ALLEGATO C

PIANO AZIENDALE MISURE DI SICUREZZA ICT (AGID) - PRESCRIZIONI PER FORNITORI

Il presente documento descrive le misure minime di sicurezza che la ditta fornitrice del/i bene/i oggetto della proposta di donazione deve garantire.

Nello specifico, l'ASL CN1 ha definito un insieme minimo di misure di sicurezza ICT estrapolate dalle misure emanate dall'AgID con Circolare 18 aprile 2017, n. 2/2017, recante «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)», pubblicata in Gazzetta Ufficiale (Serie Generale n.103 del 5-5-2017).

Nel seguito sono elencate e descritte tali misure.

Tale documento è parte integrante del Piano Aziendale per le misure di sicurezza ICT adottate nell'ASL CN1 in conformità di quanto disposto dalla Circolare 18 aprile 2017, n. 2/2017, recante «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)», pubblicata in Gazzetta Ufficiale (Serie Generale n.103 del 5-5-2017).

Le Misure Minime AgID si identificano come processo continuo di evoluzione delle procedure di sicurezza Cibernetica all'interno della PA.

"Il documento contiene le indicazioni che le pubbliche amministrazioni sono chiamate ad adottare entro dicembre 2017 per valutare e innalzare il livello di sicurezza informatica, e ha l'obiettivo di fornire alle PA un riferimento pratico per contrastare le minacce più comuni e frequenti a cui sono soggette. Esso è parte integrante del più ampio disegno delle Regole Tecniche per la sicurezza informatica della Pubblica Amministrazione, come previsto dal Piano Triennale e dalla Direttiva 1 agosto 2015 del Presidente del Consiglio dei Ministri che assegna ad AgID il compito di sviluppare gli standard di riferimento per le amministrazioni."

La ditta fornitrice deve obbligatoriamente restituire il presente documento sottoscritto su ogni pagina e rilasciare una autocertificazione, resa ai sensi di legge, in cui si impegna ad attuare le misure ivi indicate.

Legenda

Acronimo	Descrizione
ABSC	Agid Basic Security Control(s)
AD	Active Directory
AZIENDA	ASLCN1
CCSC	Center for Critical Security Control
CSC	Critical Security Control
DBA	Data Base Administrator
FNSC	Framework Nazionale di Sicurezza Cibernetica
GPO	Group Policy
NSC	Nucleo di Sicurezza Cibernetica
RDBMS	Relational Database Management System

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

ABSC_ID			Livello	Descrizione	Disposizioni di sicurezza dell'AZIENDA
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.	E' richiesto che il fornitore non effettui installazioni di software sui sistemi oggetto della proposta di donazione, se non previa autorizzazione dell'AZIENDA.
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	E' richiesto che il fornitore configuri i propri sistemi per consentire l'esecuzione di scansioni effettuate da parte dell'AZIENDA, anche attraverso l'eventuale installazione di appositi agent.

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

ABSC_ID			Livello	Descrizione	Disposizioni di sicurezza dell'AZIENDA
3	1	1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	E' richiesto che il fornitore, qualora provveda in autonomia ad installare il sistema operativo, proceda seguendo le indicazioni che verranno fornite dall'AZIENDA successivamente all'accettazione della proposta di donazione. E' richiesto obbligatoriamente che il fornitore produca all'AZIENDA, prima della messa in esercizio del sistema, un documento in cui sono descritte le configurazioni software e hardware per ciascun server e sistema, seguendo il modello che verrà fornito dall' AZIENDA successivamente all'accettazione della proposta di donazione. Tale documentazione dovrà essere mantenuta aggiornata da parte del fornitore ad ogni modifica significativa della configurazione.
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	E' richiesto che il fornitore, qualora provveda in autonomia ad installare le postazioni di lavoro, i server e altri sistemi, proceda seguendo le indicazioni che verranno fornite dall'AZIENDA successivamente all'accettazione della proposta di donazione.
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	E' richiesto che il fornitore effettui il ripristino di eventuali sistemi compromessi utilizzando la configurazione standard.
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	E' richiesto che il fornitore memorizzi le proprie immagini di installazione offline.
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).	E' richiesto che il fornitore implementi soltanto connessioni protette per le operazioni di amministrazione remota di server, workstation e altre apparecchiature.

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

ABSC_ID			Livello	Descrizione	Disposizioni di sicurezza dell'AZIENDA
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.	E' richiesto che il fornitore configuri i propri sistemi per consentire l'esecuzione di scansioni regolari per la ricerca delle vulnerabilità effettuate da parte dell'AZIENDA, anche attraverso l'eventuale installazione di agent. E' richiesto che il fornitore informi l'AZIENDA, al fine di effettuare una rivalutazione del rischio, ogni volta che apporti modifiche significative alle configurazioni dei propri sistemi, avendo cura di verificare **in proprio** la presenza di eventuali vulnerabilità note e proponendo possibili contromisure tecniche.
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	E' richiesto che il fornitore configuri i propri sistemi per consentire l'installazione automatica delle patch e aggiornamenti di sicurezza dei sistemi operativi (almeno quelle di livello critical e security): • per i sistemi Windows è richiesto che venga utilizzato il sistema aziendale di distribuzione delle patch (WSUS); • per i sistemi Linux/Unix è richiesto che vengano utilizzati gli strumenti nativi del sistema operativo per l'aggiornamento; E' richiesto che il fornitore aggiorni periodicamente le proprie applicazioni, e tutte le componenti software presenti (ad esempio: application server, middleware, RDBMS, …) installando le patch e gli aggiornamenti di sicurezza. Qualora non sia possibile procedere con un aggiornamento automatico dei sistemi operativi, verrà richiesto al fornitore di descrivere dettagliatamente le motivazioni di tale impedimento (tecnici e/o legati a certificazioni delle apparecchiature), proponendo e adottando, **a carico del fornitore**, soluzioni tecniche alternative da concordare comunque preventivamente con l'AZIENDA. E' richiesto che le eventuali attività di fermo dei sistemi per l'applicazione degli aggiornamenti di sicurezza siano concordate con l'AZIENDA. **Il fornitore deve prevedere che le relative attività di aggiornamento (almeno 2 all'anno) possano essere effettuate dopo le ore 20 o prima delle ore 7**.
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.	Qualora i sistemi oggetto della proposta di donazione siano di tipo air-gapped. il fornitore deve provvedere al loro aggiornamento periodico, fornendone evidenza all'AZIENDA attraverso la redazione di un apposito registro.

ABSC_ID			Livello	Descrizione	Disposizioni di sicurezza dell'AZIENDA
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.	Qualora non sia possibile procedere con un aggiornamento automatico dei sistemi, è richiesto che il fornitore descriva dettagliatamente le motivazioni di tale impedimento, proponendo e adottando, **a carico del fornitore**, soluzioni tecniche alternative da concordare comunque preventivamente con l'AZIENDA.
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.	E' richiesto che il fornitore applichi le patch di sicurezza a partire da quelle più critiche. Sulla base della pubblicazione di dati sulle vulnerabilità fornite dai vari CERT, l'applicazione delle patch critiche deve essere effettuata entro 72 ore lavorative dalla loro disponibilità.
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.	E' richiesto che il fornitore proponga misure alternative in caso di nuove vulnerabilità qualora non siano immediatamente disponibili patch o se i tempi di distribuzione non siano compatibili con quelli fissati dall'AZIENDA, in relazione al livello di rischio valutato dall'AZIENDA.

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

ABSC_ID			Livello	Descrizione	Disposizioni di sicurezza dell'AZIENDA
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.	E' richiesto obbligatoriamente che il fornitore comunichi i nominativi dei tecnici a cui sono affidati compiti di amministrazione secondo privilegi delegati dall'AZIENDA, ai quali verranno assegnate credenziali nominative di amministrazione. Nel caso le credenziali vengano emesse e gestite dal fornitore, è richiesto obbligatoriamente che le stesse vengano comunicate all'AZIENDA (cfr.misura 5.2.1) e che siano assegnate in forma nominativa e non generica.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	E' richiesto che le utenze amministrative vengano usate solo per operazioni che ne richiedano i privilegi. E' richiesto che tutti i sistemi ed apparecchiature forniti dal fornitore siano configurati, **con attività ed eventuali costi a carico del fornitore,** per essere oggetto di monitoraggio dei log degli amministratori di sistema attraverso il software in uso presso l'AZIENDA. In fase di installazione verrà concordata la tecnologia da usare per la trasmissione dei log al sistema centrale.
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	Nel caso le credenziali vengano emesse e gestite dal fornitore, è richiesto che ciascuna utenza amministrativa abbia solo i privilegi necessari per svolgere le attività previste.
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	Nel caso le credenziali vengano emesse e gestite dal fornitore, è richiesto che il fornitore mantenga un inventario delle stesse e che ciascuna sia formalmente autorizzata dall'AZIENDA.
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.	E' richiesto che ogni nuovo dispositivo che viene collegato in rete in attuazione del presente capitolato venga configurato in modo da sostituire le credenziali dell'amministratore predefinito dandone riscontro scritto al Sistema Informativo Direzionale dell'AZIENDA; inoltre devono essere attivate le credenziali amministrative nominative, come indicato al punto 5.1.1

ABSC_ID			Livello	Descrizione	Disposizioni di sicurezza dell'AZIENDA
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).	Qualora non venga usata l'autenticazione a più fattori, è richiesto che le credenziali amministrative soddisfino i seguenti requisiti: • Regola di lunghezza: la password deve essere composta **almeno da 14 caratteri**; • Regola di complessità: la password deve essere composta con criteri di complessità, cioè deve contenere almeno 3 delle seguenti quattro categorie di caratteri: minuscoli, maiuscoli, numeri, simboli; inoltre non deve contenere riferimenti espliciti al nome e cognome dell'utente o altre riconducibili alla sua identità; • Regola di scadenza: il sistema richiede il **cambio della password ogni due mesi**; • Regola di unicità: durante il cambio della password, il sistema rifiuta l'inserimento delle ultime quattro password inserite; • Regola di blocco: il sistema blocca Indefinitamente l'account dopo cinque tentativi falliti consecutivi di login La parola chiave deve essere mantenuta segreta dall'incaricato, quindi non può essere rivelata ad altri né memorizzata su supporti cartacei o con altre modalità facilmente accessibili.
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Si veda quanto riportato al punto 5.7.1
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Si veda quanto riportato al punto 5.7.1
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	E' richiesto che venga effettuata una completa distinzione tra utenze privilegiate e non privilegiate dei tecnici individuati come amministratori di sistema, ai quali devono corrispondere credenziali diverse. In particolare, devono essere assegnate credenziali distinte per l'accesso alle applicazioni end-user da quelle per l'accesso amministrativo ai sistemi (RDBMS, apparati e apparecchiature, ecc.). Qualora il fornitore abbia anche compiti di DBA, questo livello di autenticazione dovrà essere recepito anche dall'ambiente Database.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Si veda quanto riportato al punto 5.1.1 Per quanto attiene alla definizione delle utenze autorizzate per il fornitore queste potranno essere definite sul sistema di autenticazione AD dell'AZIENDA.

ABSC_ID			Livello	Descrizione	Disposizioni di sicurezza dell'AZIENDA
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.	E' richiesto che le utenze amministrative anonime preimpostate sui sistemi (come ad esempio "root" di Unix oppure "Administrator" di Windows) non vengano mai utilizzate. Nel caso ciò non sia possibile, è richiesto alla ditta di dettagliare i motivi e per quali operazioni ciò non sia possibile. In tal caso, è richiesto al fornitore che mantenga un registro in cui annotare il nominativo del tecnico che ha fatto uso delle credenziali amministrative anonime. Tale registro dovrà essere messo a disposizione dell'AZIENDA in qualunque momento e in qualunque condizione. Nel caso di cessazione il registro dovrà essere conservato per ulteriori 6 mesi senza oneri per l'AZIENDA.
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	La parola chiave deve essere mantenuta segreta dall'incaricato, quindi non può essere rivelata ad altri né memorizzata su supporti cartacei o con altre modalità facilmente accessibili.
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	E' richiesto che, qualora per l'autenticazione si utilizzino certificati digitali, le chiavi private siano adeguatamente protette. Al fornitore aggiudicatario verrà richiesto di descrivere le misure di sicurezza che adotta per garantire tale misura, concordandole con l'AZIENDA.

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

ABSC_ID			Livello	Descrizione	Disposizioni di sicurezza dell'AZIENDA
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' richiesto che il fornitore dichiari esplicitamente il consenso all'installazione del sistema antivirus in uso presso l'AZIENDA, che si farà carico di effettuarla su tutti i sistemi connessi alla rete locale oggetto del presente capitolato. **Il fornitore può indicare eventuali aree del sistema (cartelle o applicativi in esecuzione) che devono essere escluse dalla scansione** motivando la richiesta. Qualora non sia possibile procedere con l'installazione del sistema antivirus aziendale al fornitore verrà richiesto di descrivere dettagliatamente le motivazioni di tale impedimento (tecnici e/o legati a certificazioni delle apparecchiature), proponendo e adottando, **a carico del fornitore**, soluzioni tecniche alternative da concordare comunque preventivamente con l'AZIENDA.
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Valgono le considerazioni fatte al punto 8.1.1 in quanto il sistema antivirus aziendale implementa anche funzioni di firewall e IPS.
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	E' richiesto che il fornitore non utilizzi altri dispositivi oltre a quelli necessari per le attività richieste dal presente capitolato.
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	E' richiesto che il fornitore disattivi, dispositivi forniti, l'esecuzione automatica dei contenuti al momento della connessione di dispositivi removibili

ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID			Livello	Descrizione	Disposizioni di sicurezza dell'AZIENDA
10	1	1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	E' richiesto obbligatoriamente che il fornitore in autonomia provveda a configurare sui propri sistemi una copia di sicurezza almeno settimanale delle informazioni necessarie per il completo ripristino del sistema, compresi gli strumenti e i dispositivi necessari **a carico del fornitore**. E' richiesto obbligatoriamente che, prima della messa in esercizio del sistema oggetto della proposta di donazione, il fornitore concordi con l'AZIENDA le politiche di backup da adottare (quali dati, con quale frequenza, quale tempo di retention, dove vengono salvate le copie di sicurezza), producendo un documento che ne descriva le modalità di implementazione secondo un modello che verrà consegnato in sede di accettazione della donazione. Potrà essere richiesto dall'AZIENDA l'invio di notifiche sullo stato dell'arte di esecuzione dei salvataggi secondo i normali e consolidati standard (a titolo esemplificativo: mail, SNMP, ecc.)
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	E' richiesto obbligatoriamente che il fornitore produca all'AZIENDA un verbale di avvenuto ripristino dei dati a partire dalle copie di sicurezza quando tale attività viene effettuata, al bisogno, per popolare l'ambiente di test a partire dalle copie di sicurezza dell'ambiente di produzione. In ogni caso è da prevedere un test di ripristino almeno semestrale in accordo con l'AZIENDA.
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.	L'AZIENDA si riserva la facoltà di richiedere che le copie di sicurezza siano cifrate. La scelta della destinazione del backup è insindacabilmente effettuata dall'AZIENDA.
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.	Nella definizione delle politiche di backup di cui al punto 10.1.1, da concordare preventivamente tra fornitore e l'AZIENDA, dovrà essere stabilita una modalità che consenta di rendere le copie di sicurezza non permanentemente accessibili dal sistema (almeno una).