ALLEGATO A - ELENCO DEI CONTROLLI BASE

OC.1	Le organizzazioni che utilizzano i baseline control dovrebbero avere meno di 499 dipendenti
OC.2	Le organizzazioni dovrebbero tenere un inventario degli elementi del loro sistema informatico, in particolare di quelli che rientrano nel campo di applicazione deli baseline controls e dovrebbero motivare l'eventuale esclusione di parti dei sistemi valutando il rischio di tale esclusione.
OC.3	Le organizzazioni dovrebbero valutare i danni potenziali derivanti da una perdita di riservatezza (confidenzialità), integrità e/o disponibilità dei sistemi informativi e degli asset (strumenti).
OC.4	Le organizzazioni dovrebbero auto-valutare il livello di rischio informatico più rilevante
OC.5.1	Le aziende dovrebbero identificare una figura apicale cui affidare la responsabilità della sicurezza IT
OC.5.2	Le aziende dovrebbero definire il loro livello di spesa per tecnologie informatiche e sicurezza informatica (in valore assoluto e in percentuale rispetto al totale delle spese)
OC.5.3	Le aziende dovrebbero identificare il personale interno in forza al settore IT e sicurezza IT (come numero di persone e in percentuale rispetto al totale dello staff)
OC.5.4	Le aziende dovrebbero avere definito un impegno costante nel miglioramento del livello di sicurezza IT (almeno la periodica revisione del presente elenco di controlli)
BC.1.1	Le organizzazioni dovrebbero definire un piano di risposta agli incidenti di diversa gravità. Se un'organizzazione non è in grado di gestire alcune tipologie di incidenti autonomamente, dovrebbe avere un piano che preveda le azioni da intraprendere per il ricorso a supporti esterni.
BC.1.2	Le organizzazioni dovrebbero definire un piano scritto per rispondere agli incidenti (incident response plan) che indichi anche chi è responsabile per la gestione dell'evento e includa le informazioni di contatto per le comunicazioni all'esterno (parti interessate, autorità). Le organizzazioni dovrebbero mantenere una copia cartacea aggiornata del piano e renderla disponibile nel caso in cui le versioni "soft" (digitali) del piano non siano disponibili
BC.1.3	Le organizzazioni dovrebbero considerare l'acquisto di una polizza assicurativa che comprenda la copertura per la risposta agli incidenti e per le attività di recovery oppure dovrebbero fornire le motivazioni per cui non hanno proceduto all'acquisto di una simile copertura.
BC.2.1	Le organizzazioni dovrebbero abilitare l'aggiornamento automatico per tutti i software, sistemi operativi e firmware OPPURE dovrebbero mettere in atto una soluzione di gestione completa di analisi vulnerabilità e relative "patch"
BC.2.2	Le organizzazioni dovrebbero effettuare una valutazione dei rischi in merito all'eventuale sostituzione di hardware e software non in grado di effettuare gli aggiornamenti automatici. Se tali hardware e software vengono mantenuti tra gli asset utilizzati, dovrà essere definito un processo per garantire degli aggiornamenti regolari effettuati manualmente. In caso si software e sistemi non più aggiornabili in quanto non supportati, valutare i rischi associati al mantenimento di tali sistemi e la loro eventuale sostituzione.
BC.3.1	Le organizzazioni dovrebbero attivare soluzioni anti malware in grado di aggiornarsi e di effettuare scansioni del sistema automaticamente a intervalli regolari
BC.3.2	Le organizzazioni dovrebbero attivare i firewall software presenti nei dispositivi interni alla rete OPPURE documentare le misure alternative poste in essere al posto di tali firewall
BC.4.1	Le organizzazioni dovrebbero implementare delle configurazioni sicure per tutti i

ALLEGATO A - ELENCO DEI CONTROLLI BASE

	dispositivi, modificando le password di default, disabilitando configurazioni non sicure e abilitando le funzioni di sicurezza rilevanti. Valutare dove possibile il salvataggio di configurazioni "standard" sicure per gruppi omogenei di dispositivi.
BC.5.1	Le organizzazioni, dove possibile, dovrebbero implementare un'autenticazione a due fattori e, qualora decidessero di non attivare tale sistema, dovrebbero motivare la decisione. Le organizzazioni dovrebbero implementare l'autenticazione a due fattori per gli account critici, quali quelli finanziari (o collegabili a movimentazioni finanziarie, amministratori di sistema, amministratori di servizi cloud, utenti "privilegiati" e dirigenti / manager.
BC.52	Le organizzazioni dovrebbero forzare il cambio password solo nel caso in cui vi siano sospetti o evidenze di compromissione.
BC.5.3	Le organizzazioni dovrebbero avere policy chiare in materia di lunghezza delle password e del loro riutilizzo, sull'uso di password manager e sul "se", "quando" e "come" gli utenti possano fisicamente scrivere le password su supporti cartacei o digitali e archiviarle.
BC.6.1	Le organizzazioni dovrebbero pianificare attività regolari di sensibilizzazione e formazione in materia di cyber security per i loro dipendenti
BC.7.1	Le organizzazioni dovrebbereo effettuare il backup dei sistemi che contengono informazioni essenziali e garantire che i meccanismi di recovery basati sui dati di backup siano efficaci e funzionanti. Le organizzazioni dovrebbero valutare l'archiviazione dei dati di backup offline e/o in un sito sicuro al di fuori delle sedi aziendali OPPURE motivare la decisione di non adottare tali misure di sicurezza.
BC.7.2	Le organizzazioni dovrebbero archiviare i backup in modalità cifrata e restringere l'accesso a tali dati unicamente al personale che deve effettuare i test di funzionamento dei backup e delle operazioni di ripristino e al personale coinvolto nei processi di ripristino vero e proprio. I backup di lungo periodo (es. i backup effettuati con frequenza settimanale o più) devono essere archiviati offline, mentre i backup frequenti (es. quotidiani) possono essere archiviati online.
BC.8.1	Le organizzazioni dovrebbero definire nella policy anche di chi deve essere la proprietà dei dispositivi mobili utilizzati per l'accesso ai dati e alle informazioni aziendalie e dovrebbero dovumentare la scelta e i rischi associati.
BC.8.2	Le organizzazioni dovrebbero imporre una separazione tra i dati personali e quelli aziendali nei dispositivi mobili che hanno accesso alle risorse IT aziendali, documentando i dettagli di tale separazione.
BC.8.3	Le organizzazioni dovrebbero essere in grado di garantire che i dipendenti scarichino e installino sui dispositivi mobili esclusivamente le app presenti in una lista di applicazioni autorizzate e affidabili.
BC.8.4	Le organizzazioni dovrebbero adottare le misure necessarie per fare sì che i dispositivi mobili memorizzino tutte le informazioni sensibili in modalità sicura e cifrata.
BC.8.5	Le organizzazioni dovrebbero valutare l'implementazione di un sistema di enterprise mobility management (EMM) per tutti i dispositivi mobili OPPURE dovrebbero documentare la valutazione dei rischi e i rischi assunti (es. dalle funzioni di audit, gestione rischio e sicurezza IT) nel decidere di non implementare una tale soluzione.
BC.8.6	Le organizzazioni dovrebbero imporre o fornire istruzioni agli utenti sulle seguenti configurazioni dei dispositivi mobili: 1. disabilitazione delle connessioni automatiche alle reti aperte 2. evitare collegamento a reti Wi-Fi sconosciute 3. limitare l'utilizzo dei protocolli Bluetooth e NFC per la condivisione di informazioni sensibili 4. utilizzare reti Wi-Fi aziendali oppure reti cellulari piuttosto che reti Wi-FI pubbliche

ALLEGATO A - ELENCO DEI CONTROLLI BASE

BC.8.7	Le organizzazioni dovrebbero valutare l'utilizzo di VPN nelle occasioni in cui è richiesta la connessione a reti Wi-Fi pubbliche o sconosciute OPPURE dovrebbero documentare la scelta di non utilizzare VPN.
BC.9.1	Le organizzazioni dovrebbero attivare sistemi firewall dedicati alla difesa perimetrale dei confini delle reti aziendali con la rete Internet. Le organizzazioni dovrebbero isolare i server connessi ad Internet dal resto della rete aziendale.
BC.9.2	Le organizzazioni dovrebbero implementare un firewall DNS per verificare filtrare il traffico in uscita verso la rete Internet.
BC.9.3	Le organizzazioni dovrebbero attivare la richiesta di connessione sicura verso tutte le risorse IT aziendali, attivando VPN con autenticazione a due fattori per tutti gli accessi da remoto alle risorse aziendali.
BC.9.4	Le organizzazioni dovrebbero utilizzare solo Wi-Fi con connessioni sicure, preferibilmente con protezione WPA2-Enterprise.
BC.9.5	Le organizzazioni dovrebbero isolare i sistemi di pagamento da Internet e dalle altre aree delle reti aziendali con un firewall.
BC.9.6	Le organizzazioni dovrebbero valutare l'adozione degli standard di sicurezza dell'industria dei pagamenti PCI DSS (Payment Card Industry Data Security Standard)
BC.9.7	Le organizzazioni dovrebbero implementare il controllo DMARC nei servizi email aziendali.
BC.9.8	Le organizzazioni dovrebbero implementare filtri per le email ai punti di ingresso e di uscita.
BC.10.1	Le organizzazioni dovrebbero chiedere a tutti i loro fornitori di servizi cloud un report AICPA SSAE 18 SOC 3 che attesti la conformità ai Trust Service Principles.
BC.10.2	Le organizzazioni dovrebbero valutare il livello di conformità in relazione a "come" i loro fornitori di servizi IT hanno accesso e gestiscono le informazioni sensibili aziendali.
BC.10.3	Le organizzazioni dovrebbero valutare i requisiti normativi richiesti nelle aree giurisdizionali di competenza ai fornitori di servizi IT che trattano dati personali e informazioni sensibili e il livello di conformità tra le diverse normative.
BC.10.4	Le organizzazioni dovrebbero garantire che le proprie infrastrutture IT e i propri dipendenti comunichino tramite protocolli sicuri con tutti i servizi cloud e le applicazioni.
BC.10.5	Le organizzazioni dovrebbero garantire l'utilizzo di autenticazioni a due fattori per tutte le utenze di servizi cloud con privilegi di amministratore e che le credenziali di tali utenze siano diverse da quelle degli amministratori dei sistemi intetni.
BC.11.1	Le organizzazinoi dovrebbero garantire la conformità dei loro siti web a quanto previsto nelle linee guida OWASP ASVS Livello 1.
BC.11.2	Le organizzazioni dovrebbero assicurare di avere compreso il livello ASVS che intendono raggiungere per ciascuno dei propri siti web.
BC.12.1	Le organizzazioni dovrebbero configurare gli account utente con i privilegi minimi di accesso ai dati e alle funzionalità necessari per lo svolgimento delle attività e dovrebbero restringere i privilegi degli amministratori secondo le necessità del contesto.
BC.12.2	Le organizzazioni dovrebbero permettere agli account di amministratore di effettuare solo operazioni tipiche dell'amministratore di sistema impedendo di effettuare operazioni tipiche del livello utente come, ad esempio, la navigazione Internet e l'invio e ricezione di email.
BC.12.3	Le organizzazioni dovrebbero rimuovere gli account utente e/o le funzionalità a questi associate quando tali account o tali funzionalità non sono più richieste per

	l’esecuzione dei compiti dei dipendenti.
BC.12.4	Le organizzazioni dovrebbero valuare l’implementazione di un sistema di controllo utente centralizzato OPPURE motivare la scelta di non implementarlo.
BC.13.1	Le organizzazioni dovrebbero autorizzare unicamente l’utilizzo di memorie portatili di proprietà dell’organizzazione, mantenendo un forte controllo su tali memorie, proteggendone il contenuto tramite sistemi di crittografia.
BC.13.2	Le organizzazioni dovrebbero adottare processi di “sanificazione” (cancellazione sicura) o di distruzione fisica dei dispositivi di memoria portatili, compresi smartphone e tablet.