Città di
CAIRO
Montenotte

COPIA

VERBALE DELLA GIUNTA COMUNALE

SEDUTA NR. 47	**29/12/2017**
DELIBERAZIONE NR. 192	
ADEGUAMENTO DELL'INFRASTRUTTURA INFORMATICA COMUNALE ALLE "MISURE MINIME DI SICUREZZA ICT PER LE PUBBLICHE AMMINISTRAZIONI" DI CUI ALLA CIRCOLARE AGID N. 2 DEL 18 APRILE 2017 – APPROVAZIONE MODULO DI IMPLEMENTAZIONE E NOMINA DEL RESPONSABILE DELLA TRANSIZIONE ALLA MODALITÀ DIGITALE	

L'anno duemiladiciassette, questo giorno ventinove, del mese di dicembre, alle ore 8,50, legalmente convocata, si è riunita nella Sala delle Adunanze la Giunta Comunale.

Fatto l'appello risultano i Signori:

		Presente	Assente
- LAMBERTINI Paolo	Sindaco	SI	
- SPERANZA Roberto	Vice Sindaco	SI	
- BRIANO Maurizio	Assessore	SI	
- GARRA Caterina	Assessore		SI
- GHIONE Fabrizio	Assessore	SI	
- PIEMONTESI Ilaria	Assessore	SI	
		5	1

Partecipa alla seduta, incaricato della redazione del verbale, il Segretario Comunale Dott. Sandro AGNELLI.

Il Sindaco Paolo LAMBERTINI, assume la Presidenza e, constatato il numero legale degli intervenuti e la legalità dell'adunanza, invita i presenti alla trattazione dell'argomento indicato in oggetto.

29/12/2017

NR. 192

ADEGUAMENTO DELL'INFRASTRUTTURA INFORMATICA COMUNALE ALLE "MISURE MINIME DI SICUREZZA ICT PER LE PUBBLICHE AMMINISTRAZIONI" DI CUI ALLA CIRCOLARE AGID N. 2 DEL 18 APRILE 2017 – APPROVAZIONE MODULO DI IMPLEMENTAZIONE E NOMINA DEL RESPONSABILE DELLA TRANSIZIONE ALLA MODALITÀ DIGITALE

LA GIUNTA COMUNALE

VISTO il D.Lgs. 7 marzo 2005, n. 82 – Codice dell'Amministrazione Digitale (CAD) e s.m.i.;

VISTO il Piano Triennale per l'informatica nella PA 2017-2019, che definisce il modello di riferimento per lo sviluppo dell'informatica pubblica italiana nonché la strategia operativa di trasformazione digitale del Paese;

CONSIDERATO che a seguito della pubblicazione in Gazzetta Ufficiale (Serie Generale n. 103 del 05/05/2017) della Circolare Agid del 18 aprile 2017, n. 2/2017 "Misure minime di sicurezza ICT per le pubbliche amministrazioni (Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015)", che indica una serie di accorgimenti tecnico-organizzativi di obbligatoria adozione per tutte le Amministrazioni entro il 31/12/2017, si rende necessario individuare le azioni da intraprendere per adempiere alle prescrizioni con l'obiettivo di raggiungere un adeguato livello di sicurezza a garanzia del regolare funzionamento dell'infrastruttura informatica dell'Ente;

PRESO ATTO, pertanto, della necessità di disporre di un progetto preliminare che preveda un elenco di attività da svolgere, da parte di personale tecnico-sistemistico altamente specializzato, per prevenire e reagire ad eventi cibernetici e raggiungere gli obiettivi di sicurezza secondo gli standard forniti dall'AGID;

VISTO il modulo di implementazione alle misure minime ICT allegato alla presente deliberazione per farne parte integrante e sostanziale;

DATO ATTO che la predisposizione e l'approvazione del suddetto modulo non comportano spese aggiuntive a carico dell'Ente;

VISTA inoltre la necessità, per quanto stabilito dall'art.17 del CAD di individuare un responsabile comunale cui affidare la transizione alla modalità operativa digitale e i conseguenti processi di riorganizzazione finalizzati alla realizzazione di un'amministrazione digitale e aperta;

PRESO ATTO che tra i Servizi dell'Ente è previsto e di fatto funzionante il Servizio Sviluppo Informatico e Tecnologico, affidato alla responsabilità di apposita Posizione Organizzativa, idonea ad assumere anche la responsabilità e le mansioni relative alla transizione alla modalità digitale;

DATO ATTO che dette mansioni sono principalmente inerenti le attività di impulso e coordinamento relativi allo sviluppo dei sistemi informativi, allo sviluppo dei servizi interni ed esterni, alla sicurezza informatica di dati, sistemi e infrastrutture dell'amministrazione,

all'accesso dei soggetti disabili agli strumenti informatici, alla reingegnerizzazione dei processi, all'erogazione dei servizi in rete ai cittadini;

VISTI:

- lo Statuto comunale;
- il vigente regolamento di Contabilità;
- il decreto legislativo 18 agosto 2000 n. 267, recante il "Testo Unico delle leggi sull'ordinamento degli enti locali";

VISTO il parere espresso dal Dirigente del Terzo Settore in ordine alla regolarità tecnica ai sensi dell'art. 49 del D. Lgs. 267/2000, allegato al presente atto quale parte sostanziale;

Ad unanimità di voti espressi nella forma di legge;

DELIBERA

Per le motivazioni espresse in premessa,

1. di approvare il modulo di implementazione alle misure minime ICT così come allegato alla presente deliberazione per farne parte integrante e sostanziale nel quale si individuano le azioni da intraprendere per adempiere alle prescrizioni della circolare Agid del 18 aprile 2017 con l'obiettivo di raggiungere un adeguato livello di sicurezza a garanzia del regolare funzionamento dell'infrastruttura comunale;
2. di dare atto che la predisposizione el'approvazione del modulo allegato non comportano spese aggiuntive a carico dell'Ente;
3. di individuare nel Servizio Sviluppo Informatico l'Ufficio di riferimento per la transizione alla modalità digitale e di nominare quale responsabile la Posizione Organizzativa responsabile del Servizio stesso.

Successivamente,

LA GIUNTA COMUNALE

RAVVISATA la necessità di dare immediata esecuzione al presente atto, vista la necessità di approvare il modulo di implementazione alle misure minime ICT e la nomina del responsabile che lo dovrà sottoscrivere unitamente al Rappresentante Legale dell'Ente entro il 31/12/2017.

CON VOTI UNANIMI espressi nelle forme di legge, ai sensi e per gli effetti dell'art.134, quarto comma, del Decreto Legislativo 18/08/2000 n.267;

DELIBERA

la presente deliberazione è dichiarata immediatamente esecutiva.

AGID – MISURE MINIME DI SICUREZZA – MODULO DI IMPLEMENTAZIONE

PREMESSA

CIRCOLARE 18 aprile 2017 , n. 2/2017 .

Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)».

Premessa.

L'art. 14-*bis* del decreto legislativo 7 marzo 2005, n. 82, di seguito C.A.D., al comma 2, lettera *a)*, tra le funzioni attribuite all'AgID, prevede, tra l'altro, l'emanazione di regole, standard e guide tecniche, nonché di vigilanza e controllo sul rispetto delle norme di cui al medesimo C.A.D., anche attraverso l'adozione di atti amministrativi generali, in materia di sicurezza informatica.

La direttiva del 1° agosto 2015 del Presidente del Consiglio dei ministri impone l'adozione di standard minimi di prevenzione e reazione ad eventi cibernetici. Al fi ne di agevolare tale processo, individua nell'Agenzia per l'Italia digitale l'organismo che dovrà rendere prontamente disponibili gli indicatori degli standard di riferimento, in linea con quelli posseduti dai maggiori partner del nostro Paese e dalle organizzazioni internazionali di cui l'Italia è parte.

L a presente circolare sostituisce la circolare AgID n. 1/2017 del 17 marzo 2017 (pubblicata nella *Gazzetta Uffi ciale* n. 79 del 4 aprile 2017).

Art. 1.

S c o p o

Obiettivo della presente circolare è indicare alle pubbliche amministrazioni le misure minime per la sicurezza ICT che debbono essere adottate al fi ne di contrastare le minacce più comuni e frequenti cui sono soggetti i loro sistemi informativi.

L e 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.

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

Art. 5.

Tempi di attuazione

Entro il **31 dicembre 2017** le amministrazioni dovranno attuare gli adempimenti di cui agli articoli precedenti.

MISURE MINIME DI SICUREZZA ICT

PER LE PUBBLICHE AMMINISTRAZIONI

(*Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015*)

26 APRILE 2016

1. GENERALITÀ.

1.1. SCOPO.

Il presente documento contiene le misure minime di sicurezza ICT per le pubbliche amministrazioni le quali costituiscono parte integrante delle linee guida per la sicurezza ICT delle pubbliche amministrazioni.

Q uesto documento è emesso in attuazione della direttiva del Presidente del Consiglio dei ministri 1° agosto 2015 e costituisce un'anticipazione urgente della regolamentazione completa in corso di emanazione, al fi ne di fornire alle pubbliche amministrazioni dei criteri di riferimento per stabilire se il livello di protezione offerto da un'infrastruttura risponda alle esigenze operative, individuando anche gli interventi idonei per il suo adeguamento.

1.2 STORIA DELLE MODIFICHE

Ver.	Descrizione delle modifiche	Data emissione
1.0	Prima versione	26/04/2016

1.3 RIFERIMENTI

	ID	Descrizione
[D.1]	Direttiva 1 agosto 2015	Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015
[D.2]	SANS 20	CIS Critical Security Controls for Effective Cyber Defense - versione 6.0 di ottobre 2015
[D.3]	Cyber Security Report	La Sapienza - 2015 Italian Cyber Security Report del CIS -

1.4 ACRONIMI

Acronimo	Descrizione
ABSC	Agid Basic Security Control(s)
CCSC	Center for Critical Security Control
CSC	Critical Security Control

FNSC	Framework Nazionale di Sicurezza Cibernetica
NSC	Nucleo di Sicurezza Cibernetica

2. PREMESSA.

La direttiva del Presidente del Consiglio dei ministri 1° agosto 2015, in considerazione dell'esigenza di consolidare un sistema di reazione effi ciente, che raccordi le capacità di risposta delle singole amministrazioni, con l'obiettivo di assicurare la resilienza dell'infrastruttura informatica nazionale, a fronte di eventi quali incidenti o azioni ostili che possono compromettere il funzionamento dei sistemi e degli assetti fi sici controllati dagli stessi, visto anche l'inasprirsi del quadro generale con un preoccupante aumento degli eventi cibernetici a carico della pubblica amministrazione, sollecita tutte le amministrazioni e gli organi chiamati ad intervenire nell'ambito degli assetti nazionali di reazione ad eventi cibernetici a dotarsi, secondo una tempistica defi nita e comunque nel più breve tempo possibile, di standard minimi di prevenzione e reazione ad eventi cibernetici. A fi ne di agevolare tale processo l'Agenzia per l'Italia digitale è stata impegnata a rendere prontamente disponibili indicatori degli standard di riferimento, in linea con quelli posseduti dai maggiori partner del nostro Paese e dalle organizzazioni internazionali di cui l'Italia è parte.

L'Agenzia è costantemente impegnata nell'aggiornamento continuo della normativa tecnica relativa alla sicurezza informatica della pubblica amministrazione ed in particolare delle regole tecniche per la sicurezza informatica delle pubbliche amministrazioni la cui emanazione è però di competenza del Dipartimento per la funzione pubblica e richiede l'espletamento delle procedure previste dalla normativa comunitaria per la regolamentazione tecnica. Pertanto il presente documento, che contiene le misure minime di sicurezza ICT per le pubbliche amministrazioni e costituisce parte integrante delle linee guida per la sicurezza ICT delle pubbliche amministrazioni, viene pubblicato, in attuazione della direttiva sopra citata, come anticipazione urgente della regolamentazione in corso di emanazione, al fi ne di fornire un riferimento utile a stabilire se il livello di protezione offerto da un'infrastruttura risponde alle esigenze operative, individuando anche gli interventi idonei per il suo adeguamento.

La scelta di prendere le mosse dall'insieme di controlli noto come SANS 20, oggi pubblicato dal Center for Internet Security come CCSC «CIS Critical Security Controls for Effective Cyber Defense» nella versione 6.0 di ottobre 2015, trova giustifi cazione, oltre che nella larga diffusione ed utilizzo pratico, dal fatto che esso nasce con una particolare sensibilità per i costi di vario genere che l'implementazione di una misura di sicurezza richiede, ed i benefi ci che per contro è in grado di offrire. L'elenco dei venti controlli in cui esso si articola, normalmente riferiti come Critical Security Control (CSC), è ordinato sulla base dell'impatto sulla sicurezza dei sistemi; per cui ciascun controllo precede tutti quelli la cui implementazione innalza il livello di sicurezza in misura inferiore alla sua. È comune convinzione che i primi cinque controlli siano quelli indispensabili per assicurare il minimo livello di protezione nella maggior parte delle situazioni e da questi si è partiti per stabilire le misure minime di sicurezza per la pubblica amministrazione italiana, avendo ben presente le enormi differenze di dimensioni, mandato, tipologie di informazioni gestite, esposizione al rischio, e quant'altro caratterizza le oltre ventimila amministrazioni pubbliche.

In realtà nel defi nire gli AgID Basic Security Control(s) (ABSC) si è partiti dal confronto tra le versioni 6.0 e 5.1 dei CCSC, che può essere assunto quale indicatore dell'evoluzione della minaccia cibernetica nel corso degli ultimi anni. È infatti evidente l'aumento di importanza delle misure relative agli amministratori di sistema, che balzano dal 12° al 5° posto, entrando nella rosa dei Quick Win, mentre la sicurezza applicativa scivola dal 6° al 18° posto e gli accessi wireless dal 7° al 15° a causa della diffusione delle contromisure atte a contrastare le vulnerabilità tipiche di tali ambiti. In defi nitiva, anche per facilitare il confronto con la defi nizione originale, si è deciso di fare riferimento, nell'identifi cazione degli ABSC, alla versione 6 dei CCSC. Tuttavia l'insieme dei controlli defi niti è più vicino a quello della versione 5.1 poiché si è ritenuto che molti di quelli che nel passaggio alla nuova versione sono stati eliminati, probabilmente perché non più attuali nella realtà statunitense, siano ancora importanti nel contesto della pubblica amministrazione italiana.

Occorre inoltre osservare che il CCSC è stato concepito essenzialmente nell'ottica di prevenire e contrastare gli attacchi cibernetici, ragione per la quale non viene data particolare rilevanza agli eventi di sicurezza dovuti a casualità quali guasti ed eventi naturali. Per questa ragione, ai controlli delle prime cinque classi si è deciso di aggiungere quelli della CSC8, relativa alle difese contro i malware, della CSC10, relativa alle copie di sicurezza, unico strumento in grado di proteggere sempre e comunque le informazioni dal rischio di perdita, e della CSC13, riferita alla protezione dei dati rilevanti contro i rischi di esfi ltrazione.

I n realtà ciascun CSC è costituito da una famiglia di misure di dettaglio più fi ne, che possono essere adottate in modo indipendente, consentendo un'ulteriore modulazione utile ad adattare il sistema di sicurezza alla effettiva realtà locale. Nonostante ciò si è ritenuto che anche al secondo livello ci fosse una granularità ancora eccessiva, soprattutto sotto il profi lo implementativo, che avrebbe costretto soprattutto le piccole amministrazioni ad introdurre misure esagerate per la propria organizzazione. Per tale ragione è stato introdotto un ulteriore terzo livello, nel quale la misura di secondo livello viene decomposta in misure elementari, ancora una volta implementabili in modo indipendente. Pertanto un ABSC è identifi cato da un identifi catore gerarchico a tre livelli x, y, z, dove x e y sono i numeri che identifi cano il CSC concettualmente corrispondente e z individua ciascuno dei controlli di livello 3 in cui questo è stato raffi nato.

Al primo livello, che corrisponde ad una famiglia di controlli destinati al perseguimento del medesimo obiettivo, è associata una tabella che li contiene tutti. Nella prima colonna, sviluppata gerarchicamente su tre livelli, viene defi nito l'identifi catore univoco di ciascuno di essi. La successiva colonna «Descrizione» specifi ca il controllo attraverso una defi nizione sintetica.

Nella terza colonna, «FNSC» (Framework nazionale di sicurezza cibernetica), viene indicato l'identifi catore della Subcategory del Framework Core del Framework nazionale per la Cyber Security, proposto con il 2015 Italian Cyber Security Report del CIS «La Sapienza» presentato lo scorso 4 febbraio 2016, al quale il controllo è riconducibile. Pur non intendendo costituire una contestualizzazione del Framework, le misure minime concretizzano praticamente le più importanti ed effi caci azioni che questo guida ad intraprendere. Per il diverso contesto di provenienza ed il differente obiettivo che i due strumenti intendono perseguire, le misure minime pongono l'accento sopra gli aspetti di prevenzione piuttosto che su quelli di risposta e ripristino.

L e ultime tre colonne sono booleane e costituiscono una linea guida che indica quali controlli dovrebbero essere implementati per ottenere un determinato livello di sicurezza. La prima, «Minimo», specifi ca il livello sotto il quale nessuna amministrazione può scendere: i controlli in essa indicati debbono riguardarsi come obbligatori. La seconda, «Standard», può essere assunta come base di riferimento nella maggior parte dei casi, mentre la terza, «Alto», può riguardarsi come un obiettivo a cui tendere.

Il raggiungimento di elevati livelli di sicurezza, quando è molto elevata la complessità della struttura e l'eterogeneità dei servizi erogati, può essere eccessivamente oneroso se applicato in modo generalizzato. Pertanto ogni amministrazione dovrà avere cura di individuare al suo interno gli eventuali sottoinsiemi, tecnici e/o organizzativi, caratterizzati da omogeneità di requisiti ed obiettivi di sicurezza, all'interno dei quali potrà applicare in modo omogeneo le misure adatte al raggiungimento degli obiettivi stessi.
Le amministrazioni NSC, per l'infrastruttura che gestisce dati NSC, dovrebbero collocarsi almeno a livello "standard" in assenza di requisiti più elevati.

3. LA MINACCIA CIBERNETICA PER LA PUBBLICA AMMINISTRAZIONE.

Nel recente passato si è assistito ad una rapida evoluzione della minaccia cibernetica ed in particolare per quella incombente sulla pubblica amministrazione, che è divenuta un bersaglio specifi co per alcune tipologie di attaccanti particolarmente pericolosi.
Se da un lato la pubblica amministrazione continua ad essere oggetto di attacchi dimostrativi, provenienti da soggetti spinti da motivazioni politiche ed ideologiche, sono divenuti importanti e pericolose le attività condotte da gruppi organizzati, non solo di stampo propriamente criminale. I pericoli legati a questo genere di minaccia sono particolarmente gravi per due ordini di motivi. Il primo è la quantità di risorse che gli attaccanti possono mettere in campo, che si rifl ette sulla sofi sticazione delle strategie e degli strumenti utilizzati. Il secondo è che il primo obiettivo perseguito è il mascheramento dell'attività, in modo tale che questa possa procedere senza destare sospetti. La combinazione di questi due fattori fa sì che queste misure minime, pur tenendo nella massima considerazione le difese tradizionali, quali gli antivirus e la difesa perimetrale, pongano l'accento sulle misure rivolte ad assicurare che le attività degli utenti rimangano sempre all'interno dei limiti previsti. Infatti elemento comune e caratteristico degli attacchi più pericolosi è l'assunzione del controllo remoto della macchina attraverso una scalata ai privilegi.
Nei fatti le misure preventive, destinate ad impedire il successo dell'attacco, devono essere affi ancate da effi caci strumenti di rilevazione, in grado di abbreviare i tempi, oggi pericolosamente lunghi, che intercorrono dal momento in cui l'attacco primario è avvenuto e quello in cui le conseguenze vengono scoperte. Oltre tutto una lunga latenza della compromissione rende estremamente complessa, per la mancanza di log, modifi che di confi gurazione e anche avvicendamenti del personale, l'individuazione dell'attacco primario, impedendo l'attivazione di strumenti effi caci di prevenzione che possano sicuramente impedire il ripetersi degli eventi.
In questo quadro diviene fondamentale la rilevazione delle anomalie operative e ciò rende conto dell'importanza data agli inventari, che costituiscono le prime due classi di misure, nonché la protezione della confi gurazione, che è quella immediatamente successiva.
La quarta classe deve la sua priorità alla duplice rilevanza dell'analisi delle vulnerabilità. In primo luogo le vulnerabilità sono l'elemento essenziale per la scalata ai privilegi che è condizione determinante per il successo dell'attacco; pertanto la loro eliminazione è la misura di prevenzione più effi cace. Secondariamente si deve considerare che l'analisi dei sistemi è il momento in cui è più facile rilevare le alterazioni eventualmente intervenute e rilevare un attacco in corso.
La quinta classe è rivolta alla gestione degli utenti, in particolare gli amministratori. La sua rilevanza è dimostrata dall'ascesa, accennata in premessa, dal 12° al 5° posto nelle SANS 20, motivata dalle considerazioni cui si è fatto riferimento poco dianzi.
La sesta classe deve la sua considerazione al fatto che anche gli attacchi complessi prevedono in qualche fase l'installazione di codice malevolo e la sua individuazione può impedirne il successo o rilevarne la presenza.
Le copie di sicurezza, settima classe, sono alla fi ne dei conti l'unico strumento che garantisce il ripristino dopo un incidente.
L'ultima classe, la protezione dei dati, deve la sua presenza alla considerazione che l'obiettivo principale degli attacchi più gravi è la sottrazione di informazioni.

MODULO DI IMPLEMENTAZIONE MISURE MINIME ICT

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	File Excel chiamato “Inventario dispositivi” in fase di approntamento. Verrà conservato sul server “**servercivilia**” nella cartella al percorso **D:\DOCUMENTAZIONE AGID MISURE MINIME** e posto sotto backup automatizzato dell’Ente.
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	Ad ogni nuovo dispositivo collegato alla rete, il file di cui all’ID 1.1.1 “Inventario dispositivi” verrà aggiornato.
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.	Il file “Inventario dispositivi” riporta al suo interno anche l’indirizzo IP di ogni singola risorsa di rete.

ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
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.	File Excel chiamato “Elenco software autorizzati” in fase di approntamento. Verrà conservato sul server “**servercivilia**” nella cartella al percorso **D:\DOCUMENTAZIONE AGID MISURE MINIME** e posto sotto backup automatizzato dell’Ente.
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	E’ prevista la regolare scansione dei sistemi attraverso apposito software di rilevamento centralizzato su server.

ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

ABSC_ID			Livello	Descrizione	Modalità di implementazione
3	1	1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	E' in fase di approntamento apposito documento di Word denominato "Configurazioni standard" contenente il riepilogo di cosa viene installato sulle singole postazioni (suddiviso per server e workstation). Il file verrà conservato sul server "**servercivilia**" nella cartella al percorso **D:\DOCUMENTAZIONE AGID MISURE MINIME** e posto sotto backup automatizzato dell'Ente.
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Si veda il precedente punto 3.1.1
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Si veda il precedente punto 3.1.1
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Verranno create immagini standard dei PC (attualmente assenti) suddivise per tipologia hardware. Le immagini verranno storate in apposito NAS via FTP (da inserire ex-novo nella rete comunale) attraverso apposito software di backup (il NAS non sarà mai visibile nella rete neppure come condivisione). Stessa implementazione verrà eseguita per i server.
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).	Attualmente sono già presenti connessioni VPN protette.

ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

ABSC_ID			Livello	Descrizione	Modalità di implementazione
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.	Attualmente viene eseguita una ricerca delle vulnerabilità attraverso lo strumento di aggiornamento automatico dei sistemi Windows, sia sui server che sui PC della rete.
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	Si veda il precedente punto 4.1.1
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Si veda il precedente punto 4.1.1
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 criticità.	Allo stato attuale l'unica sede nella quale i PC non sono gestiti da Server è la sede distaccata del Palazzo di Città/ Biblioteca: in questa sede vengono adottate misure adeguate per l'aggiornamento dei sistemi.
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.	Eventuali sistemi non aggiornabili per motivi di compatibilità con i software applicativi autorizzati, vengono elencati nel file "Sistemi non aggiornabili" conservato sul server "**servercivilia**" nella cartella al percorso **D:\DOCUMENTAZIONE AGID MISURE MINIME** e posto sotto backup automatizzato dell'Ente.
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.).	Verrà predisposto ad inizio 2018.
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.	Si veda il precedente punto 4.8.1

ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
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.	Gli utenti sono tutti configurati come “power user” e non godono quindi di privilegi amministrativi, ad eccezione di quelli elencati nel file di inventario di cui al prossimo punto 5.2.1
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Sui server gli accessi vengono registrati attraverso apposito software di log. Sui PC Clients il solo utente amministratore (esclusi gli amministratori di rete) è l’utente locale chiamato “amministratore”, il quale viene gestito dall’Amministratore di Sistema su tutti i PC e con uguale password.
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	E’ in fase di approntamento apposito documento di Word denominato “Amministratori di sistema autorizzati” contenente il riepilogo in elenco degli amministratori di sistema autorizzati. Questi ultimi verranno autorizzati attraverso specifica comunicazione inviata via mail. Il file verrà conservato sul server “**servercivilia**” nella cartella al percorso **D:\DOCUMENTAZIONE AGID MISURE MINIME** e posto sotto backup automatizzato dell’Ente.
5	3	1	M	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.	La procedura verrà documentata attraverso un apposito file di Word denominato “Procedure per l’uso appropriato dei privilegi di Amministratore” in fase di approntamento. Il file verrà conservato sul server “**servercivilia**” nella cartella al percorso **D:\DOCUMENTAZIONE AGID MISURE MINIME** e posto sotto backup automatizzato dell’Ente.
5	7	1	M	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).	Già in uso. Verrà documentata nel file di cui al precedente punto 5.3.1
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Già in uso. Verrà documentata nel file di cui al precedente punto 5.3.1

5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Già in uso. Verrà documentata nel file di cui al precedente punto 5.3.1
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Già in uso. Verrà documentata nel file di cui al precedente punto 5.3.1
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Già in uso. Verrà documentata nel file di cui al precedente punto 5.3.1
5	10	3	M	Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.	Già in uso. Verrà documentata nel file di cui al precedente punto 5.3.1
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	L'elenco delle credenziali amministrative sono indicate in un apposito file di Excel denominato "Elenco credenziali amministrative" in fase di approntamento. Il file verrà conservato sul server "**servercivilia**" nella cartella al percorso **D:\DOCUMENTAZIONE AGID MISURE MINIME** e posto sotto backup automatizzato dell'Ente.
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Già in uso. Verrà documentata nel file di cui al precedente punto 5.3.1

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
8	1	1	M	Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.	E' presente un antivirus con console centralizzata sul Server comunale e su quello della Polizia Municipale, le quali provvedono alla distribuzione automatica delle definizioni ai PC Clients. Sono attivi gli aggiornamenti automatici sui server e sui singoli PC per l'applicazione delle patch di sicurezza.
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	E' presente un firewall perimetrale, a protezione dell'intera rete comunale e della rete della Polizia Municipale.
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Non vengono utilizzati dispositivi esterni se non previa autorizzazione all'uso da parte dell'Amministratore di Sistema.
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	E' già impostato il blocco dell'esecuzione automatica sulle singole postazioni di lavoro.
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	E' già impostato il blocco dell'esecuzione di macro presenti nei files di lavoro.
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	E' impostata la sola visualizzazione delle intestazioni.
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	E' già disattivata su tutte le postazioni.
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	E' già impostata come regola nel software antivirus.
8	9	1	M	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.	Non è presente alcun filtro antispam in capo alle caselle mail. E' in fase di valutazione una futura implementazione dello stesso.
8	9	2	M	Filtrare il contenuto del traffico web.	E' già attivo il filtro del contenuto del traffico web per mezzo del firewall perimetrale comunale.
8	9	3	M	Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab).	Si veda il precedente punto 8.9.1

ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID			Livello	Descrizione	Modalità di implementazione
10	1	1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	Già pianificati una serie di flussi di backup automatizzati con cadenza specificata in un apposito file di Word denominato “Pianificazione flussi di backup” in fase di approntamento. Il file verrà conservato sul server “**servercivilia**” nella cartella al percorso **D:\DOCUMENTAZIONE AGID MISURE MINIME** e posto sotto backup automatizzato dell’Ente. E’ di prossima implementazione un sistema di backup delle macchine virtuali presenti sul server comunale.
10	3	1	M	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.	Attualmente non è adottato nessun sistema di cifratura in quanto tutti i documenti di lavoro ed i database risultano essere presenti unicamente sui server interni alle diverse sedi comunali. Non sono, allo stato attuale delle cose, impostati backup remoti su cloud.
10	4	1	M	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.	Di prossima implementazione è prevista la tenuta sul NAS di cui al punto 3.3.1 di una copia mensile delle macchine virtuali. I dati non saranno accessibili in nessun modo attraverso la rete dati, ma solo attraverso connessione FTP.

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
13	1	1	M	Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica	Da una prima valutazione eseguita non sono stati individuati dati che richiedano particolari requisiti di riservatezza e che quindi necessitino di una protezione mediante crittografia.
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	Il firewall perimetrale implementa già un content filtering per il blocco da e verso URL. Verranno a breve definite le regole di blocco da e verso URL specifiche.

Città di
CAIRO
Montenotte

AREA AFFARI GENERALI
protocollo@comunecairo.it

PARERI ALLA

- deliberazione Consiglio Comunale ☐
- deliberazione Giunta Comunale ☒

OGGETTO: ADEGUAMENTO DELL'INFRASTRUTTURA INFORMATICA COMUNALE ALLE "MISURE MINIME DI SICUREZZA ICT PER LE PUBBLICHE AMMINISTRAZIONI" DI CUI ALLA CIRCOLARE AGID N. 2 DEL 18 APRILE 2017 – APPROVAZIONE MODULO DI IMPLEMENTAZIONE E NOMINA DEL RESPONSABILE DELLA TRANSIZIONE ALLA MODALITÀ DIGITALE

Ai sensi e per gli effetti dell'art. 49 del D.Lgs 18 agosto 2000 n. 267, viene espresso il seguente parere: FAVOREVOLE

Cairo Montenotte, li, 29/12/2017

IL DIRIGENTE TERZO SETTORE
AREA AFFARI GENERALI
Dott. Sandro AGNELLI

Letto, confermato e sottoscritto.

IL PRESIDENTE	IL SEGRETARIO COMUNALE
F.to P. LAMBERTINI	F.to S. AGNELLI

REFERTO DI PUBBLICAZIONE

L'Istruttore incaricato alla pubblicazione attesta che copia della presente deliberazione viene pubblicata all'Albo Pretorio on line del Comune il giorno 29/12/2017 e vi rimarrà per 15 (quindici) giorni interi e consecutivi ai sensi dell'art. 124 - 1° comma - del D.Lgs 18/08/2000, nr. 267.

Cairo Montenotte, li 29/12/2017

L'ISTRUTTORE DIRETTIVO
F.to N. CHINELLI

La presente deliberazione è dichiarata [X] **IMMEDIATAMENTE ESEGUIBILE**

CERTIFICATO DI ESECUTIVITÀ
(Art. 134, 3° comma, del D.Lgs. 18/08/2000 - nr. 267)

La presente deliberazione è divenuta esecutiva il

Cairo Montenotte, li

E' copia conforme all'originale, in carta libera, per uso amministrativo.

Cairo Montenotte, li 29/12/2017

Visto:

IL RESPONSABILE DEL SERVIZIO
Alessandro GHIONE

La firma autografa è sostituita dall'indicazione a stampa del nominativo del Responsabile del Procedimento ai sensi dell'art. 3 del D.Lgs. 12 febbraio 1993 n. 39