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.

IL LEGALE RAPPRESENTANTE DEL COMUNE DI CAIRO MONTENOTTE
(Paolo Lambertini)
f.to digitalmente

IL RESPONSABILE UFFICIO TRANSIZIONE ALLA MODALITA' DIGITALE
(Alessandro Ghione)
f.to digitalmente