Le misure **ORGANIZZATIVE** di seguito elencate sono state estrapolate da:

- Linee Guida in materia di Privacy e misure di sicurezza" Delibera n.60 del 11/12/2012
- Procedura PAC D3
- Nota SC Tecnico Patrimoniale Logistica ed Approvvigionamenti prot. 55486 del 04/10/2019

Le misure **TECNICHE** si riferiscono alla nota SC Tecnico Patrimoniale Logistica ed Approvvigionamenti prot. 60597 del 28/12/2017 in riferimento alla Circolare 18 aprile 2017, n. 2/2017, recante “Misure di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei Ministri 1° agosto 2015)”.

ID	TIPO	CATEGORIA	MISURA	ADOTTATA	IMPLEMENTAZIONE
1	Organizzative	Politiche, regolamenti e manuali	È stato definito un manuale per la gestione del protocollo informatico	SI	SI, adottato con Delibera n. 21 del 27/04/2012 e aggiornato ed integrato con Delibera n. 99 del 25/09/2014.
2	Organizzative	Politiche, regolamenti e manuali	Gli aspetti relativi alla sicurezza ICT e alla protezione dei dati sono contemplati nel piano di progetto e nella gestione del progetto.	SI	SI. (rif. nota SC TPLA prot. 55486 del 04/10/2019)
3	Organizzative	Politiche, regolamenti e manuali	Documento/regolamento sulle politiche di accesso alle informazioni, creazione utenze e relativi profili e permessi	SI	Esiste un regolamento informatico condiviso con ASL e in fase di approvazione. Esiste una "Informativa generale agli incaricati" disponibile in area Intranet e consegnata in fase di assegnazione dell'account di accesso ai sistemi. (rif. nota SC TPLA prot. 55486 del 04/10/2019)
4	Organizzative	Politiche, regolamenti e manuali	Formazione relativa al processo/applicativo in esame	SI	Si, formazione anno 2018 al Personale. Informativa inviata ai designati con nota prot. 60789 del 31/10/2019.
5	Organizzative	Politiche, regolamenti e manuali	Formazione relativa alla normativa sulla protezione dei dati	SI	In fase di implementazione, verrà utilizzata la sezione "Formazione" del Data Protection Manager

6	Organizzative	Politiche, regolamenti e manuali	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by design	SI	Regolamento Aziendale in materia di tutela dei dati personali AGGIORNAMENTO DELIBERAZIONE N. 91 DEL 24 MAGGIO 2019
7	Organizzative	Politiche, regolamenti e manuali	Sono state prese in considerazione le misure per ottemperare ai principi di Privacy by default	SI	Regolamento Aziendale in materia di tutela dei dati personali AGGIORNAMENTO DELIBERAZIONE N. 91 DEL 24 MAGGIO 2019
8	Organizzative	Ruoli e responsabilità	Sono definiti ruoli e responsabilità interne, in ambito sicurezza ICT e protezione dei dati	SI	SI, rif. nota SC TPLA prot. 55486 del 04/10/2019)
19	Organizzative	Gestione utenze	È in vigore una procedura formale per il rilascio delle credenziali e per la loro cancellazione.	SI	SI, rif. nota SC TPLA prot. 55486 del 04/10/2019.
20	Organizzative	Gestione utenze	La procedura per il rilascio delle credenziali è effettuata tramite mezzi automatizzati	NO	No, moduli cartacei. (rif. nota SC TPLA prot. 55486 del 04/10/2019)
21	Organizzative	Gestione utenze	La gestione dei privilegi e soggetta al principio del privilegio minimo ed è sottoposta a controlli formali	NO	No. La gestione è soggetta a controllo dei ruoli e dei privilegi associati agli operatori. (rif. nota SC TPLA prot. 55486 del 04/10/2019)
22	Organizzative	Gestione utenze	Le utenze rilasciate vengono controllate periodicamente tramite un procedimento formale al fine di garantirne la coerenza.	NO	No.. (rif. nota SC TPLA prot. 55486 del 04/10/2019)
23	Organizzative	Gestione utenze	I privilegi di amministrazione vengono rilasciati ai soli utenti che abbiano le competenze adeguate e la necessità operativa.	SI	SI, (rif. nota SC TPLA prot. 55486 del 04/10/2019)
24	Organizzative	Gestione utenze	È mantenuto un inventario delle utenze amministrative.	SI	SI, (rif. nota SC TPLA prot. 55486 del 04/10/2019)
25	Organizzative	Gestione utenze	Le utenze amministrative sono formalmente autorizzate.	SI	SI, (rif. nota SC TPLA prot. 55486 del 04/10/2019)

26	Organizzative	Cifratura	Nelle politiche di sicurezza ICT sono definite le politiche sull'uso della cifratura	SI	Si verso le reti esterne e verso endpoint. La crittografia dei data base e del file system non è applicabile sull'attuale infrastruttura per problemi di performance. (rif. nota SC TPLA prot. 55486 del 04/10/2019)
27	Organizzative	Cifratura	È implementato un sistema di gestione delle chiavi crittografiche	SI	SI, (rif. nota SC TPLA prot. 55486 del 04/10/2019)
28	Organizzative	Cifratura	Le chiavi private sono adeguatamente protette	SI	SI, (rif. nota SC TPLA prot. 55486 del 04/10/2019)
30	Organizzative	Copie di sicurezza	È definito un piano formalmente approvato al fine di garantire la Continuità Operativa e il Disaster Recovery	NO	Esiste una procedura di Business Continuity / Disaster Recovery condivisa con ASL e in fase di approvazione. (rif. nota SC TPLA prot. 55486 del 04/10/2019)
31	Organizzative	Copie di sicurezza	È stato redatto un manuale per la conservazione digitale	SI	Deliberazione n. 76 del 23/4/2019 "APPROVAZIONE MANUALE DEI PROCESSI DI FORMAZIONE E CONSERVAZIONE DEI DOCUMENTI ELETTRONICI". (rif. nota SC TPLA prot. 55486 del 04/10/2019)
32	Organizzative	Copie di sicurezza	Sono previste procedure di controllo al fine di garantire l'effettività delle procedure di ripristino	SI	SI. Per i backup è utilizzato un software specifico (VEEAM e MICROSOFT DATA PROTECTOR) con le relative funzioni di restore (rif. nota SC TPLA prot. 55486 del 04/10/2019).

77	Organizzative	Misure di sicurezza analogiche	Contenitori (armadi, schedari, ecc.) muniti di serratura	SI	Conservazione dei dati e dei documenti, in armadi o cassetti dotati di serratura o di altri sistemi di chiusura che ne consentano un accesso selezionato, evitando che gli stessi siano collocati in spazi liberamente accessibili al pubblico (ad es. corridoi, sale di attesa, sale riunioni, ecc...) (Rif. Linee Guida in materia di Privacy e misure di sicurezza" Delibera n.60 del 11/12/2012 - pag. 15 dell'allegato) (si veda anche (rif. nota SC TPLA prot. 55486 del 04/10/2019)
78	Organizzative	Misure di sicurezza analogiche	Chiusura a chiave dei locali	SI	Garanzia di un'adeguata chiusura dei locali nei quali sono custoditi o trattati i dati personali, durante le pause di lavoro, o al di fuori del normale orario di servizio. Si veda procedura PAC D3 e nota SC TPLA prot. 55486 del 04/10/2019)
79	Organizzative	Misure di sicurezza analogiche	Sistema di videosorveglianza	SI	L'ASL AT ha installato sistemi di videosorveglianza ed in osservanza della disciplina dettata in materia del Garante per la protezione dei dati personali ha adottato con deliberazione del Commissario n. 4 del 10 febbraio 2012 il "Regolamento dell'uso dei sistemi di videosorveglianza presso le sedi operative dell'ASL AT". Garanzia di un'adeguata chiusura dei locali nei quali sono custoditi o trattati i dati personali, durante le pause di lavoro, o al di fuori del normale orario di servizio. IN FASE DI REVISIONE (rif. nota SC TPLA prot. 55486 del 04/10/2019)
80	Organizzative	Misure di sicurezza analogiche	Cartello per divieto di accesso a soggetti non autorizzati	NO	Misura non adottata rif. nota SC Tecnico Patrimoniale Logistica ed Approvvigionamenti prot. 55486 del 04/10/2019.

81	Organizzative	Misure di sicurezza analogiche	Sistemi di controllo degli accessi	SI	Le misure di sicurezza attuate allo scopo di garantire il controllo sul movimento delle persone e dei beni consistono, a titolo di esempio, nell'avvalersi di un servizio di portineria presso l'Ospedale Cardinal Massaia di Asti, presso l'Ospedale Valle Belbo e infine, presso la sede legale/amministrativa dell'ASL AT di Via Conte Verde, 125 Asti al fine di garantire i seguenti servizi: · servizio di front office e centralino che costituisce l'interfaccia primaria che i soggetti esterni all'ASL AT hanno con l'azienda; · servizio di controllo flusso e deflusso persone in entrata/uscita dai locali aziendali al fine di garantire l'incolumità delle persone presenti e la sicurezza di cose e persone; · verifica chiusura e apertura accessi, verifica effettuata, altresì, dagli operatori amministrativi/sanitari in possesso di chiavi per i propri uffici/reparti di competenza. Il controllo degli accessi ne Presidio Cardinal Massaia avviene mediante monitor posizionati agli ingressi Parcheggio, Fornitori e Morgue; tali ingressi sono chiusi alle ore 23.00 con riapertura alle ore 5.00 del giorno successivo. Inoltre, l'utilizzo di sistemi di videosorveglianza, oltre che avere un elevato effetto deterrente, è di fondamentale importanza per verificare eventuali segnalazioni di allarme. E' attivo in azienda un servizio per la gestione dell'attività di controllo, sostituito dalle ore 20.00 alle ore 8.00 del giorno successivo da personale in reperibilità tecnica.

					Di norma i reparti sono dotati di card di reparto, documenti in cui sono inserite tutte le informazioni afferenti alle varie strutture aziendali ivi comprese le norme di comportamento. In ogni caso occorre precisare che l'accesso ai reparti è consentito negli orari definiti dalle singole strutture, accessi in orari diversi da parte di parenti o assistenti alla degenza è consentito previa autorizzazione rilasciata dal personale della struttura secondo quanto risultante dal regolamento di assistenza ai degenti. Si veda procedura PAC D3. precisare che l'accesso ai reparti è consentito negli orari definiti dalle singole strutture, accessi in orari diversi da parte di parenti o assistenti alla degenza è consentito previa autorizzazione rilasciata dal personale della struttura secondo quanto risultante dal regolamento di assistenza ai degenti. Si veda procedura PAC D3. (rif. nota SC TPLA prot. 55486 del 04/10/2019)
82	Organizzative	Misure di sicurezza analogiche	Sistemi di identificazione e registrazione per gli accessi post-orario di lavoro	SI	Al di fuori dell'orario di visita la porta di accesso al reparto è chiusa ed il personale può accedere esclusivamente attraverso l'utilizzo del badge. Si veda procedura PAC D3. (rif. nota SC TPLA prot. 55486 del 04/10/2019)
83	Organizzative	Misure di sicurezza analogiche	Sistemi antincendio	SI	Si veda procedura PAC D3. (rif. nota SC TPLA prot. 55486 del 04/10/2019)
84	Organizzative	Misure di sicurezza analogiche	Sistema antiallagamento	SI	Si presente. (rif. nota SC TPLA prot. 55486 del 04/10/2019)

85	Organizzative	Misure di sicurezza analogiche	Sistema antintrusione	SI	Si veda procedura PAC D3. (rif. nota SC TPLA prot. 55486 del 04/10/2019)
86	Organizzative	Misure di sicurezza analogiche	Sorveglianza da parte di personale autorizzato e formato	SI	Si veda procedura PAC D3. (rif. nota SC TPLA prot. 55486 del 04/10/2019)
87	Tecniche	ABSC 1	1.1 - Implementare un inventario delle risorse attive collegate alla rete.	SI	Viene mantenuto in inventario di tutte le risorse attive dall'area sistemi che viene controllato ed aggiornato puntualmente; il range degli indirizzamenti di rete e le appartenenze alle diverse VLAN sono trattati dall'area sistemi per applicare e garantire la necessaria sicurezza informatica alla infrastruttura tecnologica.
93	Tecniche	ABSC 1	3.1 - Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	SI	L'inventario è mantenuto puntualmente aggiornato sia se i sistemi sono collegati in rete attraverso l'uso di IP statici dall'area sistemi sia se sono dinamici attraverso l'informazione fornita dall'agent OCS su ogni singolo device.
95	Tecniche	ABSC 1	4.1 - Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	SI	I sistemi con IP statico sono raccolti manualmente in un file Excel mantenuto puntualmente aggiornato mentre l'OCS mantiene puntualmente aggiornati i sistemi a IP dinamico attraverso l'utilizzo di agent installati in ogni immagine con cui vengono clonati i sistemi.
100	Tecniche	ABSC 2	1.1 - 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.	SI	Gli utenti generici, escludendo gli amministratori di sistema/applicativi autorizzati e identificati sul documento relato al Provvedimento del Garante su AdS, non hanno permessi di poter installare qualsiasi software. L'elenco del software autorizzato è depositato e visibile in una opportuna area di progetto.

104	Tecniche	ABSC 2	3.1 - Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	SI	Le postazioni hanno un agent che permette, alla loro attivazione in rete, di essere visibili automaticamente sul sistema OCS in modo da rilevare anche eventuali programmi non autorizzati.
108	Tecniche	ABSC 3	1.1 - Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	SI	Vengono utilizzati per ogni sistema sul dominio Antimalware, anti vulnerabilità tramite WSUS ed utilizzando MS GPO per ulteriori restrizioni che aumentano il livello di sicurezza.
111	Tecniche	ABSC 3	2.1 - Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	SI	Nell'inserimento di nuovi sistemi nel dominio è utilizzata la distribuzione WDS afferente ad immagini già implementate in hardening (NSA) e utilizzando nella loro attivazione, le MS GPO.
112	Tecniche	ABSC 3	2.2 - Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	SI	Ciò avviene tramite utilizzo della "clonazione".
114	Tecniche	ABSC 3	3.1 - Le immagini d'installazione devono essere memorizzate offline.	SI	Tramite l'utilizzo del WDS e seguendo la procedura di backup, descritta dal documento formale di progetto del backup, le immagini del computer sono memorizzate off-line.
116	Tecniche	ABSC 3	4.1 - 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).	SI	Utilizzo per client protocollo MS msra, per device/server si utilizzano i protocolli rdp, https e ssh.

123	Tecniche	ABSC 4	1.1 - 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.	SI	Questa attività è in capo agli amministratori di sistema che utilizzando strumenti automatici quali WSUS ed interfacciandosi con fornitori di sistemi (apparati di rete, appliance, sistemi operativi, applicazioni...) effettuano gli aggiornamenti con la direzione ASL, almeno una volta ogni sei mesi.
131	Tecniche	ABSC 4	4.1 - Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	SI	Vedere 4.1.1
133	Tecniche	ABSC 4	5.1 - Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	SI	Relativamente alle postazioni di lavoro le patch vengono scaricate mensilmente su WSUS ed applicate dopo i test mentre quotidianamente sono aggiornati tutti i software antivirus, firewall, ecc.
134	Tecniche	ABSC 4	5.2 - Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.	SI	Tutti i computer sono "joined " al dominio asl19.ad
136	Tecniche	ABSC 4	7.1 - 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.	SI	Attività in capo agli amministratori di sistema.

138	Tecniche	ABSC 4	8.1 - Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabi- lità , del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).	SI	E' in corso di definizione.
139	Tecniche	ABSC 4	8.2 - 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	Attività in capo agli amministratori di sistema.
142	Tecniche	ABSC 5	1.1 -Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	SI	Realizzata attraverso la abilitazione di tali privilegi ai singoli amministratori di sistema/applicazione conformandosi al provvedimento del garante e non lasciando al singolo utente diritti di amministrazione del computer.
143	Tecniche	ABSC 5	1.2 - Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	SI	Realizzata attraverso l' abilitazione di tali privilegi ai singoli amministratori di sistema/applicazione, conformandosi al provvedimento del garante. Tale attività è normata da una procedura interna.
146	Tecniche	ABSC 5	2.1 - Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	SI	Realizzata attraverso la abilitazione di tali privilegi ai singoli amministratori di sistema/applicazione, conformandosi al provvedimento del garante. Tale attività è normata da una procedura interna.

148	Tecniche	ABSC 5	3.1 - Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.	SI	Questa restrizione è attivata nella fase di attivazione postazione di lavoro tramite la distribuzione delle immagini (MS WDS) e il "rename" dell'account amministrativo locale.
154	Tecniche	ABSC 5	7.1 - Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).	SI	Attivabile attraverso utilizzo di GPO.
156	Tecniche	ABSC 5	7.3 - Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	SI	Attivabile attraverso utilizzo di GPO.
157	Tecniche	ABSC 5	7.4 - Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	SI	Attivabile attraverso utilizzo di GPO.
162	Tecniche	ABSC 5	10.1 - Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	SI	Esiste informativa agli Amministratori di sistema nominati all'interno della conformità al provvedimento sugli AdS del Garante Privacy.
163	Tecniche	ABSC 5	10.2 - Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	SI	Realizzata nella implementazione conforma al Provvedimento sugli ADS del Garante Privacy.

164	Tecniche	ABSC 5	10.3 - 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	SI	Realizzata nella implementazione conforme al Provvedimento sugli ADS del Garante Privacy.
166	Tecniche	ABSC 5	11.1 - Conservare le credenziali amministrative in modo da garantirne disponibilità	SI	La utenza privilegiata "root" e "administrator" dei sistemi è usata soltanto per le emergenze bloccanti ed è mantenuta in busta chiusa da responsabile tecnico RTI.
167	Tecniche	ABSC 5	11.2 - Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	SI	Non usiamo certificati digitali per la autenticazione.
168	Tecniche	ABSC 8	1.1 - 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.	SI	Implementato attraverso l'utilizzo di OfficeScan (TrendMicro).
169	Tecniche	ABSC 8	1.2 - Installare su tutti i dispositivi firewall ed IPS personali.	SI	Nel progetto di e-security aziendale si è configurata una centralizzazione di tali funzionalità attivando sui singoli dispositivi in dominio le opportune MS GPO con la opportuna configurazione di OfficeScan (TrendMicro).
174	Tecniche	ABSC 8	3.1 - Limitare l’uso di dispositivi esterni a quelli necessari per le attività aziendali.	SI	Tale limitazione consiste, se autorizzato da ASL, nella collocazione di tali dispositivi esterni su una opportuna VLAN separata dalla VLAN aziendale.

181	Tecniche	ABSC 8	7.1 - Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	SI	Implementato attraverso l'utilizzo di OfficeScan (TrendMicro)e MS GPO.
182	Tecniche	ABSC 8	7.2 - Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	SI	Implementato attraverso l'utilizzo di OfficeScan (TrendMicro)e MS GPO.
183	Tecniche	ABSC 8	7.3 - Disattivare l'apertura automatica dei messaggi di posta elettronica.	SI	Implementato attraverso l'utilizzo di OfficeScan (TrendMicro)e MS GPO.
184	Tecniche	ABSC 8	7.4 - Disattivare l'anteprima automatica dei contenuti dei file.	SI	Implementato attraverso l'utilizzo di OfficeScan (TrendMicro)e MS GPO.
185	Tecniche	ABSC 8	8.1 - Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	SI	Implementato attraverso l'utilizzo di OfficeScan (TrendMicro).
186	Tecniche	ABSC 8	9.1 - Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.	SI	Implementato attraverso l'utilizzo di OfficeScan (TrendMicro).
187	Tecniche	ABSC 8	9.2 - Filtrare il contenuto del traffico web.	SI	Implementato attraverso l'utilizzo di Greylisting, antivirus e FortiGuard(Fortinet).
191	Tecniche	ABSC 10	1.1 - Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	SI	Questa funzionalità è assicurata utilizzando Veeam e DataProtector seguendo il progetto di backup formalizzato.

195	Tecniche	ABSC 10	3.1 - 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.	SI	Il backup è effettuato su network privato (non utilizzato cloud) attraverso Veeam e DataProtector che dispongono della funzionalità di crittografia nella copia dei dati anche se non attivata per evitare problemi di performances.
196	Tecniche	ABSC 10	4.1 - 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.	SI	I sistemi informativi effettuano una terza copia su tape nel sito di DR&BC di Torino (off-line file sharing e database).
197	Tecniche	ABSC 13	1.1 - 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.	SI	Trattandosi di Azienda Sanitaria, i data base contengono dati sensibili. Sarà sviluppata con l'outsourcer del Sistema Informativo e fornitore dei prodotti software, un'analisi per verificare la fattibilità tecnica per l'introduzione di strumenti di crittografia.
206	Tecniche	ABSC 13	8.1 - Bloccare il traffico da e verso url presenti in una blacklist.	SI	Nel progetto di e-security questo criterio è implementato attraverso l'utilizzo di FortiGuard (Fortinet).