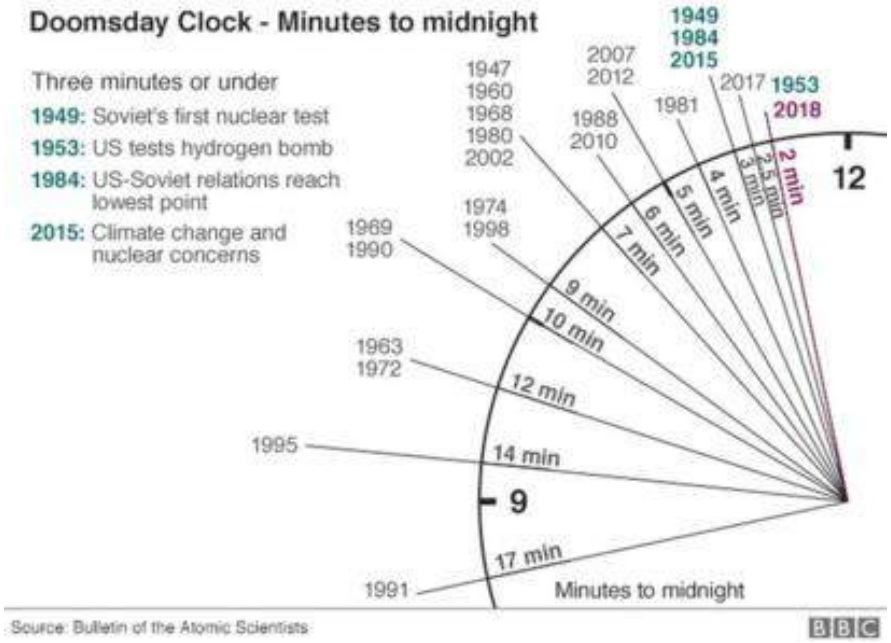
Per meglio illustrare il trend, Clusit sceglie la metafora del

"*Doomsday Clock*"



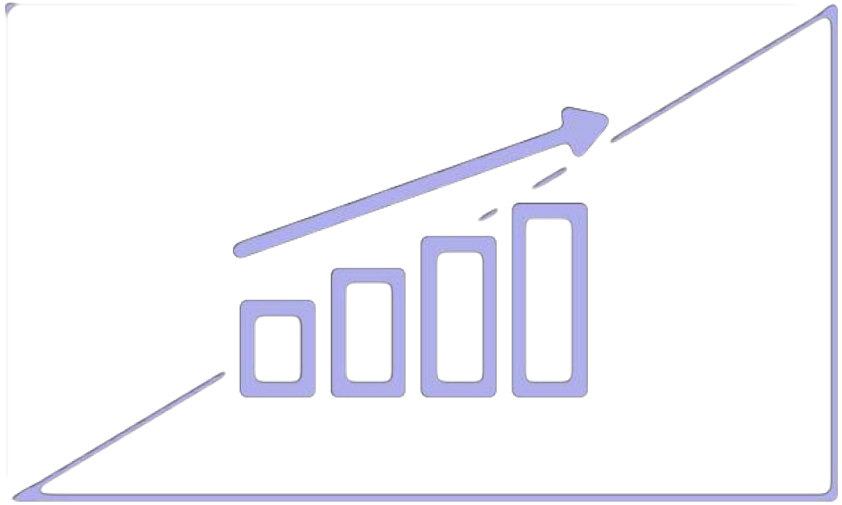
L'orologio metaforico ideato nel 1947 dagli scienziati della rivista Bulletin of the Atomic Scientists dell'Università di Chicago, in cui la mezzanotte simboleggia la fine del mondo, ed i minuti di distanza da essa la probabilità dell'apocalisse nucleare

"*Doomsday Clock*"



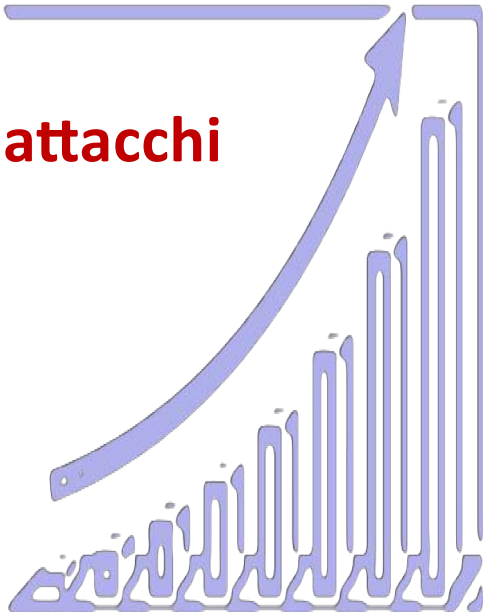
"Perché affermare che ci troviamo ormai a “due minuti dalla mezzanotte”? In sintesi, perché crediamo che **le tendenze che stiamo osservando non possano continuare ancora a lungo senza determinare un qualche genere di discontinuità**, di rottura (anche se non abbiamo modo di sapere come questa si concretizzerà) e che lo *stress* ancora sopportabile dal sistema sia limitato".

Osservando la situazione dal punto di vista quantitativo, a parità dei criteri di selezione e classificazione che applichiamo al nostro campione (aggiornati nel 2014 e mantenuti invariati da allora) nel quinquennio 2014 - 2018 la crescita degli attacchi gravi è stata del **+77,8%**



Mentre nell'arco del biennio 2017-2018 (con un'accelerazione sensibile nell'ultimo anno) il numero di attacchi gravi è cresciuto del **+37,7%**

Si prospetta un cambiamento di passo degli attacchi



Cyber Guerriglia permanente

Cyber Spionaggio

Cyber Sabotaggio e Cyber Terrorismo

Incremento delle conoscenze di AI e Machine Learning

Calcolatori sempre più performanti

Surveillance Capitalism…. [GDPR e analisi del Prof. Pizzetti]

"Cybersecurity Act" e schemi IT

Cybersecurity

- Di che si tratta?
- Direttive e Leggi nazionali

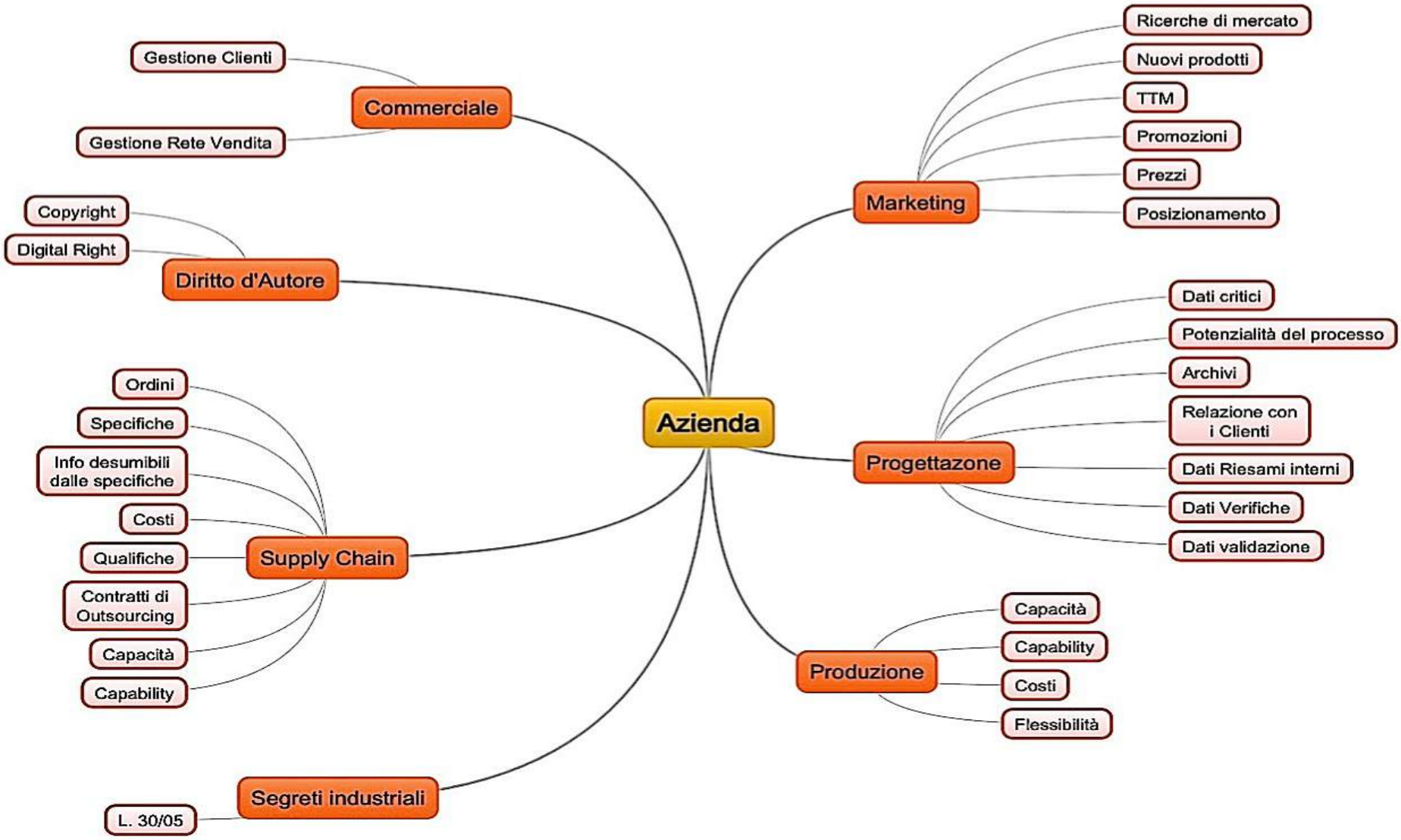
Cosa è la "CyberSecurity"?

"**Sicurezza delle Informazioni**"

La sicurezza delle Informazioni è una disciplina ampia, relativa allo studio delle possibili minacce verso le infrastrutture ICT e, in particolare, verso dati e informazioni ivi contenute e gestite o, per il loro tramite, trasmesse al fine di:

Preservare la **"riservatezza, integrità e disponibilità"** di tali dati e informazioni correlate.

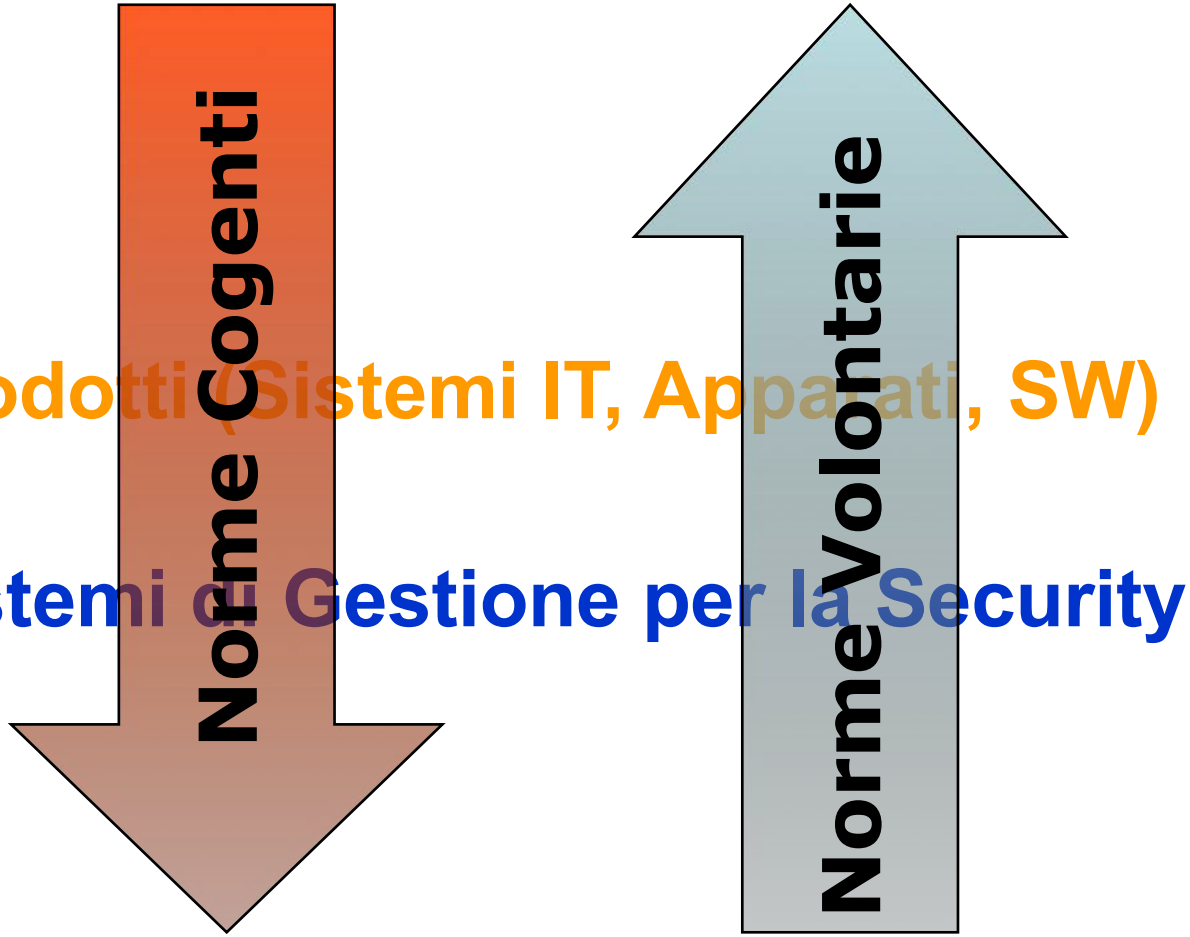
"Cybersecurity Act" e schemi IT



Prodotti (Sistemi IT, Apparati, SW)

Sistemi di Gestione per la Security

"Cybersecurity Act" e schemi IT



Prodotti (Sistemi IT, Apparati, SW)

Sistemi di Gestione per la Security

Cybersecurity

- Di che si tratta?
- Direttive e Leggi nazionali

"Cybersecurity Act" e schemi IT

D. Lgs 518/92 (L. 633/41)

L. 547/93

L. 248/00 (L. 633/41)

D. Lgs. 231/01 e smi

Reg. 338/01 (S.I.A.E)

D. Lgs. 262/05 (tutela del risparmio)

L. 48/2008 Vs D. Lgs 231/01

Direttiva UE 2016/943 e D.Lgs. 11.05.2018 n.63 (segreto ind.)

[Ex D. Lgs. 30/05 (Art. 98)]

D. Lgs 70/2003 (Artt. 14 e segg.)

D. Lgs 82/05 (Ammin. Digit.) e smi

D. Lgs. 235/2010 (Ammin. Digit. Artt. 50 e 51)

Regolamento UE 910/2014 eIDAS e correlati

Regolamento (UE) 679/2016 e D. Lgs. 101_2018

L. 12/2012 (contrasto alla criminalità ICT)

Raccolta provvedimenti AgID per SPID e Conservazione a Norma

Direttiva (UE) 2016/1148 "NIS"

Sicurezza Nazionale Cibernetica D Lg. 105/2019 e legge di conversione 18 novembre 2019, n. 133

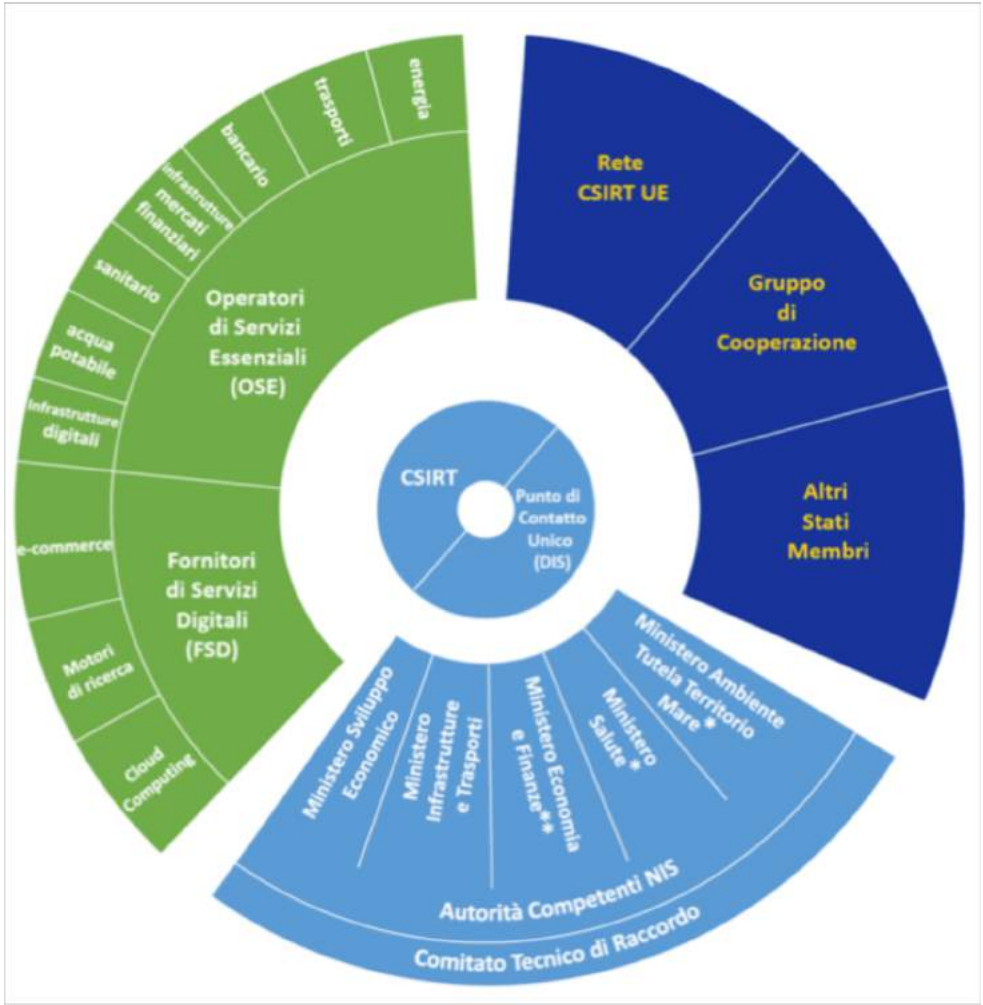
e Milleproroghe 2020 [D. Lgs. 162/2019] - Art. 27 e segg.

NIS [Livello Europeo]

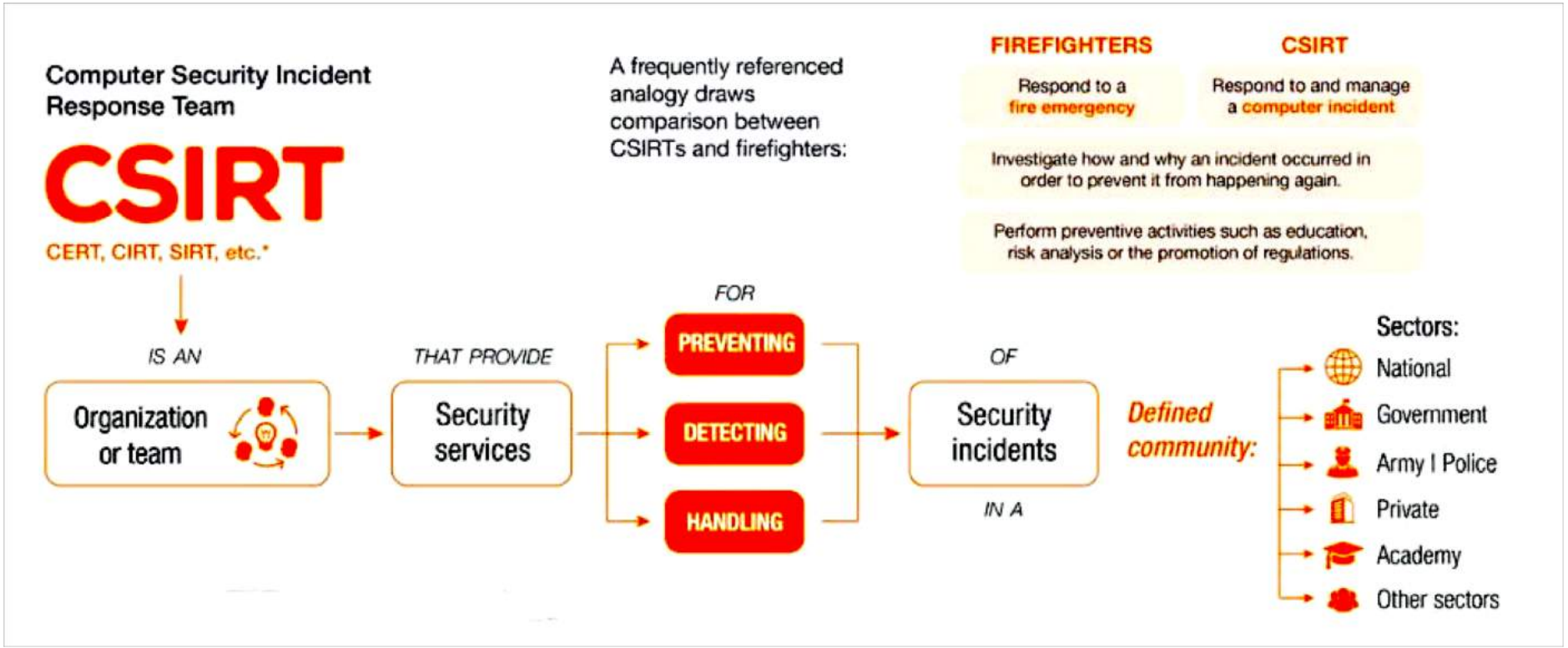
Definito il ruolo di ENISA come centro di coordinamento.

NIS [Livello Europeo]

Definizione dell'architettura di sicurezza per i servizi essenziali e operatori ICT a livello sovrannazionale.



"Cybersecurity act" e schemi IT



Sulla scorta di tale architettura è stata definito il cosiddetto

PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA

D. LGS. 105/2019 [21 Settembre]

Convertito nella Legge 133 [18 Novembre]

Sostanzialmente emendato con il D. Lgs. 162/2019, cosiddetto "milleproroghe 2020"

Art. 27 … "sono individuate le amministrazioni pubbliche e gli eneti pubblici o privati" → **"sono definiti modalità e criteri procedurali di individuazione delle…"**

"Cybersecurity act" e schemi IT

Il fine del provvedimento è quello di:

Assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori nazionali, pubblici e provati, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale.

2-bis. L'elencazione dei soggetti individuati ai sensi del comma 2, lettera a), e' contenuta in un atto amministrativo, adottato dal Presidente del Consiglio dei ministri, su proposta del *CISR [Centro Interministeriale per la Sicurezza della Repubblica*], entro trenta giorni dalla data di entrata in vigore del decreto del Presidente del Consiglio dei ministri di cui al comma 2.

Il predetto atto amministrativo, per il quale è escluso il diritto di accesso, non è soggetto a pubblicazione, fermo restando che a ciascun soggetto è data, separatamente, comunicazione senza ritardo dell'avvenuta iscrizione nell'elenco.

L'aggiornamento del predetto atto amministrativo è effettuato con le medesime modalità di cui al presente comma.

"Cybersecurity act" e schemi IT

Queste entità dovranno aggiornare annualmente l'elenco dei propri "asset" critici, compresi i servizi informatici esterni.

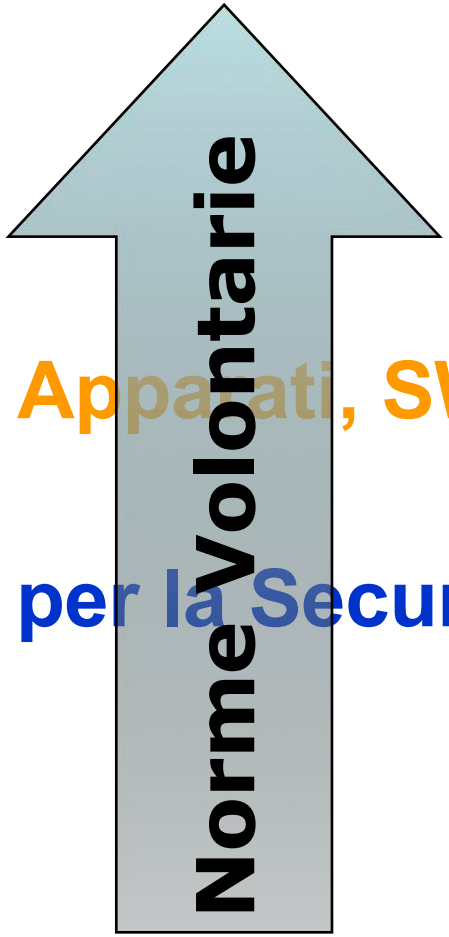
Le PA o Enti pubblici le comunicheranno alla Pres. Cons. Ministri; i privati al MISE.

Ove tali entità si avvalgano di servizi esterni, per le finalità definite dal provvedimento, oppure debbano acquisire componenti critici per tali infrastrutture, dovranno darne comunicazione preventiva al **CVCN** [da istituire entro 6 mesi dall'entrata in vigore del provvedimento] che sarà il Centro di Valutazione e Certificazione Nazionale. Questo potrà, **entro 30 gg, imporre test preventivi di sicurezza su tali "asset"**… (c'è da chiedersi se tali test dovranno essere fatti anche sulla loro integrazione, sulle biblioteche di sviluppo SW, sulle persone che operano e sanno… di tali attività, anche in funzione di cosa sanno…).

"Cybersecurity act" e schemi IT

Gli obblighi di comunicazione da parte dei soggetti interessati sono definiti come principio di prima linea, ma non è stata ancora definita la normativa specifica che indichi con dettaglio: che cosa, come e quando notificare.

Le sanzioni sono pesanti e riguardano anche la sfera penale, non ultimo con riferimento al D. Lgs. 231/01, seppure con sanzioni solo pecuniarie, per motivi fin troppo ovvi.



Prodotti (Sistemi IT, Apparati, SW)

Sistemi di Gestione per la Security

Schemi di Certificazione

- Organizzazioni
- Persone
- Servizi
- E poi?

"Cybersecurity Act" e schemi IT

Famiglie:

27001:2013
20000-1:2018
22301:2019

NIST National Institute of Standards and Technology

Cybersecurity Framework Release 1.1

ISACA COBIT 2019

27001:2013 (beh!)

- A.5 Politiche per la sicurezza delle informazioni
- A.6 Organizzazione della sicurezza delle informazioni
- A.7 Sicurezza delle risorse umane
- A.8 Gestione degli asset
- A.9 Controllo degli accessi
- A.10 Crittografia
- A.11 Sicurezza fisica ed ambientale
- A.12 Sicurezza delle attività operative
- A.13 Sicurezza delle comunicazioni
- A.14 Acquisizione, sviluppo e manutenzione dei sistemi
- A.15 Relazioni con I fornitori
- A.16 Gestione degli incidenti relative alla sicurezza delle informazioni
- A.17 Sicurezza delle informazioni nella gestione della business continuity
- A.18 Compliance

Schemi di Certificazione

- Organizzazioni
- Persone
- Servizi / Prodotto
- E poi?

"Cybersecurity Act" e schemi IT

27021 (professionisti ISMS)

11506 e **11621**

Professionisti ambito:
- IT,
- WEB e
- ICT Security

11697

Professionisti: per la Data Protection

Schemi di Certificazione

- Organizzazioni
- Persone
- Servizi / Prodotto
- E poi?

"Cybersecurity act" e schemi IT

International Organization for Standardization

19011 - Audit

"Cybersecurity act" e schemi IT

62334 (spec. 3 e 4)

15408 OCSI e Ce.Va.

Schemi di Certificazione

- Organizzazioni
- Persone
- Servizi
- E poi?

"Cybersecurity Act" e schemi IT

ACCREDIA
L'ENTE ITALIANO DI ACCREDITAMENTO

Circolare n. 1/2019/DL Roma, 28 febbraio 2019

A tutti i Laboratori di Prova accreditati/in corso di accreditamento
Loro sedi

A Ispettori/Esperti tecnici ACCREDIA DL operanti nel settore dei Vulnerability Assessments (VA)
Loro sedi

Oggetto: Circolare informativa DL n. 1/2019 - Informazioni relative all'accreditamento di Laboratori di prova operanti nel settore dei Vulnerability Assessments (VA)

Grazie per l'attenzione

www.accredia.it

info@accredia.it

Dipartimento Certificazione e Ispezione

Dipartimento Laboratori di prova

Dipartimento Laboratori di taratura