Data: 22.06.2022

Perimetro Pubbliche Amministrazioni (Misure Agid)

Ad aprile 2017 AgiD ha pubblicato nella Gazzetta Ufficiale (GuRI) le Misure Minime di Sicurezza per la PA, un documento che 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.

Le misure minime Agid sono indicate con la nomenclatura ABSC (Agid Basic Security Controll), cioè con identificatore gerarchico a tre livelli x,y.z preceduti dalla lettera M per indicare la misura come minima (**[M].x.y.z**).

Per i servizi contrattualizzati che prevedono il trattamento di questo Perimetro di Dati sono state definite le seguenti misure ulteriori misure aggiuntive a quelle previste per il perimetro dei Dati Personali Comuni.

ID MISURA	Categoria	Testo requisito
PdE-ICT.013.1 PdE-ICT.013.2	Protezione degli elaboratori	E' previsto che venga applicata una protezione crittografica sui dati rilevanti (aventi particolari requisiti di riservatezza). Per le soluzioni custom condividere contrattualmente con il cliente quali sono i dati rilevanti. **[M] 13.1.1:**
Doc-ICT.012.1	Documentazione	E' prevista l'implementazione di un inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, che registra almeno l'indirizzo IP, da aggiornare quando nuovi dispositivi approvati vengono collegati in rete. **[M] 1.1.1:** **[M] 1.3.1:** **[M]1.4.1:** **[M]1.4.1:**
PdE-ICT.014.1	Protezione degli elaboratori	E' prevista la redazione di un elenco di software autorizzati, con relative versioni, necessari per ciascun tipo di sistema, compresi server e al contempo non è consentita l'installazione di software non compreso in tale elenco. E' prevista l'esecuzione di regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato. [**M] 2.1.1:** **[M] 2.3.1:**
Bck-ICT.004.1	Back-up	Su server e per la protezione dei sistemi operativi, sono definite, impiegate e ripristinate (nel caso vengano compromessi) configurazioni standard. Le immagini d'installazione sono memorizzate offline. **[M] 3.1.1:** **[M] 3.1.1:** **[M] 3.2.1:** **[M] 3.2.2 :** **[M] 3.3.1:**
PdE-ICT.015.1	Protezione degli elaboratori	E' assicurato che gli strumenti di scansione delle vulnerabilità (anche per i sistemi separati dalla rete) siano regolarmente aggiornati adottando misure di sicurezza adeguate al livello di criticità. Inoltre è periodicamente verificato che le vulnerabilità

ID MISURA	Categoria	Testo requisito
		emerse dalle scansioni siano state risolte, documentando e accettando in caso opposto un ragionevole rischio. A ciascuna azione utile per la risoluzione delle vulnerabilità è assegnato un livello di priorità in base al rischio associato. Ad ogni modifica significativa della configurazione deve essere eseguita la ricerca delle vulnerabilità con strumenti automatici che forniscano report con indicazioni delle vulnerabilità più critiche. **[M] 4.1.1:** **[M] 4.4.1:** **[M] 4.5.2:** **[M] 4.7.1:** **[M] 4.8.2:**
PdE-ICT.016.1	Protezione degli elaboratori	Vengono scaricati automaticamente e installati le patch e gli aggiornamenti del software di sistema operativo necessari a correggere difetti e prevenire vulnerabilità della piattaforma. L'installazione avviene automaticamente qualora non preveda un'interruzione o una forte limitazione dell'operatività. In particolare sono applicate le patch per le vulnerabilità a partire da quelle più critiche. **[M] 4.5.1:** **[M] 4.7.1:** **[M] 4.8.2:**
PdE-ICT.017.1	Protezione degli elaboratori	Vengono scaricati automaticamente e installati le patch e gli aggiornamenti del software di DBMS e applicativo oggetto del SaaS, necessari a correggere difetti e prevenire vulnerabilità della piattaforma. L'installazione avviene automaticamente qualora non preveda un'interruzione o una forte limitazione dell'operatività. In particolare sono applicate le patch per le vulnerabilità a partire da quelle più critiche. **[M] 4.5.1:** **[M] 4.7.1:** **[M] 4.8.2:**
CoA-ICT.015.1	Controllo accessi	Vengono completamente distinte utenze privilegiate e non privilegiate degli amministratori (alle quali devono corrispondere credenziali diverse), mentre è consentito l'utilizzo delle utenze amministrative anonime (ad esempio “root” di UNIX o “Administrator” di Windows) solo per le situazioni di emergenza; queste vengono gestite in modo da garantire la disponibilità e la riservatezza e in modo da assicurare l’imputabilità di chi ne fa uso. **[M] 5.10.1:** **[M] 5.10.3:**
PdE-ICT.018.1	Protezione degli elaboratori	Sulle piattaforme non sono consentite l’esecuzione automatica dei contenuti, dinamici e non, e l'anteprima automatica dei contenuti dei file, anche al momento della connessione dei dispositivi removibili e l'apertura automatica dei messaggi di posta elettronica. Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali. **[M]8.3.1:** **[M] 8.7.1:** **[M] 8.7.2:**

ID MISURA	Categoria	Testo requisito
		[M] 8.7.3: **[M] 8.7.4:**
PdE-ICT.019.1	Protezione degli elaboratori	Qualsiasi supporto removibile utilizzato è automaticamente soggetto ad una scansione anti-malware, inoltre sono adottati e configurati adeguati strumenti di web filtering e nel caso di posta elettronica antispamming bloccando nella posta elettronica e nel traffico web i file potenzialmente pericolosi la cui tipologia non è strettamente necessaria per l'organizzazione. **[M] 8.8.1:** **[M] 8.9.1:** **[M] 8.9.2:** **[M] 8.9.3:**
CdC-ICT.013.1	Canali di comunicazione	Le operazioni di amministrazione remota di server, dispositivi di rete e analoghe apparecchiature sono eseguite per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri). **[M] 3.4.1:**
CdC-ICT.014.1	Canali di comunicazione	E' prevista la possibilità di bloccare il traffico da e verso url presenti in una blacklist. **[M] 13.8.1:**
Ris-ICT.013.1	Riservatezza	Risulta garantita l'applicazione delle misure di sicurezza derivanti dalle analisi del rischio (Piano di Sicurezza) relative alla piattaforma a supporto del servizio erogato. **[M] 4.8.1:**

Perimetro Scambi dati tra Pubbliche Ammistrazioni

Per i servizi contrattualizzati che prevedono il trattamento di questo Perimetro di Dati sono state definite le seguenti misure ulteriori misure aggiuntive a quelle previste per il perimetro dei Dati Personali Comuni, alle quali si aggiungono ulteriori misure in funzione della diversa tipologia di dato trattato o di specifici accordi contrattuali.

ID MISURA	Categoria	Testo requisito
AuL-ICT.001.1	Audit log	Esiste un sistema di log che riporta: - gli accessi (access log) compresi i tentativi falliti - le operazioni svolte sui dati (activity log) dagli Addetti alla gestione del Sistema Operativo e dalle utenze machine to machine (in quest'ultimo caso il sistema di destinazione dovrà tracciare anche l'informazione relativa al sistema di origine)

Misure Dati Pubbliche Amministrazioni

Data: 22.06.2022

ID MISURA	Categoria	Testo requisito
AuL-ICT.002.1	Audit log	Esiste un sistema di log che riporta: - gli accessi (access log) compresi i tentativi falliti - le operazioni svolte sui dati (activity log) dagli Addetti alla gestione applicativa e dalle utenze machine to machine (in quest'ultimo caso il sistema di destinazione dovrà tracciare anche l'informazione relativa al sistema di origine)
AuL-ICT.003.1	Audit log	Esiste un sistema di log che riporta: - gli accessi (access log) compresi i tentativi falliti - le operazioni svolte sui dati (activity log) dagli Addetti alla gestione del Database e dalle utenze machine to machine (in quest'ultimo caso il sistema di destinazione dovrà tracciare anche l'informazione relativa al sistema di origine)
AuL-ICT.004.1	Audit log	La piattaforma prevede la registrazione degli accessi e delle operazioni effettuate sui dati da parte degli End User Autorizzati, comprese le utenze machine to machine (in quest'ultimo caso il Sistema di destinazione dovrà tracciare l'informazione relativa al Sistema di origine).
AuL-ICT.005.1	Audit log	E' garantita la completezza, l'immodificabilità e la possibilità di verificare l'autenticità e la conservazione per un periodo non inferiore a 6 mesi delle registrazioni dei log relativi agli accessi ed alle operazioni svolte dagli Addetti IT e dagli End User Autorizzati tramite l'invio degli stessi a sistemi di Log Collecting centralizzati.
AuL-ICT.006.1	Audit log	I log relativi agli accessi e alle operazioni degli Addetti IT e delle utenze machine to machine dovranno almeno consentire di identificare: - le operazioni svolte sui dati e le attività di amministrazione sul sistema; - l'utenza, la data e l'ora di effettuazione delle operazioni.
AuL-ICT.007.1	Audit log	I log relativi agli accessi e alle operazioni degli End User Autorizzati e delle utenze machine to machine dovranno almeno consentire di identificare: - le operazioni svolte sui dati e le attività di amministrazione sul sistema; - l'utenza, la data e l'ora di effettuazione delle operazioni.
CdC-ICT.010.1	Canali di comunicazione	E' assicurata l'implementazione di meccanismi crittografici di robustezza adeguata (ad es. HTTPS) volti a garantire la protezione dell'autenticazione degli End User Autorizzati dal rischio di intercettazione delle credenziali.
CdC-ICT.011.1	Canali di comunicazione	Nel caso la piattaforma preveda l'utilizzo di web application esposte su rete pubblica, i server sono dotati di certificati SSL Publicly Trusted.
CoA-ICT.011.1	Controllo accessi	L'applicativo è costruito in maniera tale da prevedere l'impostazione di soglie relative al numero di utenze degli End User Autorizzati con privilegi di accesso. La valorizzazione di tali soglie è resa disponibile al Cliente PA attraverso funzionalità applicative assegnabili a profili caratterizzati da massimi privilegi (ad es. amministratore di applicativo o profili GGU).

ID MISURA	Categoria	Testo requisito
CoA-ICT.012.1	Controllo accessi	L'applicativo prevede, tramite controlli automatici, la sospensione delle credenziali di autenticazione a seguito di 10 tentativi falliti di accesso, a meno di differenti accordi con il Cliente PA. Al fine di riattivare le utenze così sospese sono previste funzionalità di riabilitazione delle utenze assegnabili a specifici profili (ad es. amministratore di applicativo o GGU).
CoA-ICT.013.1	Controllo accessi	L'applicativo prevede meccanismi di limitazione degli accessi degli End User Autorizzati per intervalli temporali o di data predeterminati. La valorizzazione di tale soglia è resa disponibile al Cliente PA attraverso funzionalità applicative assegnabili a specifici profili.
Doc-ICT.011.1	Documentazione	In presenza di personale TIM (interno od esterno) autorizzato al trattamento nonchè all'accesso ai dati personali trattati dalla piattaforma, il Gestore garantisce l'esistenza di procedure di comunicazione verso la PA Cliente dell'elenco aggiornato di tali nominativi.
Ris-ICT.020.1	Riservatezza	Sono adottate misure tecniche volte ad impedire funzionalità di estrazione massiva dei dati dalle banche dati da parte degli End User Autorizzati, al fine di proibire la creazione di autonome banche dati.
Ris-ICT.021.1	Riservatezza	Sono adottate misure volte a permettere la valorizzazione di un campo con il numero di riferimento della pratica (ad es. numero del protocollo o del verbale) ogni volta che vengono effettuate consultazioni da parte degli End User Autorizzati.

Di seguito i requisiti aggiuntivi da valutare col cliente per adeguarsi alla normativa:

ID MISURA	Categoria	Testo requisito
	Controllo accessi	L'applicativo è costruito in maniera tale da prevedere la possibilità di implementare: - forme di strong-authentication che prevedano l'uso di one-time password o di certificati di autenticazione (CNS o analoghi) da parte dell'end-user incaricato; - funzionalità di interruzione di sessione di lavoro inattiva degli end-user Autorizzati a seguito di un limite temporale definito dalla PA in sede contrattuale; - meccanismi volti ad escludere la possibilità per gli end-user Autorizzati di effettuare accessi contemporanei con le medesime credenziali da postazioni diverse, in caso di procedure di accesso via web.
	Log	L'applicativo è costruito in maniera tale da prevedere la possibilità di implementare meccanismi di monitoraggio statistico delle transazioni ed alert che individuino comportamenti anomali o a rischio al fine di consentire eventuali attività di Audit interno da parte del Cliente.