COMUNE DI SORTINO
(Prov. Reg. di SIRACUSA)

COPIA DELIBERAZIONE DELLA GIUNTA COMUNALE

N.51 DEL 18-5-2022 OGGETTO: APPROVAZIONE MISURE MINIME DI SICUREZZA ICT PER LE PUBBLICHE AMMINISTRAZIONI - CIRCOLARE AGID N. 2/2017

L'anno duemilaventidue il giorno DICIOTTO del mese di MAGGIO alle ore 19.00 nella Sala delle Adunanze della sede comunale, si è riunita la Giunta Comunale convocata nelle forme di legge.-

Presiede l'adunanza il Sig. Vincenzo Parlato nella sua qualità di Sindaco e sono rispettivamente presenti ed assenti i seguenti Sigg:

COMPOSIZIONE DELLA GIUNTA COMUNALE		*PRESENTI*	*ASSENTI*
1) SIG. VINCENZO PARLATO	*SINDACO*	X	
2) DOTT. GIUSEPPE MESSINA	*VICE SINDACO*	X	
3) DOTT. VINCENZO BASTANTE	*ASSESSORE*	X	
4) SIG. SEBASTIANO PALI'	*ASSESSORE*	X	
5) SIG. RA CARMELA TUCCITTO	*ASSESSORE*	X	
	TOTALE	5	

Con la partecipazione del segretario Comunale dr. Bartolotta Antonino
Il Presidente, constatato che gli intervenuti sono in numero legale, dichiara aperta la riunione ed invita i convocati a deliberare sull'oggetto sopraindicato;

LA GIUNTA COMUNALE

Premesso che sulla presente deliberazione relativa all'oggetto hanno espresso parere:

il responsabile del servizio interessato, per quanto concerne la regolarità tecnica:

- ☒ ***FAVOREVOLE***
- ☐ ***CONTRARIO PER LE SEGUENTI MOTIVAZIONI:_____***
- ☐ ***NON NECESSARIO IN QUANTO ATTO DI MERO INDIRIZZO.***

DATA 18/05/2022 ***F.to IL RESPONSABILE*** DOT. L. RAGNANO

il responsabile di ragioneria, per quanto concerne la responsabilità contabile e/o la copertura finanziaria ai sensi dell'Art.55 L.R.n.44/91:

- ☐ ***FAVOREVOLE***
- ☐ ***CONTRARIO CON LE SEGUENTI MOTIVAZIONI:_____***
- ☒ ***NON NECESSARIO IN QUANTO DALL'ATTO NON SCATURISCE IMPEGNO DI SPESA.***
- ☐ ***DATA*** 18-05-2022 ***F.to IL RESPONSABILE*** SIG. R. TUCCITTO

Deliberazione: Giunta Comunale

Area competente: Area Amministrativa

Responsabile del Procedimento: Dott. Luciano Magnano

Proponente: Dott. Luciano Magnano

OGGETTO: APPROVAZIONE MISURE MINIME DI SICUREZZA ICT PER LE PUBBLICHE AMMINISTRAZIONI - CIRCOLARE AGID N. 2/2017

LA GIUNTA COMUNALE

PREMESSO CHE:

- gli attacchi informatici ai sistemi rappresentano oggi un elemento di grande criticità per le aziende private e le pubbliche amministrazioni;
- l'attenzione del legislatore e del governo nazionale ed europeo è volta ad attività di prevenzione e difesa rispetto agli attacchi informatici e più in generale a favorire le azioni di ICT Security delle Pubbliche Amministrazioni;
- in questo contesto sono stati emanati vari provvedimenti legislativi quali il DPCM del 24 Gennaio 2013 recante "indirizzi per la protezione cibernetica e la sicurezza informatica nazionale", il DPCM 27 gennaio 2014 che approva il "quadro strategico nazionale per la sicurezza dello spazio cibernetico" e la direttiva 1 agosto 2015 della Presidenza del Consiglio "Sistema di informazione per la sicurezza della Repubblica";

DATO ATTO altresì che 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;

RICHIAMATA a tal fine la direttiva del 1° agosto 2015 del Presidente del Consiglio dei Ministri che ha imposto l'adozione di standard minimi di prevenzione e reazione ad eventi cibernetici. Al fine 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;

VISTA e richiamata la circolare della AGENZIA PER L'ITALIA DIGITALE n. 2 del 18 aprile 2017, rubricata "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)»." (la presente circolare sostituisce la circolare AgID n. 1/2017 del 17 marzo 2017 (pubblicata nella Gazzetta Ufficiale n. 79 del 4 aprile 2017) con cui sono introdotti l'insieme dei controlli che costituiscono le Misure Minime AgID, denominati AgID Basic Security Controls (ABSC) partendo dalla base, già consolidata e assai apprezzata dalla comunità mondiale degli esperti di

sicurezza, costituita dai cosiddetti "SANS 20" (oggi noti come Critical Security Controls) emessi dal SANS Institute;

DATO ATTO:

- i singoli controlli CSC sono stati trasposti nei controlli ABSC suddividendoli in famiglie di misure di dettaglio più fine, che possono essere adottate in modo indipendente per consentire alle Amministrazioni di graduare il proprio sistema di sicurezza per meglio adattarlo alle effettive esigenze della specifica realtà locale;
- che per facilitarne ulteriormente l'adozione, minimizzando gli impatti implementativi sull'organizzazione interessata, i controlli sono inoltre stati suddivisi in tre gruppi verticali, riferiti a livelli complessivi di sicurezza crescente. I controlli del primo gruppo (livello "Minimo") sono quelli strettamente obbligatori ai quali ogni Pubblica Amministrazione, indipendentemente dalla sua natura e dimensione, deve essere conforme in termini tecnologici, organizzativi e procedurali: essi dunque rappresentano complessivamente il livello sotto al quale nessuna Amministrazione può scendere;
- che i controlli del secondo gruppo (livello "Standard") rappresentano la base di riferimento per la maggior parte delle Amministrazioni, e costituiscono un ragionevole compromesso fra efficacia delle misure preventive ed onerosità della loro implementazione;
- che i controlli del terzo gruppo (livello "Alto") rappresentano infine il livello adeguato per le organizzazioni maggiormente esposte a rischi, ad esempio per la criticità delle informazioni trattate o dei servizi erogati, ma anche l'obiettivo ideale cui tutte le altre organizzazioni dovrebbero tendere.

PRESO ATTO che ogni Amministrazione dovrà pertanto avere cura di individuare al suo interno gli eventuali sottoinsiemi tecnici e/o organizzativi, caratterizzati da una sostanziale omogeneità di requisiti ed obiettivi di sicurezza, all'interno dei quali potrà applicare in modo omogeneo le misure adatte al raggiungimento degli obiettivi stessi;

PRECISATO che per quanto riguarda i contenuti, le Misure Minime prevedono, nella loro formulazione attuale, otto insiemi (o "classi") di controlli così dettagliati:

- I controlli delle prime due classi (ABSC 1 e 2) riguardano rispettivamente l'inventario dei dispositivi autorizzati e non autorizzati e quello dei software autorizzati e non autorizzati. In pratica essi impongono all'organizzazione di gestire attivamente i dispositivi hardware e i pacchetti software in uso, predisponendo e mantenendo aggiornati, a diversi livelli di dettaglio e con differenti modalità attuative a seconda del livello di sicurezza, i rispettivi inventari, e prevedendo inoltre meccanismi per individuare e/o impedire tutte le anomalie operative, ossia l'impiego di elementi non noti e/o esplicitamente autorizzati.
- I controlli della terza classe (ABSC 3) riguardano la protezione delle configurazioni hardware e software sui sistemi in uso presso l'organizzazione.
- I controlli della quarta classe (ABSC 4) sono finalizzati ad individuare tempestivamente, e correggere, le vulnerabilità dei sistemi in uso, minimizzando la finestra temporale nella quale le vulnerabilità presenti possono essere sfruttate per condurre attacchi contro l'organizzazione.
- I controlli della quinta classe (ABSC 5) sono rivolti alla gestione degli utenti, in particolare gli amministratori, ed hanno lo scopo di assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi sui sistemi in uso.
- I controlli della sesta classe (ABSC 8) hanno lo scopo di contrastare l'ingresso e la diffusione nell'organizzazione di codice malevolo di qualsiasi provenienza.
- I controlli della settima classe (ABSC 10) sono relativi alla gestione delle copie di

sicurezza delle informazioni critiche dell'organizzazione, che in ultima analisi sono l'unico strumento che garantisce il ripristino dopo un incidente.

- L'ottava ed ultima classe (ABSC 13) riguarda infine la protezione contro l'esfiltrazione dei dati dell'organizzazione, in considerazione del fatto che l'obiettivo principale degli attacchi più gravi è la sottrazione di informazioni.

PRESO ATTO pertanto che, come previsto dalla citata circolare, ciascuna Amministrazione debba non solo implementare i controlli rilevanti, ma anche dare brevemente conto della modalità di implementazione compilando un apposito modulo il quale andrà poi firmato digitalmente/ marcato temporalmente e conservato dall'Amministrazione stessa, salvo inviarlo al CERT-PA in caso di incidenti;

VISTO inoltre il Regolamento generale sulla protezione dei dati (GDPR, General Data Protection Regulation - Regolamento UE 2016/679) - pienamente applicato entro il 25 maggio 2018 - con il quale la Commissione europea intende rafforzare e unificare la protezione dei dati personali entro i confini dell'Unione europea aumentando il livello di responsabilizzazione introducendo il concetto di misure idonee alle organizzazioni che sono chiamate ad attuare quanto necessario per la sicurezza a fronte di pesanti sanzioni;

DATO ATTO che l'aspetto primario per un adeguato piano di sicurezza è quello organizzativo, questa giunta intende definire con le presenti linee guida gli aspetti fondamentali in relazione alle responsabilità, individuazione dei dati da difendere, formazione agli utenti, principali misure tecniche;

VISTO l'allegato modulo di implementazione di cui all'allegato 2 della CIRCOLARE 18 aprile 2017 , n. 2/2017 emanata dalla Agenzia per l'Italia Digitale, debitamente compilato nei controlli del primo gruppo (livello "Minimo") ovvero quelli strettamente obbligatori ai quali ogni Pubblica Amministrazione, indipendentemente dalla sua natura e dimensione, che deve essere conforme in termini tecnologici, organizzativi e procedurali rappresentando complessivamente il livello sotto al quale nessuna Amministrazione può scendere, denominato Modulo di implementazione delle Misure Minime di Sicurezza ICT per le pubbliche amministrazioni (MMS-PA), sottoscritto digitalmente dal competente Responsabile di Area e con marcatura temporale, parte integrante e sostanziale del presente atto (allegato A);

PROPONE CHE LA GIUNTA DELIBERI

Per le motivazioni esposte in premessa e che qui si intendono interamente richiamate:

1. di approvare il Modulo contenente le Misure Minime di Sicurezza ICT per le pubbliche amministrazioni (MMS-PA) debitamente compilato nei controlli del primo gruppo (livello "Minimo"), nel testo allegato al presente provvedimento quale parte integrante sostanziale (allegato A) firmato digitalmente con marcatura temporale, conservato e, in caso di incidente informatico, trasmesso al CERT-PA insieme con la segnalazione dell'incidente stesso;

2. di dare mandato al Responsabile dei sistemi informativi dell'Ente di attuare le misure MMS- PA individuate e di portarle a conoscenza per quanto necessario ai responsabili di Area e Settore dell'Ente.

3. Di impegnarsi ad adottare i provvedimenti di propria competenza utili alla sua attuazione;

4. di provvedere alla pubblicazione del piano sul sito web istituzionale dell'Ente, nella sezione Amministrazione Trasparente in Altri contenuti / Dati ulteriori "Transizione al digitale"

5. Di dare atto che il presente provvedimento non comporta impegni di spesa, e che alle misure attuative del Piano che richiedano spese, si provvederà con specifici provvedimenti e/o nell'ambito delle risorse che saranno appositamente assegnate attraverso il Piano Esecutivo di Gestione;

6. Di dichiarare il presente atto immediatamente eseguibile ai sensi dell'art.134, comma 4, del T. U. E. L. D. Lgs. 267 del 18.8.2000

F/to

CAPO SETTORE AMMINISTRATIVO
Dott. Luciano Magnano

Città di Sortino

MODULO "MISURE MINIME PER LA SICUREZZA ICT NELLA PUBBLICA AMMINISTRAZIONE" COME PREVISTO DALLA CIRCOLARE AGID N. 2/2017

Maggio 2022

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	L'inventario delle risorse attive è riportato in un file Excel mantenuto dall'Ufficio CED - Sistemi Informativi. Il file Excel, costituito da più fogli di lavoro, viene aggiornato in tempo reale ogni qualvolta un nuovo dispositivo viene collegato alla rete aziendale e verificato ogni 6 mesi. Contiene l'elenco di Personal Computer, Notebook, Server, Stampanti/Fotocopiatrici, Telefoni VOIP, Switch di Rete, Router, collegati in rete in modo permanente o provvisorio.
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	
1	2	1	S	Implementare il "logging" delle operazione del server DHCP.	E' attivo il logging sui server DHCP, mediante software Graylog (opensource).
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	Gli elenchi di cui alla misura 1.1.1 vengono aggiornati a cura dell'Amministratore di Sistema o suoi delegati. L'aggiornamento avviene in tempo reale ogni qual volta un nuovo dispositivo viene collegato alla rete aziendale.
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	
1	4	1	M	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	Misura adottata con l'implementazione di cui al punto 1.1.1.
1	4	2	S	Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine, la funzione del sistema, un titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o	Misura adottata con l'implementazione di cui al punto 1.1.1.

				personale.	
1	4	3	A	Dispositivi come telefoni cellulari, tablet, laptop e altri dispositivi elettronici portatili che memorizzano o elaborano dati devono essere identificati, a prescindere che siano collegati o meno alla rete dell'organizzazione.	
1	5	1	A	Installare un'autenticazione a livello di rete via 802.1x per limitare e controllare quali dispositivi possono essere connessi alla rete. L'802.1x deve essere correlato ai dati dell'inventario per distinguere i sistemi autorizzati da quelli non autorizzati.	
1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	

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.	L'inventario dei software autorizzati è riportato in un file Excel curato ed aggiornato dall'Amministratore di Sistema o suoi delegati. La necessità di ulteriori software non presenti in elenco viene evidenziata all'Amministratore di Sistema o proprio delegato, che ne verificano la reale esigenza ed eventualmente provvedono affinché sia installato, con conseguente aggiornamento dell'elenco. Le abilitazioni all'installazione del software sono state concesse solamente all'Amministratore di Sistema o suoi delegati (si veda la misura 5.1.1).
2	2	1	S	Implementare una "whitelist" delle applicazioni autorizzate, bloccando l'esecuzione del software non incluso nella lista. La "whitelist" può essere molto ampia per includere i software più diffusi.	
2	2	2	S	Per sistemi con funzioni specifiche (che richiedono solo un piccolo numero di programmi per funzionare), la "whitelist" può essere più mirata. Quando si proteggono i sistemi con software personalizzati che può essere difficile inserire nella "whitelist", ricorrere al punto ABSC 2.4.1 (isolando il software	

				personalizzato in un sistema operativo virtuale).	
2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	E' data facoltà di effettuare installazioni sui dispositivi attestati sull'infrastruttura di rete solo all'Amministratore di Sistema o suoi delegati, pertanto è esclusa la possibilità di rilevare sui sistemi la presenza di software non autorizzato.
2	3	2	S	Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop.	Misura adottata con l'implementazione di cui al punto 2.1.1.
2	3	3	A	Installare strumenti automatici d'inventario del software che registrino anche la versione del sistema operativo utilizzato nonché le applicazioni installate, le varie versioni ed il livello di patch.	
2	4	1	A	Utilizzare macchine virtuali e/o sistemi air-gapped per isolare ed eseguire applicazioni necessarie per operazioni strategiche o critiche dell'Ente, che a causa dell'elevato rischio non devono essere installate in ambienti direttamente collegati in rete.	

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.	La procedura di installazione dei sistemi operativi in uso, prevede l'utilizzo di una specifica immagine standard distribuita tramite WDS (Windows Deployment System), comune a tutte le postazioni di lavoro. Le immagini - conservate come descritto alle misure 3.3.1 e 3.3.2 - sono costantemente aggiornate con le ultime versioni di Sistema Operativo, dei software e dei driver relativi alle periferiche installate.
3	1	2	S	Le configurazioni sicure standard devono corrispondere alle versioni "hardened" del sistema operativo e delle applicazioni installate. La procedura di hardening comprende tipicamente: eliminazione degli account non necessari (compresi gli account	

				di servizio), disattivazione o eliminazione dei servizi non necessari, configurazione di stack e heaps non eseguibili, applicazione di patch, chiusura di porte di rete aperte e non utilizzate.	
3	1	3	A	Assicurare con regolarità la validazione e l'aggiornamento delle immagini d'installazione nella loro configurazione di sicurezza anche in considerazione delle più recenti vulnerabilità e vettori di attacco.	
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Misura adottata con l'implementazione di cui al punto 3.1.1.
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Misura adottata.
3	2	3	S	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	L'amministratore di sistema e i suoi delegati, mantengono copie delle immagini d'installazione su NAS di Backup, creato con cadenza giornaliera. Le immagini vengono conservate per 3 mesi.
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	Le immagini di installazione salvate su NAS di Backup sono conservate in una stanza accessibile agli amministratori di sistema.
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).	Per attività di gestione effettuate da reti esterne alla rete comunale vengono utilizzate da parte dei fornitori connessioni VPN o comunque criptate. Inoltre sono consentire l'accesso ai fornitori esterni solo tramite l'attivazione su richiesta della regole presenti sul firewall.
3	5	1	S	Utilizzare strumenti di verifica dell'integrità dei file per assicurare che i file critici del sistema (compresi eseguibili di sistema e delle applicazioni sensibili, librerie e configurazioni) non siano stati alterati.	
3	5	2	A	Nel caso in cui la verifica di cui al punto precedente venga eseguita da uno strumento automatico, per qualunque alterazione di tali file deve essere generato un alert.	
3	5	3	A	Per il supporto alle analisi, il sistema di segnalazione deve essere in grado di mostrare la cronologia dei cambiamenti della	

				configurazione nel tempo e identificare chi ha eseguito ciascuna modifica.	
3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	
3	6	1	A	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	
3	7	1	A	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	

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.	Misura parzialmente adottata. E' in fase valutazione/implementazione il software Opervas (opensource) che è in grado di effettuare scansioni su eventuali vulnerabilità presenti sui dispositivi attestati nella rete comunale.
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	Implementato il software di cui alla misura 4.1.1, sarà effettuata con cadenza semestrale una scansione su tutta la rete da parte dell'Amministratore di sistema o di un suo delegato.
4	1	3	A	Usare uno SCAP (Security Content Automation Protocol) di validazione della vulnerabilità che rilevi sia le vulnerabilità basate sul codice (come quelle descritte dalle voci Common Vulnerabilities ed Exposures) che quelle basate sulla configurazione (come elencate nel Common ConfigurationEnumeration Project).	
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	

4	3	1	S	Eseguire le scansioni di vulnerabilità in modalità privilegiata, sia localmente, sia da remoto, utilizzando un account dedicato che non deve essere usato per nessun'altra attività di amministrazione.	
4	3	2	S	Vincolare l'origine delle scansioni di vulnerabilità a specifiche macchine o indirizzi IP, assicurando che solo il personale autorizzato abbia accesso a tale interfaccia e la utilizzi propriamente.	
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	Implementato il software di cui alla misura 4.1.1, ne verrà garantito l'aggiornamento da parte dell'Amministratore di sistema o di un suo delegato.
4	4	2	S	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione	
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Quando una patch di vulnerabilità è disponibile, ne viene schedulata l'installazione dall'Amministratore di Sistema o da un suo delegato. Qualora l'applicazione automatica delle patch non abbia avuto successo o provochi gravi problemi al funzionamento dei sistemi, l'Amministratore di Sistema o un suo delegato valutano e motivano a quale livello di patching occorra fermarsi. Se l'impossibilità di aggiornare i sistemi è causata da un'incompatibilità della nuova patch con uno dei software gestionali presenti nell'Ente, si procede ad informarne il fornitore di detto software, al fine di renderne disponibili i correttivi.
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.	Sono state date disposizioni dall'Amministratori di Sistema di controllare periodicamente (almeno ogni 6 mesi) ed aggiornare manualmente i sistemi non raggiungibili via rete.
4	6	1	S	Verificare regolarmente che tutte le attività di scansione effettuate con gli account aventi privilegi di amministratore siano state eseguite secondo delle policy predefinite.	
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.	Sono state date disposizioni dall'Amministratore di Sistema di verificare la risoluzione delle vulnerabilità. Nel caso non siano state trovate o applicate le patch necessarie, l'Amministratore di Sistema o un suo delegato documentano il caso su apposito

					registro conservato presso l'ufficio CED – Sistemi Informativi, indicando le eventuali contromisure o la motivazione della mancata risoluzione della vulnerabilità.
4	7	2	S	Rivedere periodicamente l'accettazione dei rischi di vulnerabilità esistenti per determinare se misure più recenti o successive patch possono essere risolutive o se le condizioni sono cambiate, con la conseguente modifica del livello di rischio.	
4	8	1	M	Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità , del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).	
4	8	2	M	Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.	
4	9	1	S	Prevedere, in caso di nuove vulnerabilità, misure alternative se non sono immediatamente disponibili patch o se i tempi di distribuzione non sono compatibili con quelli fissati dall'organizzazione.	
4	10	1	S	Valutare in un opportuno ambiente di test le patch dei prodotti non standard (es.: quelli sviluppati ad hoc) prima di installarle nei sistemi in esercizio.	

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.	I privilegi di amministrazione sono attribuiti solo all'Amministratore di Sistema e ai suoi delegati espressamente nominati.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	E' attivato il log di sistema per registrare gli accessi con credenziali di amministrazione su PC, server e firewall di rete.
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi	

				necessari per svolgere le attività previste per essa.	
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	L'amministratore di Sistema è nominato con apposito decreto sindacale. Allo stesso modo, i delegati nominati dall'Amministratore di Sistema ricevono specifica nomina agli atti del protocollo generale dell'ente. I fornitori software vengono indicati come amministratori dei loro software/macchine.
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	
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.	L'Amministratore di Sistema ha fornito ai suoi delegati adeguate istruzioni in tal senso.
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	
5	6	1	A	Utilizzare sistemi di autenticazione a più fattori per tutti gli accessi amministrativi, inclusi gli accessi di amministrazione di dominio. L'autenticazione a più fattori può utilizzare diverse tecnologie, quali smart card, certificati digitali, one time password (OTP), token, biometria ed altri analoghi sistemi.	
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).	L'Amministratore di Sistema e i suoi delegati utilizzano password "forti", composte da almeno 12 caratteri fra alfanumerici, maiuscole e caratteri speciali.
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Il sistema di autenticazione è configurato per obbligare tutti gli utenti al cambio password ogni 6 mesi.

5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Il sistema di autenticazione è configurato per impedire il riutilizzo delle ultime 6 password per tutti gli utenti.
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	
5	8	1	S	Non consentire l'accesso diretto ai sistemi con le utenze amministrative, obbligando gli amministratori ad accedere con un'utenza normale e successivamente eseguire come utente privilegiato i singoli comandi.	
5	9	1	S	Per le operazioni che richiedono privilegi gli amministratori debbono utilizzare macchine dedicate, collocate su una rete logicamente dedicata, isolata rispetto a Internet. Tali macchine non possono essere utilizzate per altre attività.	
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Misura adottata con l'implementazione di cui al punto 5.1.2.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Dall'Amministratore di Sistema sono state fornite ai delegati adeguate istruzioni al riguardo.
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.	Dall'Amministratore di Sistema sono state fornite ai delegati adeguate istruzioni al riguardo. In ogni caso l'utenza "administrator" di Windows, è utilizzata solo ed esclusivamente per svolgere circostanziate operazioni di amministrazione sul Domain Controller, che non possono essere eseguite con altra utenza.
5	10	4	S	Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).	
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Tutte le credenziali amministrative sono note solo all'Amministratore di Sistema e ai suoi delegati, che hanno necessità di utilizzarle.
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Non si utilizzano certificati digitali per l'autenticazione delle utenze amministrative.

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.	Su tutti i PC, portatili e server è installato un antivirus con aggiornamento automatico (Kaspersky).
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	E' installato un firewall di rete (Endian) a protezione di tutti i dispositivi attestati sulla LAN aziendale.
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	
8	2	1	S	Tutti gli strumenti di cui in ABSC_8.1 sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione.	
8	2	2	S	È possibile forzare manualmente dalla console centrale l'aggiornamento dei sistemi anti-malware installati su ciascun dispositivo. La corretta esecuzione dell'aggiornamento è automaticamente verificata e riportata alla console centrale.	
8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Istruzioni in merito sono già contenute nel vigente DPS, quali ad esempio ridurre al minimo l'utilizzo di HDD esterni, chiavette USB, ecc... Verranno inoltre impartite a tutti i dipendenti disposizioni volte a limitare l'uso di PC e altri dispositivi non censiti nell'elenco di cui alla misura 1.1.1.
8	3	2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	
8	4	1	S	Abilitare le funzioni atte a contrastare lo sfruttamento delle vulnerabilità, quali Data ExecutionPrevention (DEP), Address Space Layout Randomization (ASLR), virtualizzazione, confinamento, etc. disponibili nel software di base.	
8	4	2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	
8	5	1	S	Usare strumenti di filtraggio che operano sull'intero flusso del	

				traffico di rete per impedire che il codice malevolo raggiunga gli host.	
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	E' stata data disposizione dall'Amministratore di Sistema ai suoi delegati di configurare in tal senso le postazioni di lavoro.
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	E' stata data disposizione dall'Amministratore di Sistema ai suoi delegati di configurare in tal senso le postazioni di lavoro.
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	E' stata data disposizione dall'Amministratore di Sistema ai suoi delegati di configurare in tal senso le postazioni di lavoro.
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	E' stata data disposizione dall'Amministratore di Sistema ai suoi delegati di configurare in tal senso le postazioni di lavoro.
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	E' stata data disposizione dall'Amministratore di Sistema ai suoi delegati di configurare in tal senso le postazioni di lavoro.
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.	
8	9	2	M	Filtrare il contenuto del traffico web.	Sul firewall di rete (Endian) è attiva la funzione di URL Filtering.
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).	
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	
8	11	1	S	Implementare una procedura di risposta agli incidenti che preveda la trasmissione al provider di sicurezza dei campioni di software sospetto per la generazione di firme personalizzate.	

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	Le politiche di backup applicate prevedono un backup full giornaliero, contenente anche le informazioni necessarie al

				completo ripristino del sistema.	completo ripristino del sistema.
10	1	2	A	Per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono riguardare il sistema operativo, le applicazioni software e la parte dati.	Misura adottata.
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	Misura adottata.
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	Misura adottata.
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.	Le copie di sicurezza sono conservate in stanze separate in appositi armadi, il cui accesso è consentito solo all'Amministratore di Sistema e suoi delegati.
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.	Misura adottata con l'implementazione di cui al punto 10.3.1.

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	Attualmente, particolari livelli di riservatezza sono garantiti attraverso la compartimentazione dei dati in cartelle il cui accesso è regolato da specifici criteri (ACL - Access Control List). Sarà compito del DPO/RDP valutare la necessità di garantire ulteriori livelli di riservatezza anche attraverso l'implementazione della protezione crittografica.
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	
13	3	1	A	Utilizzare sul perimetro della rete strumenti automatici per bloccare, limitare ovvero monitorare in maniera puntuale, sul traffico uscente dalla propria rete, l'impiego di crittografia non autorizzata o l'accesso a siti che consentano lo scambio e la potenziale esfiltrazione di informazioni.	

13	4	1	A	Effettuare periodiche scansioni, attraverso sistemi automatizzati, in grado di rilevare sui server la presenza di specifici "data pattern", significativi per l'Amministrazione, al fine di evidenziare l'esistenza di dati rilevanti in chiaro.	
13	5	1	A	Nel caso in cui non sia strettamente necessario l'utilizzo di dispositivi esterni, implementare sistemi/configurazioni che impediscano la scrittura di dati su tali supporti.	
13	5	2	A	Utilizzare strumenti software centralizzati atti a gestire il collegamento alle workstation/server dei soli dispositivi esterni autorizzati (in base a numero seriale o altre proprietà univoche) cifrando i relativi dati. Mantenere una lista aggiornata di tali dispositivi.	
13	6	1	A	Implementare strumenti DLP (Data LossPrevention) di rete per monitorare e controllare i flussi di dati all'interno della rete in maniera da evidenziare eventuali anomalie.	
13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	Misura adottata con l'implementazione di cui al punto 8.9.2.
13	9	1	A	Assicurare che la copia di un file fatta in modo autorizzato mantenga le limitazioni di accesso della sorgente, ad esempio attraverso sistemi che implementino le regole di controllo degli accessi (e.g. Access Control List) anche quando i dati sono trasferiti al di fuori del loro repository.	

PARERE EX ART. 53 DELLA LEGGE 142/90

RECEPITO DALLA L.R. 48/91 E MODIFICATO DALLA L.R. 23/12/200 N.30

OGGETTO: PIANO TRIENNALE PER L'INFORMATICA DEL COMUNE DI SORTINO TRIENNIO 2021-2023 - APPROVAZIONE

Per la **Regolarità TECNICA** si esprime parere FAVOREVOLE

Sortino, 18/05/2022

F.to

Il Responsabile Area Amministrativa
(Dott. Luciano Magnano)

Comportando la presente:

□ prenotazione impegno n._____;

□ diminuzione di entrata;

☒ non comporta riflessi diretti o indiretti sulla situazione economico finanziaria o sul patrimonio dell'Ente;

□ altro _____

Per la **regolarità CONTABILE** si esprime parere FAVOREVOLE

Sortino, 18-05-2022.

Il Responsabile del Settore Contabile

F.to (Tuccio Michele)

LA GIUNTA

VISTA la superiore proposta.

Visto il vigente O.R.E.L.

Con voti unanimi espressi per alzata di mano.

D E L I B E R A

DI APPROVARE siccome approva la suesposta proposta.

IL PRESIDENTE

F.to Sig. Parlato Vincenzo

L'ASSESSORE A.

F.to Dott. V. Basiano

IL SEGRETARIO

F.to Dott. Bartolotta Antonino

Con successiva votazione unanime il presente atto viene dichiarato immediatamente eseguibile ai sensi dell'art. 134, 4° comma del D. lgs. 267/2001.

IL PRESIDENTE

F.to Sig. Parlato Vincenzo

L'ASSESSORE A.

F.to Dott. V. Basiano

IL SEGRETARIO

F.to Dott. Bartolotta Antonino

CERTIFICATO DI PUBBLICAZIONE

Su conforme attestazione del messo comunale si certifica che copia integrale della presente deliberazione è stata pubblicata all'Albo Pretorio Comunale on line dal ...19 MAG. 2022 03 GIU. 2022 ~~19 MAG. 2022~~ *al n.ro* 620 *registro delle pubblicazioni.*

Dalla Residenza Municipale,li ...19 MAG. 2022

IL MESSO COMUNALE
F.to Sig. Scamporlino M.

IL SEGRETARIO COMUNALE
F.to Dott. Antonino Bartolotta

CERTIFICATO DI ESECUTIVITA'

Il sottoscritto Segretario Comunale, visti gli atti di ufficio

ATTESTA

- *Che la presente deliberazione, è divenuta esecutiva il* ...18-5-2022...
- ☐ *Decorsi 10 giorni dalla data d'inizio della pubblicazione.*
- ☒ *Perché dichiarata immediatamente esecutiva (art.12, 2° comma L.R. n. 44/91)*

IL SEGRETARIO COMUNALE
F.to Dott. Antonino Bartolotta

Dalla Residenza Municipale,li .....

E' copia conforme all'originale

Dalla Residenza Municipale, ...

IL SEGRETARIO COMUNALE
F.to Dott. Antonino Bartolotta