REPORT DI CYBERSECURITY PER IL COMUNE DI MARSCIANO

Contestualizzazione del Framework Nazionale per la Cybersecurity

a cura di:

Dott. Carlo Ciocchetti

Responsabile tecnico e consulente ICT – TCS - Total Consulting System Srl

Marco Caselli, PhD

Cybersecurity Engineer e cofondatore Gruppo PAOSoft

Dott.ssa Lucia Padiglioni

Responsabile ICT – Comune di Marsciano

Gruppo PAOSoft

Comune di Marsciano

TCS TOTAL CONSULTING SYSTEM SRL

Indice:

INTRODUZIONE

1.1 Cybersecurity e contesto di applicazione

Negli ultimi decenni, internet e la digitalizzazione hanno rappresentato una rivoluzione epocale che ha influenzato profondamente tutti i settori della società. Ogni dispositivo elettronico potenzialmente può essere connesso in rete e tratta, trasporta e contiene una serie di informazioni che possono essere considerate più o meno importanti e più o meno sensibili: quindi da proteggere e salvaguardare.

Accanto a termini come "connessione", "digitalizzazione" ed "IoT" - sempre più in uso nel linguaggio comune - vengono ultimamente affiancati termini come "resilienza", "difesa", "sicurezza", "protezione". Con l'aumento della digitalizzazione, infatti, sono parallelamente aumentate anche le minacce informatiche: la cybersecurity, quindi, deve essere inclusa a tutti gli effetti nella trasformazione digitale.

Già nel 2016 la NATO ha riconosciuto il cyberspazio come quinto dominio operativo[5]: un attacco individuato all'interno di quel dominio sarà un attacco convenzionale.

Il quadro normativo italiano, attraverso il Codice dell'Amministrazione Digitale, la Direttiva del Presidente del Consiglio dei Ministri 1 Agosto 2015 ed il DPCM del 17 febbraio 2017[6], pone criteri di riferimento di sicurezza informatica da adottare per le Pubbliche Amministrazioni, individuando nell'Agenzia per l'Italia Digitale (AgID) l'Ente con compiti di vigilanza e controllo sul rispetto delle norme, di emanazione di regole e di adozione di atti amministrativi generali in materia di sicurezza informatica.

Poiché economia e cyberspazio nell'immediato futuro saranno sempre più sovrapposti, la protezione di quest'ultimo è condizione necessaria per la prosperità economica: la sicurezza informatica non è quindi solo un obbligo normativo ma una necessità per innalzare la resilienza del sistema paese.

Da qui la necessità, per le Pubbliche Amministrazioni, di adottare una metodologia per analizzare il proprio stato attuale in materia di sicurezza informatica ed innalzare il proprio livello di maturità e resilienza nei confronti di eventuali attacchi informatici, garantendo la continuità operativa dell'ente ed il rispetto delle Misure Minime di sicurezza ICT per le Pubbliche Amministrazioni pubblicate dall'AgID[1].

Le Pubbliche Amministrazioni, per la mole e la tipologia di informazioni che trattano,

stanno diventando sempre più vulnerabili e sempre più appetibili; è necessario quindi adottare dei meccanismi e delle procedure condivise che permettano di difendere l'ente dagli attachi cyber, di condividere le informazioni e diffondere la cultura della cybersecurity all'interno dell'organizzazione. E' noto che gli attaccanti fanno squadra passandosi , nel dark web, tutti i tipi di informazioni possibili. La condivisione delle informazioni, la sensibilizzazione e l'aggiornamento permanente, la cooperazione tra pubblico e privato possono permettere l'innalzamento della sicurezza informatica del paese[4].

Su questi principi è stato scelto di utilizzare il Framework Nazionale della Cybersecurity[2] quale linguaggio comune e base di partenza, essendo un documento conosciuto e condiviso sul quale diversi asset strategici del paese hanno già operato adattamenti alla propria realtà aziendale. Del Framework Nazionale è stata operata una contestualizzazione per le Pubbliche Amministrazioni Locali fino a 20.000 abitanti, integrandola con le direttive AgID sulla sicurezza informatica[1] e stimando i costi necessari per eseguire determinate attività al fine di realizzare le pratiche di sicurezza indicate . Su quest'ultimo modello è stata operata un'analisi per il Comune di Marsciano.

Ne nasce il lavoro illustrato di seguito, che ha lo scopo di mettere in luce la situazione attuale dell'Ente sul piano della sicurezza informatica e tracciare il percorso che il Comune di Marsciano vorrà intraprendere nel prossimo futuro per innalzare sempre più il proprio livello di maturità e resilienza nei confronti di possibili eventi dannosi sotto il profilo della cybersecurity, così da garantire protezione per i dati del Comune e continuità operativa per i servizi offerti ai propri cittadini.

Non vi può essere, infatti, amministrazione digitale senza un'adeguata sicurezza informatica.

1.2 Scopo del documento

Il documento redatto analizza le criticità in ambito di cybersecurity del Comune di Marsciano innalzando la consapevolezza del rischio che si potrebbe correre e permettendo di stabilire le priorità delle azioni da intraprendere, anche nell'ottica di

eventuali investimenti sul fronte della sicurezza informatica.

Il lavoro è stato realizzato in 3 fasi:

- analisi dettagliata della situazione dell'Ente per delineare il profilo attuale e gli strumenti e le procedure interne di rilevazione e risposta agli attacchi informatici;
- redazione dell'allegato 2 della Circolare AgID n. 2/2017 recante le Misure Minime di sicurezza ICT per le pubbliche amministrazioni[1];
- compilazione dello schema di contestualizzazione del Framework Nazionale della Cybersecurity per Pubbliche Amministrazioni Locali fino a 20.000 abitanti e redazione del presente documento.

Il presente documento riporta, nella tabella di contestualizzazione, il profilo attuale dell'ente dal punto di vista della sicurezza informatica e fa una stima, anche dal punto di vista economico, del lavoro necessario per progredire nei livelli di maturità e raggiungere il profilo target. I livelli di maturità sono strettamente collegati alle richieste implementative presenti nelle subcategory del framework nazionale della cyber security[2] redatto dalla Sapienza, Università di Roma, ed alle misure minime di sicurezza informatica[1] dettate da Agid.

Le misure minime riguardano un insieme ordinato e ragionato di "controlli", ossia azioni puntuali di natura tecnica od organizzativa, che l'Agenzia per l'Italia Digitale ha predisposto al fine di fornire alle Pubbliche Amministrazioni un riferimento pratico per valutare e innalzare il proprio livello di sicurezza informatica, avvalendosi in ciò della sua facoltà di dettare "indirizzi, regole tecniche e linee guida in materia di sicurezza informatica" anche in ottemperanza alla direttiva del 1° agosto 2015 del Presidente del Consiglio dei Ministri che impone l'adozione di standard minimi di prevenzione e reazione ad eventi cibernetici.
Il percorso di digitalizzazione della P.A. per conto di AgID rientra nel ben più ampio progetto dell'Agenda Digitale Europea, una delle sette iniziative faro della Strategia Horizon 2020 che si propone di migliorare il potenziale delle tecnologie dell'informazione e della comunicazione (ICT) al fine di favorire innovazione, crescita economica e progresso.

Il Framework Nazionale per la Cyber Security[2], invece, è un documento redatto dal CIS della Sapienza Università di Roma (Cyber Intelligence and Information Security Center) e dal CINI (Consorzio Interuniversitario Nazionale per l'Informatica) e rappresenta un insieme di pratiche riconosciute e internazionalmente valide che permettono di quantificare, valutare e stimare il grado di resilienza di un Ente nei confronti di eventuali attacchi informatici. Pubblicato il 4 febbraio 2016, è il linguaggio comune che consente il dialogo tra diversi attori sul tema della sicurezza informatica.

Il Framework Nazionale per la Cyber Security[2] ha diversi punti in comune con il Framework del NIST – così da realizzare un'armonizzazione internazionale – ma è stato specializzato sulla realtà produttiva italiana e rappresenta un riferimento nel quale possono essere inquadrati gli standard e le norme di settore esistenti. Si propone lo scopo di elencare e categorizzare le aree informatiche che comprendono le procedure che AgID mette a disposizione. Ogni "category", così vengono chiamate le diverse sezioni in cui vengono suddivise le 5 Functions, ha diverse sotto aree più specifiche chiamate "subcategory", che, per quanto riguarda la Pubblica Amministrazione, sono strettamente associate alle direttive informatiche del documento presentato dall'Agenzia per l'Italia Digitale.
Il Framework, pubblicato il 4 febbraio 2016, rappresenta un linguaggio comune in grado di agevolare, se non di permettere, il dialogo tra attori diametralmente opposti, siano questi all'interno dell'organigramma delle imprese o delle pubbliche amministrazioni (ad esempio tecnici e dirigenti), sia organizzazioni vere e proprie in corso di collaborazione o di appalti di fornitura.

1.3 Contestualizzazione del Framework Nazionale

Il Framework nazionale redatto dalla Sapienza[2] descrive le aree principali (category) concernenti l'ambito ICT che hanno un ruolo chiave nella sicurezza cibernetica. Contestualizzare il Framework per un settore produttivo o per una categoria omogenea di organizzazioni significa specificare il suo core, ovvero selezionare le Category e Subcategory per le quali ha senso definire le priorità rispetto alle altre dal punto di vista della normativa, del settore produttivo, della tipologia degli impiegati, della dimensione

e della dislocazione sul territorio del Comune, specificando i livelli di maturità per le Subcategory selezionate.
Il primo passo per la contestualizzazione consiste quindi nella scelta di quelle Categorie e Sottocategorie che, per le ragioni sopra elencate, devono essere selezionate e per le quali deve essere definita la rispettiva priorità.
Nel caso delle Pubbliche Amministrazioni locali con meno di 20.000 abitanti, il lavoro di contestualizzazione è stato realizzato tenendo soprattutto in considerazione le direttive che AgID presenta[1] e che mette direttamente in relazione con le subcategory del frame work, ovvero quelle che vengono chiamate ABSC (Agid Basic Security Controls). Ogni subcategory della contestualizzazione del framework può contenere una o più ABSC; la combinazione di queste contribuirà a definire la priorità per quella subcategory, e i possibili livelli di maturità raggiungibili dall'Ente. Lì dove la subcategory non racchiude alcuna ABSC, la scelta della priorità e dei possibili livelli di maturità raggiungibili viene fatta sulla base della definizione fornita dal Framework Nazionale.
Per irrobustire la contestualizzazione e completare il quadro fornendo all'ente informazioni utili anche dal punto di vista operativo e contabile, accanto alle colonne dedicate alle ABSC AgID, sono state inserite 2 colonne: una riguarda un suggerimento di soluzione per implementare la rispettiva ABSC, l'altra riguarda una stima dei costi necessari per applicare la soluzione e far innalzare il livello di maturità dell'ente a quello successivo.

Nella pagina successiva è riportata una porzione della tabella di contestualizzazione del Framework Nazionale della cybersecurity per Pubbliche Amministrazioni locali fino a 20.000 abitanti.
La tabella completa viene fornita all'ente su formato excel; non viene riportata completamente in questo documento per motivi di visibilità e di formattazione: il file excel si sviluppa su 252 righe e 21 colonne e sarebbe pertanto di difficile impaginazione.
Le prime 4 colonne (Function, Category, Subcategory, Priorità) corrispondono alla tabella del Framework Nazionale redatto dal CINI.
La colonna dei Livelli di Maturità, contenente all'interno 4 colonne, riporta il range di possibili livelli .Per ogni subcatory, i livelli raggiungibili sono evidenziati in azzurro;

notare, ad esempio, che per la subcategory ID.AM-4 i possibili livelli sono solo 2 mentre per le altre i livelli sono 4. Il livello di maturità raggiunto dall'ente sarà evidenziato con una X.

Nelle successive colonne sono state riportate, per ogni subcategory, tutte le ABSC AgID ad essa riconducibili e che su essa possano avere un peso nella realizzazione dell'adeguamento.

Accanto a determinate ABSC è stata anche aggiunta una colonna descrittiva che riporta una possibile modalità di realizzazione dell'adeguamento.

Function	Category	Subcategory	Priorità	Livelli di Maturità				ABSC			
				Insufficiente	Minimo	Standard	Alto	NUMERO	DESCRIZIONE	LIVELLO DI SICUREZZA	SOLUZIONE PROPOSTA
IDENTIFY	Asset Management (ID.AM): I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi di business e con la strategia di rischio dell'organizzazione	ID.AM-1: Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione	ALTA					1.1.1		MINIMO	YYYYYYYYYYYYYYYYYYY
								1.1.2		STANDARD	XXXXXXXXXXXXXXXXXXXXX
								1.1.3		ALTO	
								1.1.4		ALTO	
								1.2.1		STANDARD	
								1.2.2		STANDARD	
								1.3.1		MINIMO	XXXXXXXXXXXXXXXXXXXXX
								1.3.2		STANDARD	XXXXXXXXXXXXXXXXXXXXX
								1.4.1		MINIMO	XXXXXXXXXXXXXXXXXXXXX
								1.4.2		STANDARD	XXXXXXXXXXXXXXXXXXXXX
								1.4.3		ALTO	
								1.5.1		ALTO	
								1.6.1		ALTO	
								13.5.2		ALTO	
		ID.AM-2: Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione	ALTA					2.1.1		MINIMO	YYYYYYYYYYYYYYYYYYY
								2.2.1		STANDARD	YYYYYYYYYYYYYYYYYYY
								2.2.2		STANDARD	YYYYYYYYYYYYYYYYYYY
								2.2.3		ALTO	YYYYYYYYYYYYYYYYYYY
								2.3.1		MINIMO	YYYYYYYYYYYYYYYYYYY
								2.3.2		STANDARD	YYYYYYYYYYYYYYYYYYY
								2.3.3		ALTO	YYYYYYYYYYYYYYYYYYY
								2.4.1		ALTO	
		ID.AM-3: I flussi di dati e comunicazioni inerenti l'organizzazione sono identificati	ALTA					5.1.4		ALTO	
								13.3.1		ALTO	
								13.4.1		ALTO	
								13.6.1		ALTO	
								13.6.2		ALTO	
								13.7.1		ALTO	
								13.8.1		MINIMO	YYYYYYYYYYYYYYYYYYY
		ID.AM-4: I sistemi informativi esterni all'organizzazione sono catalogati	BASSA								

ABSC					Somma della spesa per la progressione di livello				Informative References	Guide Lines (Vedi scheda "Rif. Priorità")
NUMERO	DESCRIZIONE	LIVELLO DI SICUREZZA	SOLUZIONE PROPOSTA	STIMA DELLA SPESA	Insufficiente	Minimo	Standard	Alto		
1.1.1		MINIMO	YYYYYYYYYYYYYYYYYYYY	$$$						
1.1.2		STANDARD	XXXXXXXXXXXXXXXXXXXXX	$$$						
1.1.3		ALTO								
1.1.4		ALTO								
1.2.1		STANDARD								
1.2.2		STANDARD								
1.3.1		MINIMO	XXXXXXXXXXXXXXXXXXXXX	$$$						
1.3.2		STANDARD	XXXXXXXXXXXXXXXXXXXXX	$$$		$$	$$$$		. Inventario mobiliare. COBIT 5 BAI09.01, BAI09.02. ISA 62443-2-1:2009 4.2.4.3. ISA 62443-3-3:2013 SR 7.8. ISO/IEC 27001:2013 A.8.1.1, A.9.1.2. NIST SP 800-53 Rev. 4 CM-8. MISURE MINIME DI SICUREZZA ICT PER LE PUBBLICHE AMMINISTRAZIONI	in conformità alle richieste di sicurezza minime da adottare, da parte di una P.A, secondo il modello AgID, riduce 1,2. in quanto: si gestisce attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso
1.4.1		MINIMO	XXXXXXXXXXXXXXXXXXXXX	$$$						
1.4.2		STANDARD	XXXXXXXXXXXXXXXXXXXXX	$$$						
1.4.3		ALTO								
1.5.1		ALTO								
1.6.1		ALTO								
13.5.2		ALTO								
2.1.1		MINIMO	YYYYYYYYYYYYYYYYYYYY	$$$						
2.2.1		STANDARD	YYYYYYYYYYYYYYYYYYYY	$$$						
2.2.2		STANDARD	YYYYYYYYYYYYYYYYYYYY	$$$						
2.2.3		ALTO	YYYYYYYYYYYYYYYYYYYY	$$$						
2.3.1		MINIMO	YYYYYYYYYYYYYYYYYYYY	$$$						
2.3.2		STANDARD	YYYYYYYYYYYYYYYYYYYY	$$$						
2.3.3		ALTO	YYYYYYYYYYYYYYYYYYYY	$$$					. D.L. 90/2014 art. 24 – quater comma 2. CCS CSC 2. COBIT 5 BAI09.01, BAI09.02, BAI09.05. ISA 62443-2-1:2009 4.2.3.4. ISA 62443-3-3:2013 SR 7.9. ISO/IEC 27001:2013 A.8.1.1, A.8.1.2. NIST SP 800-53 Rev. 4 CM-8. MISURE MINIME DI SICUREZZA ICT PER LE PUBBLICHE AMMINISTRAZIONI	in conformità alle richieste di sicurezza minime da adottare, da parte di una P.A, secondo il modello AgID. Riduce 1,2 in quanto si Gestisce attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione
2.4.1		ALTO								
5.1.4		ALTO								
13.3.1		ALTO								
13.4.1		ALTO								
13.6.1		ALTO								
13.6.2		ALTO								
13.7.1		ALTO								
13.8.1		MINIMO	YYYYYYYYYYYYYYYYYYYY	$$$					. CCS CSC 1 . COBIT 5 DSS05.02 . ISA 62443-2-1:2009 4.2.3.4 . ISO/IEC 27001:2013 A.13.2.1 . NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8 MISURE MINIME DI SICUREZZA ICT PER LE PUBBLICHE AMMINISTRAZIONI	in conformità alle richieste di sicurezza minime da adottare, da parte di una P.A, secondo il modello AgID. Riduce 1,3, in quanto: evita l'esfiltrazione dei dati, mitiga gli effetti e garantisce la riservatezza e l'integrità delle informazioni Rilevanti
									. COBIT 5 APO02.02 . ISO/IEC 27001:2013 A.11.2.6 . NIST SP 800-53 Rev. 4 AC-20, SA-9	

In quest'altra porzione di tabella della contestualizzazione del Framework Nazionale della cybersecurity per Pubbliche Amministrazioni locali fino a 20.000 abitanti viene illustrato il collegamento tra le ABSC AgID, le soluzioni proposte e la spesa stimata per realizzare ogni singola soluzione e, più in generale, per realizzare la progressione da un livello di maturità a quello più avanzato

1.4 Acronimi, abbreviazioni e definizioni

ABSC = AgID Basic Security Controls

AgID = Agenzia per l'Italia Digitale

CERT-PA = Computer Emergency Response Team Pubblica Amministrazione

P.A. = Pubblica Amministrazione

REGISTRO DELLE VERSIONI E RELATIVE DISTRIBUZIONI

N°Ver/Rev/Bozza	Data emissione	Sintesi delle modifiche apportate	Osservazioni	Distribuito a
1.0	20/12/2017	Prima versione		Uff. Informatica
2.0	02/03/2018	Tabella di contestualizzazione e stima dei costi		Uff. Informatica

DESCRIZIONE DEL PROCEDIMENTO:

2.1 Livelli di Maturità e di Rilevanza:

Prima di andare a trattare la corrispondenza tra le risposte date dall'Ente e i livelli di maturità di ciascuna subcategory definita a priorità alta nella contestualizzazione del Framework è necessario andare a ridefinire il concetto di livello di maturità. I **livelli di maturità** forniscono un punto di riferimento in base al quale ogni Pubblica Amministrazione può valutare la propria implementazione delle subcategory presenti nel framework nazionale per la cybersecurity[2] della Sapienza e fissare obiettivi e priorità per la propria implementazione.

Nello specifico tratteremo i livelli di maturità come livelli progressivi in cui ogni livello superiore deve prevedere pratiche e controlli incrementali rispetto al livello di maturità inferiore. Ogni subcategory avrà un proprio numero di livelli di maturità fissati possibili, e questo numero varia da un **minimo** di 1 ad un **massimo** di 3 livelli di maturità per subcategory, più il livello "insufficiente". Ciò significa che avremo subcategory in cui è presente un unico livello di maturità (definito "Minimo") oltre a quello "insufficiente", altre con due possibili livelli di maturità ("Minimo" e "Standard") oltre a quello "insufficiente" e altre ancora con tre possibili livelli ("Minimo", "Standard" e "Alto"). Lo stesso framework nazionale per le cybersecurity[2] specifica che per alcune subcategory non è possibile definire dei livelli di maturità, perché quelle stesse subcategory non hanno più di una pratica implementativa da poter applicare.
Il numero dei livelli di maturità è stato deciso in conformità alle implementazioni che AgID fornisce per ciascuna subcategory legata al framework[1]. L'Agenzia per l'Italia digitale ha messo a disposizione infatti delle tecniche implementative alle quali è stata associata la rilevanza di quella stessa pratica rispetto alla subcategory corrispondente. La **rilevanza** di questi controlli è legata al livello di sicurezza che si riesce a raggiungere per una determinata subcategory se quella determinata pratica venisse implementata.

Abbiamo tre tipi di livelli di rilevanza:

1)**Alta:** indica una pratica che deve essere assolutamente implementata se si vuole avere un livello di sicurezza minimo. Corrisponde alla lettera M nella colonna "Liv" dell'allegato 2 della Circolare AgID n. 2/2017[1].
2)**Media:** una rilevanza di questo livello è associata a quei controlli che non sono fondamentali quanto quelli a rilevanza alta per la subcategory di riferimento, ma possono aumentare comunque il livello di sicurezza della stessa. Corrisponde alla lettera S nella colonna "Liv" dell'allegato 2 della Circolare AgID n. 2/2017[1].
3)**Bassa:** si tratta di pratiche di sicurezza che possono venir trattate come un obiettivo a cui tendere. Corrisponde alla lettera A nella colonna "Liv" dell'allegato 2 della Circolare AgID n. 2/2017[1].

I livelli di maturità sono stati definiti invece in questa maniera:
1)**Insufficiente**: specifica un livello di maturità in cui non sono stati adottati tutti i controlli a rilevanza Alta per una data subcategory
2)**Minimo:** sta ad indicare un livello di maturità in cui tutte le pratiche a rilevanza alta di una data subcategory vengono applicate dalla P.A.
3)**Standard:** un livello "standard" viene assegnato ad una determinata subcategory se tra i controlli applicabili alla stessa sono stati implementati tutti quelli a rilevanza alta ed almeno uno a rilevanza media o bassa, ma non sono state applicate tutte le procedure.
4)**Alto:** questo livello viene assegnato a quelle subcategory che hanno implementato tutti i controlli.

2.2 Assegnare i livelli di maturità in base all'analisi effettuata sull'Ente

Per le subcategory per le quali AgID ha definito procedure solo a rilevanza Alta[1], queste hanno due livelli di maturità: quello minimo e quello insufficiente (nel caso alcuni controlli non venissero applicati). Per le subcategory in cui invece sono stati definiti controlli a rilevanza Alta e solamente uno a rilevanza Media o Bassa, queste hanno tre livelli di maturità possibili: insufficiente , minimo e standard. Per tutte le altre sono stati definiti tutti e quattro i livelli di maturità: insufficiente, minimo, standard e alto.

2.3 Priorità

La colonna delle Priorità nella tabella di contestualizzazione del Framework Nazionale della cybersecurity per Pubbliche Amministrazioni locali fino a 20.000 abitanti è stata anch'essa definita guardando innanzitutto alle Misure Minime AgID[1].
In particolare, la regola seguita per definire la priorità di una determinate subcategory, è stata la seguente:

- Se la subcategory contiene anche una sola ABSC a rilevanza alta, la priorità per quella subcategory sarà ALTA.
- Se la subcategory contiene solo ABSC a rilevanza media o bassa, la priorità per quella subcategory sarà MEDIA.
- Se la subcategory contiene solo ABSC a rilevanza bassa, la priorità per quella subcategory sarà BASSA.
- Se la subcategory non può essere presa in considerazione perché riguarda ambiti non trattati dall'ente, la sua Priorità sarà definita NON SELEZIONATA. Resta inteso che, poiché la contestualizzazione è stata pensata per Comuni fino a 20.000 abitanti, è molto più probabile che un Comune che la adotti decida di "riattivare" la Priorità di una subcategory NON SELEZIONATA facendola diventare BASSA, piuttosto che "disattivare" una subcategory a Priorità ALTA, MEDIA o BASSA facendola diventare NON SELEZIONATA.

Per le subcatory a priorità ALTA, quindi, essendoci un rapporto diretto con le misure minime a rilevanza alta, si dovrà fare in modo che il livello di maturità dell'Ente sia necessariamente "minimo" e non "insufficiente". Questa dev'essere intesa come una prerogativa e un obbligo, così come indicato anche nella Circolare AgID n. 2/2017[1].

Per tutte le subcategory che non contengono riferimenti alle Misure Minime AgID[1], il criterio usato è quello del paragrafo 3.2 del Framework Nazionale per la Cybersecurity[1].
Si considerano i 3 fattori chiave del rischio cyber, ovvero:

1. esposizione alle minacce, intesa come l'insieme dei fattori che aumentano o diminuiscono la facilità con cui la minaccia stessa può manifestarsi;
2. probabilità di loro accadimento, ovvero la frequenza con cui una specifica minaccia può verificarsi nel tempo;
3. impatto conseguente sulle Business Operations o sugli Asset aziendali, intesa come l'entità del danno conseguente al verificarsi di una minaccia.

La definizione di priorità sarà, quindi:

ALTA	interventi che permettono di ridurre sensibilmente uno dei tre fattori chiave del rischio cyber. Questi interventi sono prioritari e per loro natura sono da attuare indipendentemente dalla complessità realizzativa degli stessi;
MEDIA	interventi che permettono di conseguire una riduzione di uno dei tre fattori chiave del rischio cyber e che risultano generalmente anche di semplice implementazione;
BASSA	interventi che permettono di conseguire una riduzione di uno dei tre fattori chiave del rischio cyber, ma la cui complessità realizzativa è generalmente considerata elevata (ad esempio cambiamenti organizzativi rilevanti e/o modifiche infrastrutturali significative)
NON SELEZIONATA	E' una subcategory che non esiste nel contesto in cui viene redatto il framework (PA Locali fino a 20.000 abitanti): di conseguenza potrebbe anche non essere indicata nella tabella del framework

I DATI DI QUESTE PAGINE SONO A DISPOSIZIONE UNICAMENTE DEL COMUNE DI MARSCIANO

I DATI DI QUESTE PAGINE SONO A DISPOSIZIONE UNICAMENTE DEL COMUNE DI MARSCIANO

I DATI DI QUESTE PAGINE SONO A DISPOSIZIONE UNICAMENTE DEL COMUNE DI MARSCIANO

I DATI DI QUESTE PAGINE SONO A DISPOSIZIONE UNICAMENTE DEL COMUNE DI MARSCIANO

I DATI DI QUESTE PAGINE SONO A DISPOSIZIONE UNICAMENTE DEL COMUNE DI MARSCIANO

I DATI DI QUESTE PAGINE SONO A DISPOSIZIONE UNICAMENTE DEL COMUNE DI MARSCIANO

I DATI DI QUESTE PAGINE SONO A DISPOSIZIONE UNICAMENTE DEL COMUNE DI MARSCIANO

I DATI DI QUESTE PAGINE SONO A DISPOSIZIONE UNICAMENTE DEL COMUNE DI MARSCIANO

I DATI DI QUESTE PAGINE SONO A DISPOSIZIONE UNICAMENTE DEL COMUNE DI MARSCIANO

I DATI DI QUESTE PAGINE SONO A DISPOSIZIONE UNICAMENTE DEL COMUNE DI MARSCIANO

I DATI DI QUESTE PAGINE SONO A DISPOSIZIONE UNICAMENTE DEL COMUNE DI MARSCIANO

RIFERIMENTI BIBLIOGRAFICI E SITOGRAFICI

1. Agenzia per l'Italia Digitale, *Misure Minime di sicurezza ICT per le Pubbliche Amministrazioni*: http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/cert-pa/misure-minime-sicurezza-ict-pubbliche-amministrazioni
2. 2015 Italian Cyber Security Report: http://www.cybersecurityframework.it/sites/default/files/CSR2015_web.pdf
3. ISTAT, *Rilevazione sulle Tecnologie dell'Informazione e della Comunicazione nelle Pubbliche Amministrazioni locali*: https://www.istat.it/it/archivio/195035
4. Roberto Balboni, Rocco De Nicola, Paolo Prinetto, *Il libro bianco sulla Cybersecurit. Il Futuro della Cybersecurity in Italia: Ambiti Progettuali Strategici*: https://www.consorzio-cini.it/images/Libro-Bianco-2018.pdf
5. *Dichiarazione congiunta dell'8 luglio 2016 dei presidenti del Consiglio europeo e della Commissione e del Segretario generale della NATO*: http://europa.eu/rapid/press-release_STATEMENT-16-2459_en.htm
6. *DPCM del 17 febbraio 2017 (GU n. 87 del 13 aprile 2017)*: http://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2017-04-13&atto.codiceRedazionale=17A02655&elenco30giorni=false

AUTORI E CONTATTI

Marco Caselli, Phd
marco@gruppopaosoft.com
www.gruppopaosoft.com

Dott. Carlo Ciocchetti
carlo@tcsconsulting.it
www.tcsconsulting.it

Dott.ssa Lucia Padiglioni
l.padiglioni@comune.marsciano.pg.it
D.ssa Chiara Poggioni
c.poggioni@comune.marsciano.pg.it
Dott. Massimiliano Cecchini
informatica@comune.marsciano.pg.it
www.comune.marsciano.pg.it