## Ciclo di webinar in diretta

# Sicurezza informatica & Protezione dei dati negli enti locali

## La cybersecurity awareness nella pubblica amministrazione locale

## 25-01-2024

Relatore: Dottor Antonio Guzzo Funzionario Informatico Agenzia delle Entrate

Cyber security expert

DPO CERTIFIED ISO IEC 17024 e UNI 11697:2017

ASMEL - Associazione per la Sussidiarietà e la Modernizzazione degli Enti Locali
Email info@dpoinrete.it
Numero Verde 800.16.56.54 (int.3)
Web: www.dpoinrete.it, www.asmel.eu


# Indice

- **Definizione di cybersecurity awareness (regolamento UE 2841/2023)**
- **Gli elementi**
- **Gli obiettivi**
- **The NIST Cybersecurity Framework 2.0**
- **CISA Cybersecurity Awareness Program**

# CYBERSECURITY AWARENESS

- Con il termine cybersecurity awareness si fa riferimento alla consapevolezza e comprensione delle minacce informatiche, costituendo un elemento cruciale nell'arsenale difensivo di un'organizzazione
- La traduzione letterale dell'espressione “cyber security awareness” rimanda al concetto di consapevolezza di quelle che sono le caratteristiche, i contenuti e le criticità della sicurezza IT all'interno delle strutture aziendali.

# CYBERSECURITY AWARENESS

- Il concetto di cybersecurity awareness è strettamente correlato al concetto di governance per la sicurezza che viene per la prima volta introdotto con il regolamento UE sulla cybersicurezza approvato il 13-12-2023 n° 2841/2023

# CYBERSECURITY AWARENESS

- (6) Per raggiungere un livello comune elevato di cibersicurezza, è necessario che ogni soggetto dell'Unione istituisca un quadro interno di gestione, governance e controllo dei rischi per la cibersicurezza («quadro»), che garantisca una gestione efficace e prudente di tutti i rischi per la cibersicurezza e tenga conto della continuità operativa e della gestione delle crisi. Il quadro dovrebbe stabilire politiche in materia di cibersicurezza, comprensive di obiettivi e priorità, per la sicurezza dei sistemi informativi e di rete che costituiscono la totalità dell'ambiente TIC non riservato. Il quadro dovrebbe basarsi su un approccio multirischio che miri a proteggere i sistemi informativi e di rete e il loro ambiente fisico da eventi quali furti, incendi, inondazioni, problemi di telecomunicazione o interruzioni di corrente, o da qualsiasi accesso fisico non autorizzato nonché dai danni alle informazioni detenute dai soggetti dell'Unione e ai loro impianti di trattamento delle informazioni e dalle interferenze con tali informazioni o impianti che possano compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi, trattati o accessibili tramite i sistemi informativi e di rete.

# CYBERSECURITY AWARENESS

- I continui e frequenti attacchi cyber che si sono succeduti da marzo 2020 in poi con l'utilizzo sempre più massivo e pervasivo dei device collegati alla rete, in primis fra tutti gli smartphone, device ad oggi sempre più pervasivi ed ubiqui, hanno evidenziato con l'avvento della pandemia da covid 19 le debolezze e le vulnerabilità nel nostro paese in termini di cultura alla cyber security awareness. Oggi la consapevolezza e la percezione da parte delle aziende, degli enti pubblici e cittadini in generale sul cyber risk, dopo l'avvento della pandemia è sempre più forte, ma ha evidenziato le carenze di natura formativa, a livello generale, degli strumenti di prevenzione alla cybersecurity.

# CYBERSECURITY AWARENESS

- L’istituzione con la legge 4 agosto 2021 n° 109 della neonata Agenzia Nazionale sulla Cybersecurity ha testimoniato come l’attenzione su queste tematiche sia massima da parte del legislatore, anche se ha evidenziato come il sistema di istruzione italiano sia altamente carente in termini di prevenzione agli attacchi cyber sin dalle scuole primarie, dove i fenomeni di cyber bullismo dominano la scena nazionale. Oggi termini come *insider threats* (minacce interne), phishing, ransomware, malware, supply chain attacks (attacchi alla catena dell’offerta), sono ignari alla stragrande maggioranza dei dipendenti pubblici, mentre pian piano nelle aziende si sta sempre più investendo in formazione sul cyber risk ai dipendenti. Il sistema scolastico sin dalle scuole primarie non investe in tal senso creando un gap in termini di *digital divide* in ambito cyber.

# CYBERSECURITY AWARENESS

- Oggi tutte le tutte le organizzazioni sono vulnerabili a qualsivoglia tipologia di cyber attack da parte dei dipendenti che possono utilizzare il proprio accesso autorizzato a strutture, persone o informazioni per danneggiare la propria organizzazione, intenzionalmente o meno. Il danno può variare da comportamenti connotati da negligenza, come la mancata protezione dei dati o il clic su un collegamento di *spear-phishing*, ad attività consapevolmente dannose come il sabotaggio, il furto della proprietà intellettuale, la frode sul posto di lavoro, ecc. Proprio per questo che la minaccia umana è divenuta, pertanto, un elemento significativo nell'attuale panorama delle minacce cibernetiche e, da un punto di vista organizzativo e gestionale, un problema collegato è divenuto quello su come incorporare questi vettori di minacce nei piani di gestione del rischio organizzativo al fine di mitigare le minacce interne.

# CYBERSECURITY AWARENESS

- Oggi le nuove generazioni non hanno consapevolezza di quali minacce possa creare l'utilizzo del proprio *device* in termini di accesso alla rete e non hanno minimamente contezza del rischio di tracciabilità mediante gli identificativi che lo stesso *device* genera (MC Address, Indirizzo IP, etc).
- Oggi come oggi un potenziale attaccante ha un proprio profilo motivazionale che lo spinge a compiere attacchi sulla rete come il *data leak* che consiste nella mera esfiltrazione di dati e le motivazioni che lo spingono sono di natura finanziaria, di spionaggio (il cd. *espionage*), di puro divertimento (*fun*), di *hactivism*, di *resource theft* ed altre.

# CYBERSECURITY AWARENESS

- Sarebbe opportuno che il sistema scolastico educhi le nuove generazioni a sessioni formative sin dalle scuole primarie con appositi training in ambito normativo ( rendere edotte le nuove generazioni quali sono i rischi legali sui cd computer's crimes con approfondimenti sulla legge 48/2008 che disciplina i reati informatici), tecnologico con l'applicazione del Nist Cyber security framework a tutte le organizzazioni nonchè l'applicazione dello standard ISO 27001, il cd global cyber security standard.
- Oggi la pa italiana, grazie anche alla spinta del Piano Nazionale di Ripresa e Resilienza, sta muovendo i primi passi in tal senso ma la mancanza diffusa di competenze IT, mescolata ad una scarsa formazione in tal senso sta rendendo la nostra pa estremamente vulnerabile al cyber risk con evidenti danni reputazionali notevoli al sistema pubblico, derivanti nella stragrande maggioranza da errori umani per mancata e scarsa formazione al dipendente pubblico. Ciò è ancor più vero nella situazione pandemica attuale, in cui bisogna tener, nel debito conto, gli aspetti psicologici a cui è stata sottoposta la forza lavoro remotizzata derivante dallo smart working massiccio.

# GLI ELEMENTI

- **Il framework NIST copre cinque funzioni fondamentali: identificazione, protezione, rilevamento, risposta e recupero.**
- Identificazione. Identificare **quali** risorse devono essere protette è fondamentale per le aziende. ...
- Protezione. ...
- Rilevamento. ...
- Risposta. ...
- Recupero.

# GLI OBIETTIVI

- -Ridurre il numero di errori accidentali.
- Individuare nuove soluzioni moderne di cybersecurity (ad esempio, per la sostituzione delle password)
- Migliorare la cultura interna ed elevare il morale delle persone.
- Ridurre perdite di tempo e costi legati agli incidenti.

# NIST II CYBERSECURITY FRAMEWORK

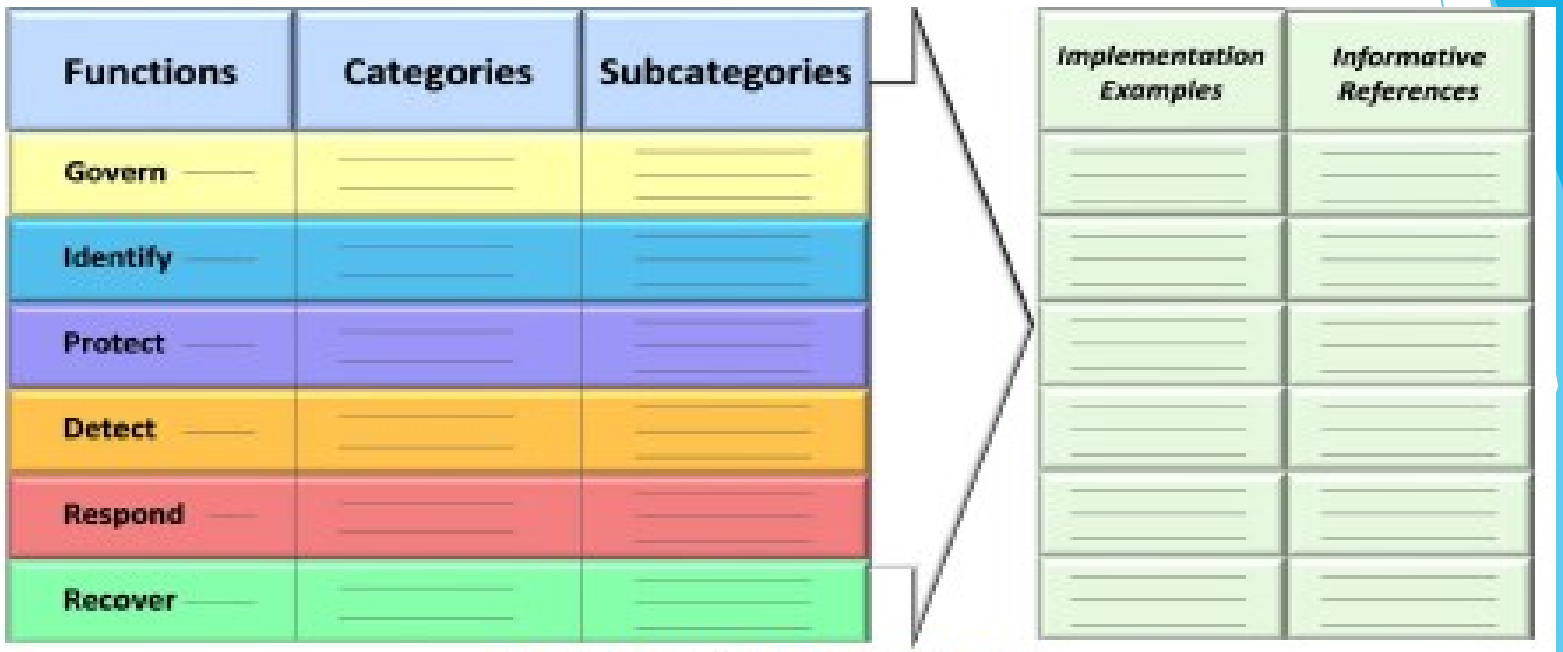


Fig. 1. Cybersecurity Framework Core

# NIST II CYBERSECURITY FRAMEWORK

Il CSF si basa sulla gestione del rischio informatico e considera 5 classi di attività o “Functions” che devono integrarsi in modo sequenziale per identificare, gestire e reagire ai rischi ed agli attacchi cyber.

Le 5 funzioni – rappresentate con cinque colori diversi – sono:
ID Identify (identificare)
PR Protect (proteggere)
DE Detect (indagare)
RS Respond (reagire)
RC Recover (riparare)

# NIST II CYBERSECURITY FRAMEWORK


Fig. 2. Framework Functions

# NIST II CYBERSECURITY FRAMEWORK

Le funzioni organizzano le attività di base della cyber security al loro livello più alto e – come si può vedere – strutturano la gestione del rischio di cybersecurity in modo sequenziale, secondo una scansione temporale rispetto all'incidente informatico, con un "prima" (Identify e Protect), un "durante (Detect) ed un "dopo" (Respond e Recover).

Il Framework può essere utilizzato per confrontare le attuali attività di cyber security di un'organizzazione con quelle delineate nel Core Framework. Attraverso la creazione di un profilo attuale (lo stato "as is"), le organizzazioni possono eseguire una Gap Analysis: valutare in che misura sono lontane dallo stato "to be", cioè dai risultati descritti nelle Categorie e Sottocategorie del Core, allineate nelle cinque Funzioni di alto livello: Identificare, Proteggere, Rilevare, Rispondere e Recuperare.

# NIST II CYBERSECURITY FRAMEWORK

Queste cinque Funzioni permettono di esaminare in modo sintetico i concetti fondamentali del rischio di cybersecurity, per poter valutare come vengono gestiti i rischi identificati e come la propria organizzazione si colloca rispetto agli standard, alle linee guida ed alle pratiche di cyber security esistenti.

Il Framework può anche aiutare un'organizzazione a rispondere a domande fondamentali, tra cui "Come stiamo andando?". In questo modo potrà muoversi con maggiore cognizione di causa per rafforzare le proprie pratiche di cybersecurity e potrà definire quali siano gli investimenti necessari e compatibili con un'analisi costi/benefici.

# NIST II CYBERSECURITY FRAMEWORK


Fig. 3. Cybersecurity Framework Profiles

# NIST II CYBERSECURITY FRAMEWORK

Il meccanismo del Framework per descrivere la postura di cybersecurity attuale e target di un'organizzazione è definito Framework Profile. I profili vengono utilizzati per comprendere, valutare, dare priorità e adattare i risultati del CSF Core (cioè Funzioni, Categorie e Sottocategorie) in base agli obiettivi dell'organizzazione, alle aspettative degli stakeholder, all'ambiente di minaccia, come illustrato nella Fig. 3.

Il meccanismo del Framework per descrivere la postura di cybersecurity attuale e target di un'organizzazione è definito Framework Profile. I profili vengono utilizzati per comprendere, valutare, dare priorità e adattare i risultati del CSF Core (cioè Funzioni, Categorie e Sottocategorie) in base agli obiettivi dell'organizzazione, alle aspettative degli stakeholder, all'ambiente di minaccia, come illustrato nella Fig. 3.

# NIST II CYBERSECURITY FRAMEWORK

Esistono due tipi di profili:

Un Current Profile (Profilo attuale) che definisce i risultati del CSF Core che un'organizzazione sta attualmente raggiungendo (o cercando di raggiungere) e caratterizza come o in che misura ciascun risultato viene raggiunto. È quello che si definisce stato "as is".
Un Target Profile (Profilo obiettivo, è lo stato "to be") che comprende i risultati desiderati che un'organizzazione ha selezionato e reso prioritari dal Core per raggiungere i propri obiettivi di gestione del rischio di cyber security. Un Target Profile tiene conto dei cambiamenti previsti per la postura di cyber security dell'organizzazione, come i nuovi requisiti, l'adozione di nuove tecnologie e le tendenze delle informazioni sulle minacce di cyber security.

# NIST II CYBERSECURITY FRAMEWORK

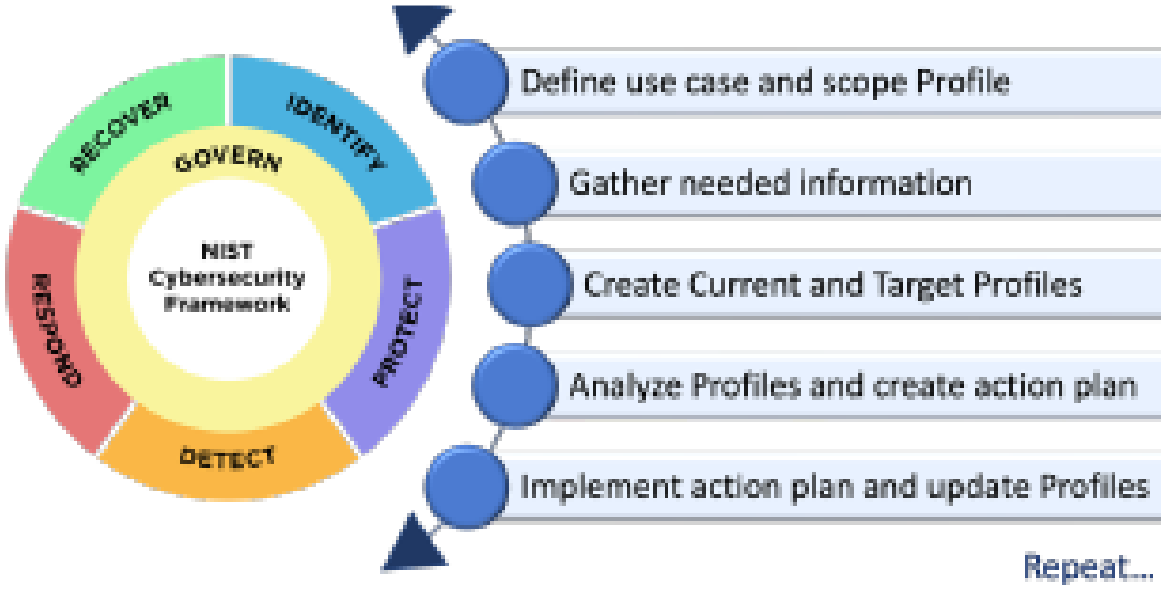


Fig. 4. Steps for creating and using Cybersecurity Framework Profiles

# NIST II CYBERSECURITY FRAMEWORK

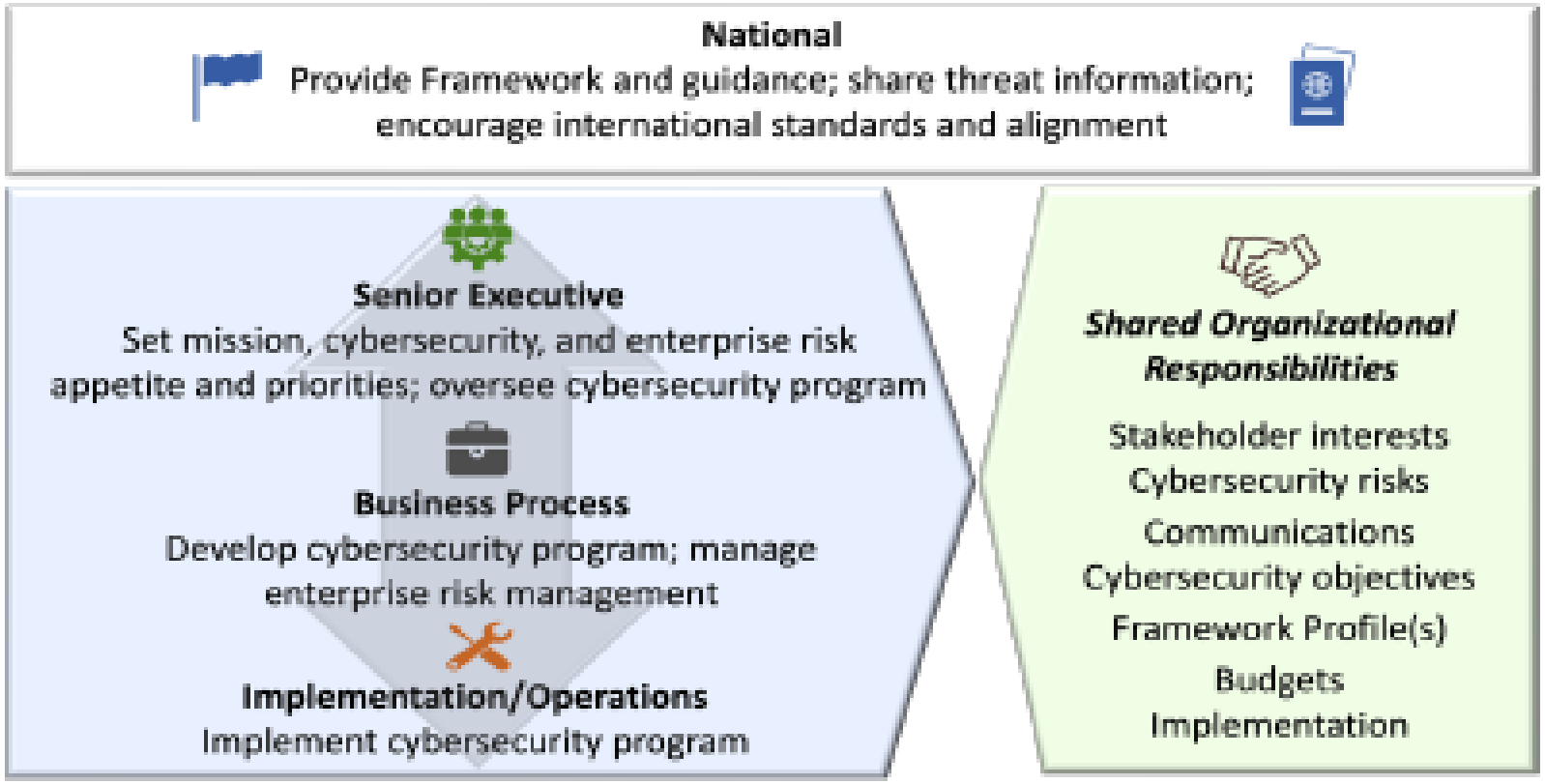


Fig. 6. Using the Cybersecurity Framework to Improve communication

# NIST II CYBERSECURITY FRAMEWORK

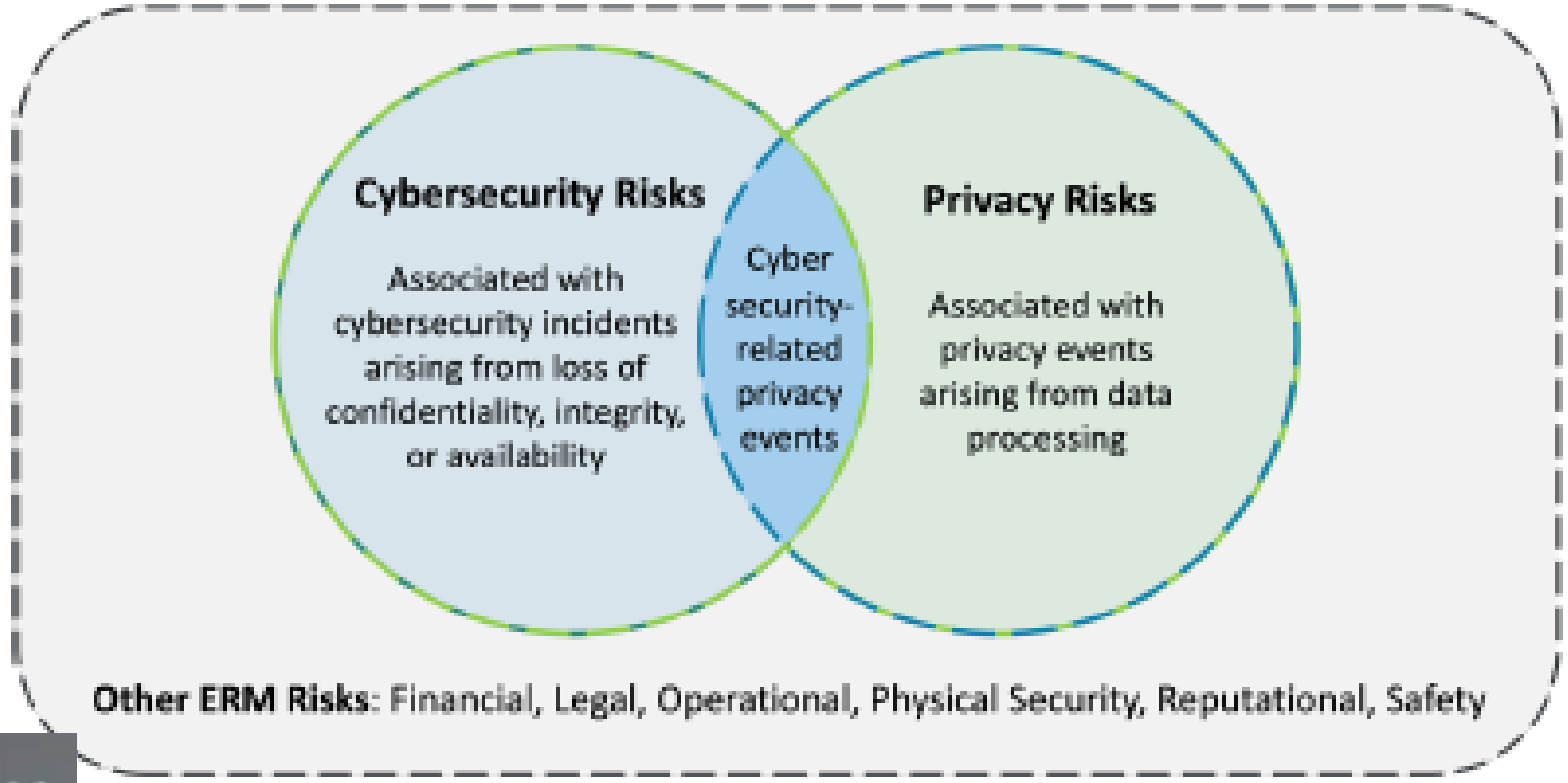


Fig. 7. Integrating cybersecurity and privacy risks

# NIST II CYBERSECURITY FRAMEWORK

La sezione 4.1 della bozza pubblicata l'8 agosto 2023 illustra appunto un esempio di integrazione degli approcci di gestione del rischio, utilizzando insieme il Cybersecurity Framework e il Privacy Framework, come illustrato nella Fig. 7, dove Il bordo esterno della Fig. 7 indica l'intera gamma di rischi ERM di un'organizzazione, con esempi di rischi finanziari, legali, operativi, di sicurezza fisica, di reputazione e di sicurezza, oltre ai rischi di cybersecurity e di privacy.

# NIST II CYBERSECURITY FRAMEWORK

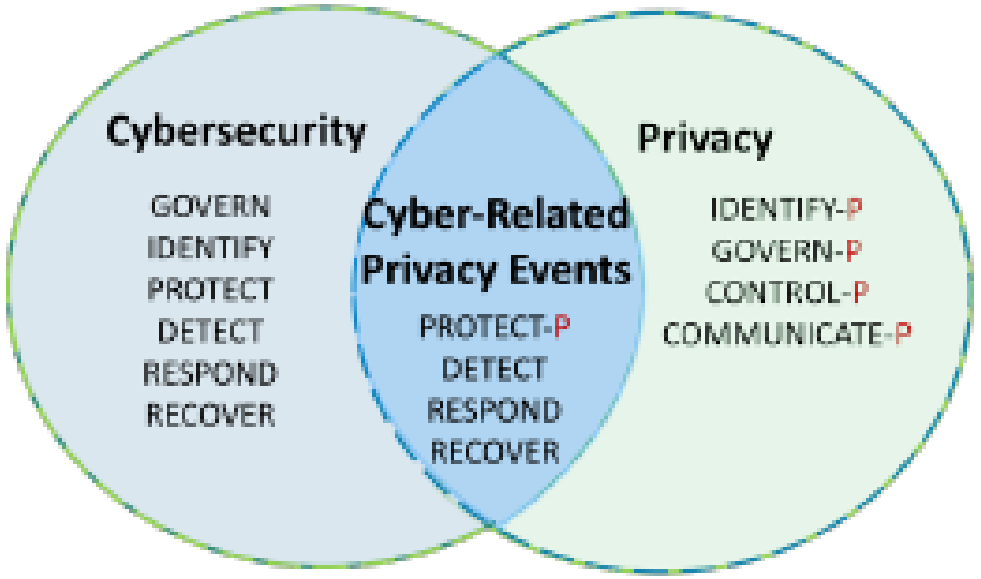


Fig. 8. Cybersecurity Framework and Privacy Framework alignment

# ENISA CYBERSECURITY MONTH 2022


# ENISA CYBERSECURITY MONTH 2022


Figure 2. Motto Choose To Be Safe Online

# ENISA CYBERSECURITY MONTH 2022


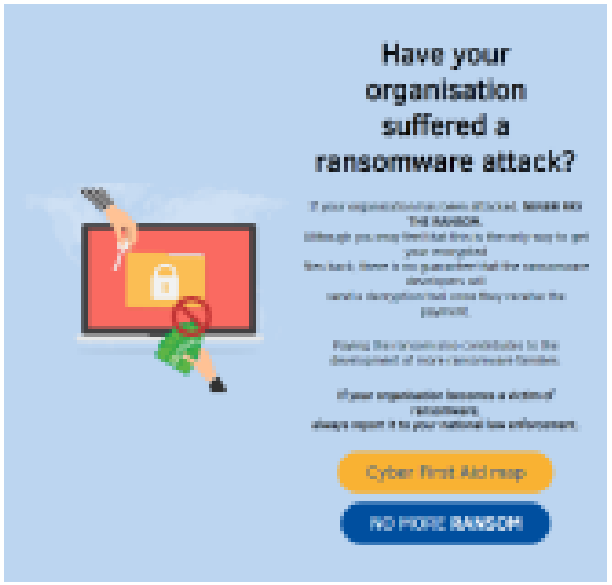



Figure 4. Cyber First Aid Map link

# ENISA CYBERSECURITY MONTH 2022

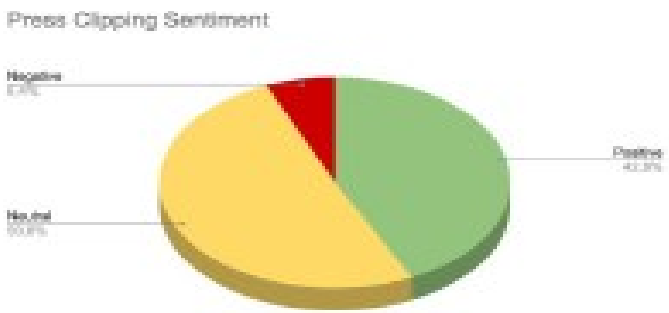


Figure 5. Press Clipping Sentiment

- **Keywords' Distribution**

The keywords were distributed as follows:

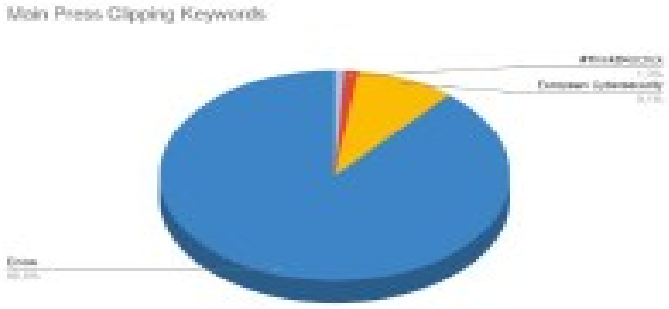


Figure 6. Main Press Clipping Keywords

# ENISA CYBERSECURITY MONTH 2022

Social Media Video views
**5.913.457**

Social Media Total Clicks
**47.892**

Figure 8. Social Media Views & Clicks

- Campaign Audience:

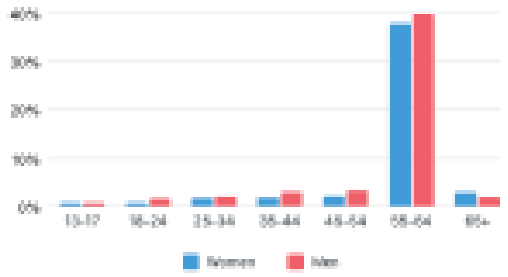


Figure 9. Campaign Audience

# CYBERSECURITY AWARENESS E DATA BREACH

- Per capire come le minacce interne generate dal fattore umano possano scatenare dei veri e propri data breach è sufficiente analizzare alcuni casi verificatisi nel 2020 e nel 2021 che hanno colpito alcune pubbliche amministrazioni sia in Italia che in Europa
- **Anonymous attacca i siti della Regione Basilicata e dei comuni della Val D'Agri**
- Denunciare lo sfruttamento petrolifero del territorio lucano e l'inquinamento. È questa la matrice dell'attacco informatico ai siti della Regione Basilicata e dell'Università lucana, perpetrato il 15-02-2020 dagli hacker di Anonymous.

# CYBERSECURITY AWARENESS E DATA BREACH

- L’attacco informatico era stato preannunciato sul blog del gruppo il 14 febbraio, aveva stati colpito i portali web istituzionali di Giunta Regione, Consiglio Regionale, Apt, il vecchio sito dell’Unibasilicata e quelli dei Comuni della Val D’Agri, con obiettivo di divulgare nomi, cognomi, username, password ed email degli amministratori, oltre che le credenziali di 198 aziende lucane, con tanto di nome, email, telefono, siti web, partita Iva e codice fiscale, e una lista di una trentina di uffici per le relazioni col pubblico, l’elenco del personale amministrativo ed altro. L’attacco si è reso necessario per denunciare "le persone che hanno avuto e che hanno tuttora un ruolo nella situazione di sfruttamento petrolifero del territorio lucano e i relativi danni ambientali.

# CYBERSECURITY AWARENESS E DATA BREACH

- L’attacco si è reso necessario per denunciare "le persone che hanno avuto e che hanno tuttora un ruolo nella situazione di sfruttamento petrolifero del territorio lucano e i relativi danni ambientali. L’attacco informatico di Anonymous si è concretizzato in un accesso non autorizzato su applicazioni in parte già dismesse e in parte in corso di dismissione e sostituzione, nell’ambito di un piano di verifica dell’integrità e sicurezza delle applicazioni che la Regione stessa stava portando avanti. Gli utenti e gli amministratori dei vari sistemi oggetto degli attacchi sono stati contattatati al fine di adottare le relative azioni di sicurezza. Come da prassi la Regione ha provveduto alla notifica e **segnalazione di Data Breach** all’Autorità Garante sulla Privacy ai sensi del Regolamento generale sulla protezione dei dati (GDPR).

# CYBERSECURITY AWARENESS E DATA BREACH

- **Danimarca, sanzionati due comuni che avevano notificato Data Breach per furto di computer**

- L'autorità di controllo per la protezione dei dati danese il 13 marzo 2020 ha rilevato che due comuni, quello di ladsaxe e quello di Hørsholm non garantiscono un livello adeguato di sicurezza dei dati come richiesto dal Gdpr. Per i comuni di Gladsaxe e Hørsholm sono state quindi proposte multe rispettivamente di 100.000 e 50.000 corone danesi, ovvero circa 13mila euro nel primo caso e 6mila euro nel secondo. Il garante danese era venuto a conoscenza di entrambi i casi a seguito della notifica di Data Breach riguardanti violazioni relative al furto di computer contenenti dati personali, che gli stessi comuni avevano inviato all'autorità per ottemperare a quanto previsto dall'art.33 del Gdpr.

# CYBERSECURITY AWARENESS E DATA BREACH

- Nessuno dei due computer era protetto dalla crittografia e la perdita di dati personali da parte dei comuni rappresentava pertanto un rischio indebito per i cittadini. In uno dei casi, l'inadeguato livello di sicurezza ha comportato una grave violazione dei dati personali, in quanto uno dei computer rubati al municipio di Gladsaxe conteneva dati personali di 20.620 cittadini, conteneva anche informazioni di natura sensibile. Un'altra violazione della sicurezza è avvenuta quando il computer di un dipendente del comune di Hørsholm è stato rubato dalla sua automobile. Sul computer c'erano informazioni riguardanti circa 1.600 dipendenti dello stesso comune, comprese informazioni di natura sensibile, rientranti nelle "categorie particolari di dati personali" ai sensi dell'art.9 del Regolamento UE 2016/679. Secondo **quanto rilevato dall'autorità danese**, tali violazioni manifestavano alcune delle possibili conseguenze dell'insufficiente livello di sicurezza che comporta un rischio elevato per tutti i cittadini di cui il comune tratta i dati personali, e perciò ha proposto le due sanzioni.

# CYBERSECURITY AWARENESS E DATA BREACH

- **Ransomware colpisce il Comune di Marentino**
- Con un **comunicato sul proprio sito istituzionale**, il Comune di Marentino il 13-4-2020 aveva informato tutti gli interessati, residenti e non, di aver recentemente subito un attacco informatico di tipo **ransomware** che, sfruttando il periodo emergenziale causato dall'epidemia, ha violato i dati personali presenti sul server centrale. L'Ente aveva affermato di essersi prontamente attivato, procedendo anche a notificare il Data Breach al Garante per la protezione dei dati personali come previsto dal Gdpr. Ad accorgersi dell'accaduto sono stati i dipendenti comunali, quando da casa si sono collegati all'account dell'ente per lavorare in smartworking, come sono costretti a fare in questo periodo per disposizioni governative relative all'emergenza Covid-19.

# CYBERSECURITY AWARENESS E DATA BREACH

- I criminali informatici hanno inoculato un cryptoLocker che ha messo fuori uso il sistema per poi cancellare anche il backup dei file, chiedendo un riscatto in bitcoin per sbloccare i dati, "in misura ridotta" di 50mila euro se il pagamento fosse avvenuto entro due giorni, cifra che è però raddoppiata a 100mila euro dopo la scadenza del termine. Preso atto della violazione, il piccolo comune piemontese aveva iniziato un processo di adeguamento per adottare tutte le misure più idonee a porre rimedio alla situazione di rischio, attenuando i possibili effetti negativi e tutelare i diritti e le libertà delle persone fisiche purtroppo coinvolte nella violazione. Nel frattempo, l'attacco era stato denunciato ai carabinieri di Sciolze ed è stata informata anche la polizia postale.

# CYBERSECURITY AWARENESS E DATA BREACH 2020

## GIUGNO

**Pubblica amministrazione**

Mail malevola avverte la vittima di un fantomatico "Contenzioso Civile"

Il CERT-AgID: Il cybercrime ha lanciato una massiccia campagna malspam per diffondere FTCODE via PEC in Italia. I bersagli sono le strutture della Pubblica Amministrazione e i privati. Il malware sfrutta un presunto contenzioso civile al Tribunale di Napoli

*Fonte: https://www.difesaesicurezza.com/*

2020

## MARZO

**Settore della Sanità**

Il data breach al San Raffaele ha esposto i dati di ben 2400 dipendenti e 600 pazienti.

San Raffaele: data breach di gravità "media", ospedale obbligato a notificare gli utenti

*Fonte: https://www.agendadigitale.eu/*

## SETTEMBRE

**Settore finanziario**

E-mail di spear-phishing che utilizzano come esca le normative KYC (Know Your Customer regulations).

Remote Access Trojan, arriva PyVil: cosa lo rende così temibile, come difendersi

*Fonte: https://www.cybersecurity360.it/*

# CYBERSECURITY AWARENESS E DATA BREACH 2021

- **Sistema informativo del Comune di Brescia paralizzato da ransomware. Attacco hacker al Comune di Brescia, chiesto un riscatto da 1,3 milioni**

- Sempre nel mese di aprile 2021 è stato attaccato il sistema di posta elettronica e l'intera operatività dei server del Comune di Brescia. Come si legge nella nota pubblicata nello stesso sito istituzionale della pubblica amministrazione lombarda, la causa della paralisi è stata un attacco ransomware avvenuto il 30 marzo, e la richiesta di riscatto per fornire la chiave di sblocco avanzata dai criminali informatici per restituire la disponibilità dei dati è di 26 Bitcoin, l'equivalente al cambio odierno di 1,3 milioni di euro. Secondo quanto riferito dai media locali, il ransomware che ha colpito il Comune di Brescia è DoppelPaymer, per la verità non nuovo alle amministrazioni pubbliche italiane, il quale è capace di entrare silenziosamente nei server e bloccarne l'accesso crittografandone i file contenuti (il riscatto, appunto, servirebbe a ottenere la chiave per decriptarli).

# CYBERSECURITY AWARENESS E DATA BREACH 2021

- Mentre gli uffici dell'amministrazione lombarda sono al lavoro per tentare di far ripartire la macchina digitale del comune che conta circa 200mila abitanti, resta ora da capire quanto ci metteranno i tecnici a ripristinare la normalità, perché ad essere bloccato, non è solo il sito web, ma anche il sistema che gestisce le gare e gli appalti, l'Archiweb per le pratiche edilizie, tutto il sistema scolastico e quello cimiteriale, le postazioni di lavoro della Ragioneria, della Loggia, dell'Anagrafe e della Polizia Locale. La riattivazione di alcuni servizi essenziali, incluso un sito web "muletto" per garantire le comunicazioni con i cittadini, dovrebbe avvenire nel giro di alcuni giorni, anche se fonti interne smorzano facili ottimismi: senza pagamento del riscatto, occorreranno mesi, addirittura anni per recuperare i dati criptati dal malware. L'unica alternativa, per ora, sarà quella di contare sui back up, sperando siano abbastanza aggiornati.

# CYBERSECURITY AWARENESS E DATA BREACH 2021

- **Attacco informatico ai server dell'Agenzia Territoriale per la Casa di Torino, oltre mezzo milione di euro il riscatto chiesto dagli hacker**

- Un attacco informatico verificatosi nel week end e scoperto dai tecnici al rientro è avvenuto lunedì mattina 11 aprile 2021 che ha mandato in tilt i server dell'ATC Torino (Agenzia Territoriale per la Casa), l'azienda pubblica che gestisce 30mila appartamenti di edilizia popolare. Gli hacker hanno chiesto all'ente un riscatto di 700mila dollari per restituire i dati rubati e criptati. L'attacco riguarda circa 43 terabyte di dati gestiti. L'attacco si è svolto mediante la ricezione di una mail da parte del personale con la richiesta di un cospicuo riscatto dell'importo corrispondente al cambio attuale a 584mila euro, messaggio che si sarebbe subito autodistrutto dopo la lettura senza lasciare tracce, motivo per cui pare che dietro l'attacco di tipo ransomware vi siano professionisti di alto profilo.

# CYBERSECURITY AWARENESS E DATA BREACH 2021

- Il Data Breach è stato denunciato alla Polizia Postale e regolarmente notificato al Garante per la protezione dei dati personali, ma sembra che l'ATC non abbia nessuna intenzione di pagare il riscatto e di non cedere alle richieste dei criminali informatici, anche se nel frattempo il personale è stato costretto a tirare fuori dal cassetto carta e penna e tornare a trasmettere comunicazioni tramite il fax.

# CISA CYBERSECURITY AWARENESS PROGRAM

Il CISA Cybersecurity Awareness Program è un programma di sensibilizzazione da parte degli USA volto ad aumentare la comprensione delle minacce informatiche e a consentire al popolo americano di essere più sicuro e protetto online. La sicurezza informatica è una responsabilità condivisa e ognuno di noi ha un ruolo da svolgere. Quando tutti adottiamo semplici misure per essere più sicuri online – a casa, sul posto di lavoro e nelle nostre comunità – l'utilizzo di Internet diventa un'esperienza più sicura per tutti.

# CISA CYBERSECURITY AWARENESS PROGRAM

Questo programma fa parte di uno sforzo senza precedenti da parte dei governi federali e statali, dell'industria e delle organizzazioni no-profit per promuovere comportamenti e pratiche online sicuri. Si tratta di un partenariato pubblico-privato unico, implementato in coordinamento con la National Cyber Security Alliance.

Gli americani utilizzano sempre di più le nuove tecnologie e trascorrono più tempo online. La nostra crescente dipendenza dalla tecnologia, unita alla crescente minaccia di attacchi informatici, richiede maggiore sicurezza nel nostro mondo online. Ciò presenta la necessità di risorse e suggerimenti semplici e di facile comprensione per garantire la loro sicurezza.

Il programma CISA Cybersecurity Awareness fornisce agli americani l'accesso alle risorse e agli strumenti di cui hanno bisogno per prendere decisioni più informate quando utilizzano Internet.

# CISA CYBERSECURITY AWARENESS PROGRAM

- Negli USA sin al 2004, il Presidente degli Stati Uniti e il Congresso hanno dichiarato ottobre il mese della sensibilizzazione alla sicurezza informatica, aiutando le persone a proteggersi online man mano che le minacce alla tecnologia e ai dati riservati diventano più comuni. La Cybersecurity and Infrastructure Security Agency (CISA) e la National Cybersecurity Alliance (NCA) guidano uno sforzo di collaborazione tra governo e industria per aumentare la consapevolezza della sicurezza informatica a livello nazionale e internazionale.

# CISA CYBERSECURITY AWARENESS PROGRAM

- Per tale motivo è stato istituto il CYBERSECURITY AWARENESS MONTH. Il tema della campagna che si è tenuto ad ottobre del 2022- denominata "Vedi te stesso nel cyber" - dimostra che mentre la sicurezza informatica può sembrare un argomento complesso, in definitiva, è davvero tutta una questione di persone. Questo ottobre si concentrerà sulla parte "persone" della sicurezza informatica, fornendo informazioni e risorse per aiutare a educare i partner CISA e il pubblico e garantire che tutti gli individui e le organizzazioni prendano decisioni intelligenti sul lavoro, a casa o a scuola, ora e nel futuro. Incoraggiamo ciascuno di voi a impegnarsi negli sforzi di quest'anno creando le proprie campagne di sensibilizzazione informatica e condividendo questo messaggio con i propri colleghi

# CISA CYBERSECURITY AWARENESS PROGRAM

- Sin dal 2012 l'ENISA (Agenzia dell'Unione europea per la sicurezza informatica) organizza l'ECSM, il mese europeo della sicurezza informatica che è la campagna annuale dell'Unione europea dedicata alla promozione della sicurezza informatica tra i cittadini e le organizzazioni dell'UE e alla fornitura di informazioni aggiornate sulla sicurezza online attraverso la sensibilizzazione e la condivisione di buone pratiche. Ogni anno, per l'intero mese di ottobre, si svolgono centinaia di attività in tutta Europa, tra cui conferenze, workshop, corsi di formazione, webinar, presentazioni e altro, per promuovere la sicurezza digitale e l'igiene informatica.

# CISA CYBERSECURITY AWARENESS PROGRAM

a) In Italia AGID (Agenzia per l'Italia Digitale) ha approvato il Piano Triennale per la PA AGID 2020-2022 con l'obiettivo di **Aumentare la consapevolezza del rischio cyber *(Cyber SecurityAwareness)* nelle PA. Questo è lo stato dell'arte:**

- Da settembre 2020 nei procedimenti di acquisizione di beni e servizi ICT le pubbliche amministrazioni fanno riferimento alle Linee guida sulla sicurezza nel *procurement* ICT ai sensi della Determinazione AGID 17/2020

# CISA CYBERSECURITY AWARENESS PROGRAM

- Da novembre 2020 tutte le pubbliche amministrazioni fanno riferimento al documento tecnico *Cipher Suite* protocolli TLS minimi per la comunicazione tra le PA e verso i cittadini che. Nello specifico tutti gli applicativi web dovranno utilizzare il protocollo TLS (Transport Layer Security) che di recente ha largamente sostituito il protocollo SSL per la comunicazione sicura su internet, ma molti browser utilizzano SSL 3.0 quando non è disponibile una connessione TLS. Si raccomanda l'utilizzo di TLS 1.2 o 1.3. La versione più diffusa di questo protocollo è TLS 1.2. La successiva versione TLS 1.3 aggiunge ulteriori requisiti sulle suite di cifratura, ma essendo stata standardizzata solo ad agosto 2018 non è ancora molto diffusa. Le suite di cifratura definite per TLS 1.2 non sono in generale utilizzabili con TLS 1.3 (e viceversa), salvo diversa indicazione nella loro definizione. Il Cypher suite è una suite di cifratura, denominata anche suite di crittografia o con il termine in inglese cipher suite è un insieme di algoritmi utilizzati per rendere sicuri i collegamenti di rete basati su Transport Layer Security (TLS) o sul suo predecessore, ora deprecato, Secure Socket Layer (SSL). L'insieme di algoritmi che costituisce una suite comprende tipicamente: un algoritmo per lo scambio delle chiavi crittografiche, un algoritmo di crittografia ed un algoritmo di message authentication code (MAC).

# CISA CYBERSECURITY AWARENESS PROGRAM

- Da luglio 2021 tutte le PA che intendono istituire i CERT (COMPUTER EMERGENCE RESPONSE TEAM) di prossimità devono far riferimento alle Linee guida per lo sviluppo e la definizione del modello di riferimento per i CERT di prossimità (https://docs.italia.it/AgID/documenti-in-consultazione/lg-cert-regionali/it/bozza/index.html).
- Da dicembre 2021 tutte le pubbliche amministrazioni potranno valutare l'utilizzo del *tool di Cyber Risk Assessment* per l'analisi del rischio e la redazione del Piano dei trattamenti. L'approccio metodologico da utilizzare è quello suggerito da AgID e si basa sui principi e le linee guida dettati dallo standard ISO 31000 [DR-3] e sull'information risk assessment methodology 2 (IRAM2), metodologia prodotta dall'Information Security Forum (ISF). Questa metodologia consente di valutare il rischio legato ad una certa minaccia rispetto ai servizi erogati o utilizzati da una PA, senza interessare gli asset che li compongono

# CISA CYBERSECURITY AWARENESS PROGRAM

- Da marzo 2022 tutte le pubbliche amministrazioni dovranno definire, sulla base di quanto proposto dal RTD, all'interno dei piani di formazione del personale, interventi sulle tematiche di *Cyber Security Awareness*
- Da giugno 2022 tutte le pubbliche amministrazioni dovranno adeguarsi alle Misure minime di sicurezza ICT per le pubbliche amministrazioni aggiornate.