Allegato A

Piano per la sicurezza informatica e per la tutela dei dati personali

ASP Ambito 9

Approvato con Delibera del Consiglio di Amministrazione n. 35 del 25.07.2024

Sommario

Premessa

Importanza del Piano di Sicurezza Informatica e della Tutela dei Dati Personali

La sicurezza informatica e la tutela dei dati personali sono fondamentali per qualsiasi organizzazione, specialmente per un ente pubblico che gestisce informazioni sensibili e critiche. Un piano di sicurezza ben strutturato è essenziale per proteggere i dati da accessi non autorizzati, perdite o alterazioni, garantendo la continuità operativa e la fiducia dei cittadini. Gli obiettivi principali di tale piano includono:

- **Disponibilità:** Assicurare che i documenti e le informazioni siano sempre accessibili quando necessario.
- **Integrità:** Mantenere la correttezza e la completezza dei dati.
- **Riservatezza:** Proteggere le informazioni da accessi non autorizzati.

Questi aspetti sono indispensabili per il corretto funzionamento e la trasparenza dell'ente. Inoltre, è cruciale che il piano di sicurezza informatica sia sottoposto a revisioni periodiche per adeguarsi alle continue evoluzioni tecnologiche e normative, mantenendo un elevato livello di sicurezza e conformità con le leggi vigenti.

Infrastruttura e Scenari dell’ASP Ambito 9

L'infrastruttura dell'ASP Ambito 9 prevede vari scenari e attori, descritti nei paragrafi seguenti. **Questo documento si concentra principalmente sulla rete LAN, lo scenario predominante per l'ente**, dove risiedono dati critici come le cartelle di rete e il sistema di gestione documentale. La rete LAN è gestita in parte dall’ASP Ambito 9, in parte dal Servizio Sviluppo Tecnologico del Comune di Jesi, per mezzo di apposito contratto di servizio.

Prospettive Future

Si sottolinea che il presente documento rappresenta una fotografia della situazione attuale (AS-IS). Sono previste significative modifiche all’attuale configurazione già nel 2025, con la programmata migrazione al Polo Strategico Nazionale dei server attualmente allocati presso i locali del comune di Jesi.

Componente Organizzativa della Sicurezza

La struttura organizzativa preposta alla sicurezza informatica e alla protezione dei dati nell'ente pubblico è articolata in diverse componenti chiave e personale specializzato. Il personale preposto include un responsabile dei sistemi informativi dell'ASP Ambito 9 (che afferisce all'Unità Operativa Amministrativa), e il servizio sviluppo tecnologico del Comune di Jesi.

1. Rete LAN

L'infrastruttura hardware dell'ASP Ambito 9 e del Comune di Jesi è progettata per supportare in modo robusto le operazioni quotidiane, garantendo al contempo una connettività affidabile e sicura.

Per l'ASP Ambito 9 (d'ora in avanti ASP), la connettività Internet è fornita tramite un ponte radio che riceve il segnale da un analogo ponte radio presso il Comune di Jesi. Questo setup permette una connessione efficiente e continua, essenziale per le operazioni quotidiane dell'ASP. All'interno dell'Ente, sistemi di switch dedicati gestiscono il traffico di rete tra le varie postazioni di lavoro, assicurando una comunicazione fluida e sicura tra gli utenti e i servizi centralizzati.

L'ASP dispone di due sedi poste una di fronte all'altra: la casa di riposo "Vittorio Emanuele II" e "Villa Borgognoni", entrambe in via Gramsci a Jesi. Il ponte radio principale, che comunica con il comune di Jesi, è dislocato sulla sede della casa di riposo e il segnale viene trasmesso alla sede in Villa Borgognoni tramite un secondo ponte radio.

Nel contesto del Comune di Jesi, l'infrastruttura hardware include un ponte radio simile per garantire la connessione Internet, sistemi di switch per la gestione del traffico di rete e due server centrali. Questi server ospitano applicazioni critiche e dati sensibili, supportando le funzioni amministrative e di servizio verso i cittadini (Figura 1)

Entrambe le infrastrutture sono progettate con un focus sulla sicurezza e l'affidabilità, supportate da controlli di accesso e monitoraggio continuo per proteggere l'integrità dei dati e garantire la continuità operativa.

Le misure di sicurezza fisica e logica specifiche e le procedure comportamentali adottate per la protezione dell'infrastruttura del sistema di gestione documentale, delle informazioni e dei dati sono dettagliate nei paragrafi seguenti.

Il Servizio Sviluppo Tecnologico del Comune di Jesi comprende un Help Desk remoto di primo livello, dedicato alla risoluzione dei malfunzionamenti che impediscono il regolare funzionamento delle postazioni informatiche nelle sedi dell'ASP di Via A. Gramsci, 95 e Villa Borgognoni. In queste sedi, vengono condivisi gli standard tecnologici del Comune di Jesi per la gestione del Dominio Microsoft, la sicurezza informatica perimetrale (firewall), i processi di backup, la gestione del database Oracle, i servizi di Intranet, la connettività a Internet, la distribuzione del software e la manutenzione dei sistemi marcatempo. Inoltre, è

previsto l'aggiornamento del software "sicr@web" per l'uso esclusivo dell'ASP e l'erogazione dei servizi per la rilevazione delle presenze e l'elaborazione delle paghe. L'infrastruttura comprende anche il mantenimento del software Intranet per la gestione delle Badanti, dello Storage comunale acquisito dall'ASP, del server in Cloud di rete civica per il sito istituzionale dell'ASP.

A livello infrastrutturale, l'ASP dispone di due macchine virtuali conservate dal Comune di Jesi:

- **ASP-MAG-AS:** sistema di protocollo e gestione documentale (JIRIDE di Sicr@WEB)
- **ASP-MS-FS:** cartelle di rete dell'ente

Sono predisposti regolari backup dei dati e un piano di disaster recovery per garantire il ripristino rapido e completo delle informazioni in caso di perdita o danneggiamento dei dati.

Il backup è organizzato nel seguente modo:

- Backup primario: frequenza 1v/dì, con 14-21 punti di recupero
- Backup secondario: frequenza di conservazione giornaliera, backup immodificabile per 14gg, con una politica di Retention a Lungo Termine di un Full per 1 settimana

  I Backup sono conservati in due differenti Sale Macchine dislocate in due diversi palazzi della sede Municipale.

- Disaster recover: invio delle repliche, con frequenza giornaliera, 1 punto di recupero (1gg), inviato al Palazzetto dello sport

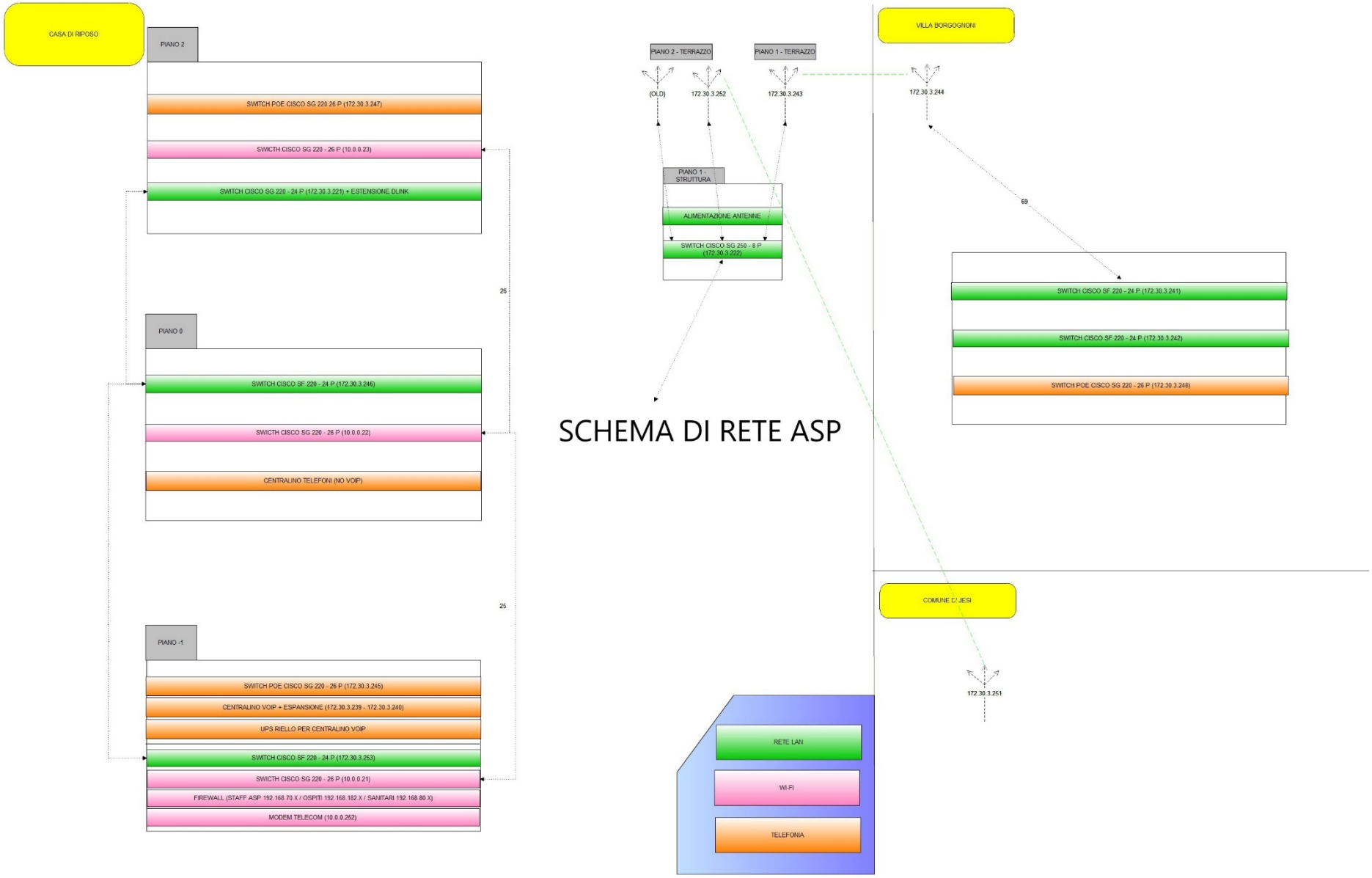

Figura 1- scherma di rete dell'ASP Ambito

Componente Fisica della Sicurezza

In questa sezione si descrivono le misure di sicurezza fisica adottate per proteggere le risorse informatiche e i dati.

Alla data di stesura del presente documento, le risorse fisiche hardware (SERVER) sono posizionate nella sala CED presso la sede del Comune di Jesi, con due backup memorizzati in diversi palazzi della sede Municipale, ed un sito di Disaster Recovery situato presso il Palazzetto dello Sport. Queste misure includono:

- **Controllo degli accessi fisici ai locali tecnici:** Vengono implementati sistemi di controllo per limitare l'accesso ai soli autorizzati
- **Misure di protezione da incendi:** Sono in atto misure preventive come sensori di fumo e sistemi di spegnimento automatico degli incendi

Componente Logica della Sicurezza

In questa sezione si illustreranno le misure di sicurezza logica implementate per garantire la riservatezza, l'integrità e la disponibilità dei dati. Queste misure includono:

- **Gestione degli account utente e delle password:** la gestione degli account e delle password in un dominio Windows avviene in modo centralizzato e sicuro, applicando criteri di complessità e scadenza, e mantenendo un audit completo delle attività. Questo permette di avere un maggiore controllo e protezione degli accessi ai sistemi e alle informazioni. Nello specifico:
    - Gestione centralizzata degli account: In un dominio Windows, gli account utente sono gestiti centralmente dal controller di dominio. Questo permette di avere un unico punto di amministrazione e controllo degli accessi.
    - Autenticazione centralizzata: Quando un utente accede al dominio, la sua autenticazione viene gestita dal controller di dominio, che verifica le credenziali (nome utente e password) contro il database degli account.
    - Criteri di password: Il controller di dominio può applicare criteri di complessità e scadenza delle password, come lunghezza minima, requisiti di caratteri speciali, scadenza periodica, ecc. Questi criteri vengono applicati in modo uniforme a tutti gli account del dominio.
    - Archiviazione sicura delle password: Le password degli utenti non vengono archiviate in chiaro, ma vengono memorizzate in forma hash (una rappresentazione crittografica della password) sul controller di dominio. Questo impedisce l'accesso diretto alle password.
    - Audit e monitoraggio: Tutte le attività di accesso e modifica degli account e delle password vengono registrate nei log di dominio
- **Sistemi di autenticazione e autorizzazione:** Sono implementati sistemi robusti di autenticazione e autorizzazione per garantire l'accesso controllato alle risorse informatiche e ai dati sensibili. Gli utenti possono accedere a questi dati attraverso il sistema di gestione documentale descritto nei paragrafi successivi, nonché attraverso cartelle di rete memorizzate su un server dedicato e accessibili tramite condivisioni di rete. È fondamentale notare che l'accesso alle cartelle di rete è limitato ai soli utenti autorizzati e avviene esclusivamente quando sono connessi alla rete del dominio, garantendo così la sicurezza e l'integrità dei dati attraverso controlli rigorosi

di autenticazione e autorizzazione. Le abilitazioni di accesso alle cartelle di rete vengono richieste tramite apposito processo di richiesta all'helpdesk. Invece le abilitazioni di accesso al sistema di gestione documentale vengono rilasciate dal responsabile dei sistemi informativi dell'ASP.

- **Sistemi antivirus e anti-malware:** Vengono utilizzati software antivirus e anti-malware aggiornati regolarmente per proteggere i sistemi da software dannoso e prevenire attacchi informatici (alla data di stesura del presente documento, il software utlizzato è Sophos Antivirus)
- **Firewall e sistemi di prevenzione delle intrusioni:** Sono installati firewall e sistemi di prevenzione delle intrusioni (IPS) per monitorare e bloccare attività sospette o non autorizzate sulla rete.
- **Backup e disaster recovery:** Sono predisposti regolari backup dei dati e un piano di disaster recovery per garantire il ripristino rapido e completo delle informazioni in caso di perdita o danneggiamento dei dati.

  Il backup è organizzato nel seguente modo

  - Backup primario: frequenza 1v/dì, con 14-21 punti di recupero
  - Backup secondario: frequenza di conservazione giornaliera, backup immodificabile per 14gg, con una politica di Retention a Lungo Termine di un Full per 1 settimana

  I Backup sono conservati in due differenti Sale Macchine dislocate in due diversi palazzi della sede Municipale.

  - Disaster recover: invio delle repliche, con frequenza giornaliera, 1 punto di recupero (1gg), inviato al Palazzetto dello sport

Queste misure sono fondamentali per proteggere l'infrastruttura informatica e assicurare che i dati rimangano sicuri, accessibili solo a chi è autorizzato e integri nel tempo.

2. Reti dei Comuni - Personale Dislocato

Le postazioni dei dipendenti dell'ASP Ambito 9, operativi presso i comuni che hanno delegato i servizi sociali all'ASP (UPS), generalmente utilizzano attrezzature fornite dalle amministrazioni locali, in conformità con le normative di sicurezza vigenti nell'ente di competenza. In situazioni eccezionali, in cui i comuni non siano in grado di fornire postazioni adeguate, l'ASP provvede alla distribuzione di computer portatili configurati per connettersi alle reti dei comuni interessati. Questi portatili sono equipaggiati con l'ultima versione del sistema operativo Windows, con aggiornamenti automatici e software antivirus attivi.

Dato l'aleatorietà degli scenari e la difficoltà di verificare le reti esterne all'ASP, tutti i dipendenti sono stati formati sui principi della sicurezza informatica, includendo obblighi e divieti, specificati nel regolamento dei sistemi informativi dell'ASP, che stabilisce prescrizioni dettagliate per garantire la sicurezza delle informazioni.

La gestione delle postazioni presso i comuni è attualmente oggetto di studio e revisione, con l'obiettivo di centralizzare la gestione dei dati attualmente residenti su postazioni esterne

al dominio del Comune di Jesi, migliorando l'efficienza e la sicurezza del sistema informativo dell'ASP.

3. Rete Wi-Fi

Componente Fisica della sicurezza

Nella sede dell'ASP allocata presso la "casa di riposo" è disponibile una rete Wi-Fi, su una linea separata rispetto alla rete LAN. Questa rete Wi-Fi è utilizzata dai dipendenti dell'ASP, dagli ospiti della casa di riposo e dal personale sanitario operante nella struttura. Lo schema di rete della componente fisica si evince dalla figura 1.

E' previsto un firewall perimetrale il cui software è regolarmente aggiornato dalla ditta che con la quale è in essere un contratto di manutenzione, da una serie di switch ed Access Point dislocati all'interno della struttura.

Componente Logica della sicurezza

La rete è organizzata in tre VLAN distinte per garantire la separazione delle reti e la sicurezza.

- **VLAN Staff ASP:** destinata ai dipendenti della casa di riposo, accessibile tramite user e password periodicamente sostituite.
- **VLAN Ospiti:** accessibile mediante registrazione.
- **VLAN Sanitari:** sicura tramite accesso vincolato a specifiche postazioni riconosciute mediante MAC address. Questa VLAN è utilizzata da personale non dipendente dell'ASP, ossia dipendente delle cooperative che di volta in volta risultano aggiudicatrici dell'appalto per la gestione della casa di riposo, alle quali vengono consegnate istruzioni e raccomandazioni di utilizzo.

4. Servizi in Cloud SaaS

Alcuni servizi sono stati affidati a fornitori terzi in modalità cloud SaaS, come la posta elettronica dei dipendenti, lo sportello telematico polifunzionale (per accogliere le domande on-line dei cittadini) e il software di contabilità. In queste situazioni, la sicurezza è demandata ai gestori dei servizi, responsabili dell'implementazione e della manutenzione delle misure di protezione necessarie per garantire la riservatezza, l'integrità e la disponibilità dei dati.

5. Dispositivi Gestiti da Fornitori Esterni

Nell'infrastruttura descritta, alcuni dispositivi sono connessi alla rete del Comune di Jesi ma gestiti da fornitori esterni mediante appositi contratti di manutenzione, come stampanti multifunzione e switch per la telefonia VoIP (Figura 1)

Inoltre, anche i dispositivi della rete Wi-Fi "NON" connessi alla rete LAN del comune di Jesi (firewall, switch, access point) sono gestiti tramite appositi contratti di manutenzione con fornitori esterni.

Infine, la casa di riposo ha un sistema di videosorveglianza su circuito chiuso, le cui immagini non sono proiettate in rete e quindi non accessibili dall'esterno.

Livelli di sicurezza "Minimi" per le Pubbliche Amministrazioni

Il documento "Misure minime di sicurezza ICT per le Pubbliche Amministrazioni" del 26 aprile 2016, elaborato dall'Agenzia per l'Italia Digitale, fornisce una guida pratica per le Pubbliche Amministrazioni italiane al fine di implementare un livello minimo di sicurezza informatica, in linea con le indicazioni della Direttiva del Presidente del Consiglio dei Ministri del 1 agosto 2015

Il documento sottolinea come il panorama delle minacce informatiche stia rapidamente evolvendo e come anche la Pubblica Amministrazione sia diventata un bersaglio specifico. In particolare, si evidenzia il ruolo di attori ostili organizzati, dotati di notevoli risorse, che agiscono in modo silenzioso per ottenere il controllo remoto dei sistemi, spesso attraverso l'acquisizione di privilegi elevati. Diventa quindi fondamentale per la PA non solo dotarsi di misure preventive tradizionali, come antivirus e firewall, ma anche di strumenti di rilevamento delle anomalie, in grado di individuare tempestivamente eventuali compromissioni.

Per rispondere a questa esigenza, il documento definisce un set di controlli di sicurezza di base, denominati AgID Basic Security Controls (ABSC), che traggono ispirazione dai primi 5 CSC, considerati essenziali per garantire un livello minimo di protezione. A questi si aggiungono le misure relative alle difese contro i malware (CSC 8), alle copie di sicurezza (CSC 10) e alla protezione dei dati (CSC 13), ritenute fondamentali nel contesto italiano. Ciascun ABSC viene scomposto in misure specifiche, organizzate su tre livelli di dettaglio, per consentire alle amministrazioni di adattare il sistema di sicurezza alle proprie esigenze specifiche.

Le informazioni presentate nei paragrafi seguenti si riferiscono alla rete LAN, come specificato in premessa, che rappresenta lo scenario predominante per l'ente. In questa rete risiedono dati critici come le cartelle di rete e il sistema di gestione documentale. La gestione della rete LAN è in parte affidata al Servizio Sviluppo Tecnologico del Comune di Jesi, tramite un apposito contratto di servizio. Pertanto, tali informazioni sono state raccolte, per quanto di competenza, dal suddetto servizio, Tuttavia, potrebbero non essere aggiornate e si rimanda alla documentazione aggiornata disponibile presso il Comune di Jesi.

ABSC 1 (INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI)

Gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso

- *Implementare un inventario delle risorse attive.*
  - SI, tramite aggiornamento manuale
- *Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.*
  - SI, tramite aggiornamento manuale
- *Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP*
  - SI, per dispositivi censiti e autorizzati.

ABSC 2 (INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI)

Gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione

- *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'istallazione di software non compreso nell'elenco*
  - In fase di potenziamento. Allo stato attuale è previsto un controllo centralizzato per i software sulle postazioni che richiedono permessi amministrativi.
- *Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato*
  - Non attualmente, in fase di potenziamento

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

Istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni

- *Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi*
  - SI (sulla base delle valutazioni delle "configurazioni sicure standard" effettuate dall'ente)
- *Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.*
  - SI (sulla base delle valutazioni delle "configurazioni sicure standard" effettuate dall'ente)
- *Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.*
  - SI (mediante formattazione della postazione)
- *Le immagini d'installazione devono essere memorizzate offline*
  - SI (in caso di formattazione si può ricorrere al software nativo disponibile in rete)
- *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, tramite canale sicuro

ABSC 4 (VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ)

Acquisire, valutare e intraprendere continuamente azioni in relazione a nuove informazioni allo scopo di individuare vulnerabilità, correggere e minimizzare la finestra di opportunità per gli attacchi informatici.

- *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 abbiamo strumenti che possono essere attivati ad hoc.
- *Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza*
  - SI
- *Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni*
  - SI per il sistema operativo, IN PARTE per il software (in fase di potenziamento)
- *Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.*
  - Non sono previsti sistemi air-gapped. Per i dispositivi staccati dalla rete LAN del comune, sono configurati gli aggiornamenti automatici del sistema operativo. Per l'aggiornamento dei dispositivi di rete afferenti alla rete Wi-Fi (Access Point, Firewall) si è dato mandato alla ditta con il quale è attivo apposito contratto di manutenzione.
- *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
- *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.)*
  - SI (utilizzo degli stessi standard per tutta la rete)
- *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 (per il sistema operativo)

ABSC 5 (USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE)

Regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi.

- *Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.*
  - SI

- *Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato*
  - SI (inteso come login)
- *Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.*
  - SI (per l'amministratore di sistema, è registrata l'afferenza ad un ufficio autorizzato).
- *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
- *Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza*
  - SI (l'autenticazione a due fattori è usata per l'accesso esterno).
- *Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).*
  - SI per le credenziali di dominio, in valutazione/in corso il password aging per utenti amministratori
- *Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).*
  - SI
- *Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.*
  - SI
- *Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona*
  - IN CORSO
- *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*
  - IN CORSO
- *Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza*
  - SI
- *Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette*
  - IN SPERIMENTAZIONE l'utilizzo di certificati digitali

ABSC 8 (DIFESE CONTRO I MALWARE)

Controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive

- *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 (per le workstation e i server)
- *Installare su tutti i dispositivi firewall ed IPS personali*
  - SI (installazione dei Firewall di Windows per le workstation)

- *Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.*
  - SI
- *Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili*
  - IN PARTE SI (interviene l'antivirus)
- *Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file*
  - IN PARTE SI (interviene l'antivirus), nei limiti dell'operatività che deve essere garantita.
- *Disattivare l'apertura automatica dei messaggi di posta elettronica*
  - ok, l'ASP ha adottato una webmail ove la sicurezza è garantita dalla sandbox del browser assieme ad altri filtri che sanitizzano eventuale codice malevolo.
- *Disattivare l'anteprima automatica dei contenuti dei file*
  - come sopra
- *Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione*
  - IN PARTE (interviene l'antivirus nel momento in cui viene effettuata una azione)
- *Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam*
  - SI: Il servizio di posta (in cloud) è dotato di sistema antispam, i messaggi che superano una certa soglia di assoluta certezza vengono distrutti mentre quelli potenzialmente in dubbio vengono spostati nella cartella "Posta indesiderata" dove i link non sono cliccabili ed è presente un avviso per l'utente.
- *Filtrare il contenuto del traffico web*
  - SI
- *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: Molte estensioni sono bloccate indipendentemente dalla presenza di codice pericoloso al loro interno: bat|chm|cmd|com|dll|do|exe|hta|js|jse|lnk|ocx|pif|reg|scr|shb|shm|cab|wsf|vbs|vbe|vbx|ace|jar|bin

ABSC 10 (COPIE DI SICUREZZA)

Procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità.

- *Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema*
  - SI per le cartelle di rete e per il repository del software di gestione documentale.
- *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*

- IN PARTE (La protezione fisica è garantita. Le repliche sono copie fisiche delle Virtual Machine: la crittografia è assicurata per i metadati associati alle Virtual Machine)

- *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 (le copie sono fisicamente delocalizzate)

ABSC 13 (PROTEZIONE DEI DATI)

Processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti

- *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*
  - Abbiamo requisiti di sicurezza trasversali a tutti i dati. Le cartelle di rete non sono crittografate. La situazione in evoluzione data l'imminente migrazione al Polo Strategico Nazionale ove si sta valutando se adottare storage "crittografato".
- *Bloccare il traffico da e verso url presenti in una blacklist.*
  - SI

Il Sistema di gestione documentale

Il Sistema informatico

Il sistema informatico è l'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle amministrazioni per la gestione dei documenti. (DPR 445/2000, art.1, lettera r).
La gestione dei flussi documentali è un insieme di funzionalità che consentono di trattare e di organizzare la documentazione prodotta (in arrivo, in partenza e interna) dalle amministrazioni.

Sicurezza del Sistema informatico

La sicurezza dei dati, delle informazioni e dei documenti informatici memorizzati (poi archiviati) nel sistema di gestione documentale è garantita dall'applicazione informatica adottata dall'ASP Ambito 9.
I dati, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento, vengono custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, agendo secondo il principio di privacy by default.
Gli elaboratori sono protetti contro il rischio di intrusione ad opera di programmi di cui all'art. 615 quinquies del codice penale (virus) mediante idonei programmi antivirus, la cui efficacia e il cui aggiornamento sono verificati periodicamente.

Il sistema di gestione documentale

Il sistema di gestione documentale è costituito dall'insieme delle tecnologie e da tutti i dispositivi e i programmi presenti presso le sedi dell'ASP Ambito 9 e del Comune di Jesi (ove risiede parte dell'infrastruttura hardware, di rete e software in uso nell'Ente) che permettono l'utilizzo del sistema.
In particolare, sono parte integrante dell'infrastruttura i cablaggi e gli apparati di rete presenti presso le sedi sopracitate e necessari per la connettività, i sistemi informatici e le componenti software sottese al sistema di autenticazione e tutte le postazioni di lavoro utilizzate dagli utenti del sistema di gestione documentale.
Le misure di sicurezza fisica e logica specifiche e le procedure comportamentali adottate per la protezione dell'infrastruttura del sistema di gestione documentale, delle informazioni e dei dati sono riportate nei paragrafi seguenti.

Le postazioni di lavoro

Per l'utilizzo del sistema di gestione documentale è previsto il coerente utilizzo delle postazioni di lavoro, da tavolo o portatili e l'impiego di dispositivi (hardware) e programmi (software) tali da consentire il corretto funzionamento e il mantenimento in condizioni di sicurezza ai fini del regolare svolgimento dell'attività lavorativa.

Le postazioni di lavoro soddisfano i criteri minimi di sicurezza, in particolare:
- il sistema operativo è aggiornato e aggiornabile;
- gli applicativi installati e i loro componenti software aggiuntivi (ad es., plug-in) sono aggiornati e aggiornabili;

• sono dotate di un programma antivirus con funzionalità automatica di aggiornamento periodico;
• l'accesso al sistema operativo della postazione di lavoro è protetto da password di adeguata complessità, cambiata con cadenza regolare;

Accesso ai dati e ai documenti informatici

Il sistema di gestione documentale adottato dall'ASP Ambito 9 garantisce:

• la protezione delle informazioni relative a ciascun utente nei confronti degli altri;
• la garanzia di accesso ai documenti, alle informazioni e ai dati esclusivamente agli utenti abilitati;
• il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppo di utenti;
• la registrazione delle attività svolte da ciascun utente anche rilevanti ai fini della sicurezza, in modo tale da garantirne l'identificazione;
• l'immodificabilità dei contenuti e, comunque, la loro tracciabilità.

Il controllo degli accessi è assicurato dall'utilizzo di credenziali di autenticazione con differenti profili di autorizzazione in relazione ai diversi ruoli di ciascun utente.

Sicurezza dei documenti informatici

L'accesso al sistema di gestione documentale da parte di ciascun utente dell'ASP Ambito 9 è gestito centralmente ed è subordinato all'abilitazione a cura del Responsabile della gestione documentale, di concerto con il responsabile del Servizio Informatica.
Le identità digitali utilizzate per l'accesso al sistema di gestione documentale sono costituite da nome utente e password. Il sistema di gestione documentale rispetta le misure di sicurezza previste dal Regolamento UE 2016/679 GDPR – General Data Protection Regulation relativo alla protezione dei dati personali.

Profili di abilitazioni di accesso interno alle informazioni documentali

Attraverso una access control list – ACL – il sistema di gestione documentale permette l'assegnazione differenziata dei profili di abilitazione, intervento, modifica e visualizzazione dei documenti di protocollo, in rapporto alle funzioni e al ruolo svolto dagli utenti e garantisce la protezione dei dati personali e dei dati sensibili.
L'accesso al sistema di gestione documentale, l'accessibilità e la riservatezza delle registrazioni, dei dati personali e di quelli sensibili, sono garantite tramite l'assegnazione differenziata di profili di abilitazione, in rapporto alla UOC e ufficio di appartenenza, alle funzioni e al ruolo svolto dagli utenti.

Criteri e modalità per il rilascio delle abilitazioni di accesso

A ciascun utente del sistema sono attribuiti diritti di visibilità diversificati in ragione dell'appartenenza a un determinato settore dell'organizzazione e delle specifiche funzioni derivanti dal ruolo e dai compiti assegnati.
Le abilitazioni di accesso per ciascun utente, la cessazione delle utenze del personale non più assegnato a funzioni che richiedano l'abilitazione al sistema, e la cessazione dal servizio dei dipendenti devono essere inoltrate dai responsabili delle UOC o del Servizio Risorse Umane al Responsabile della gestione documentale (coadiuvato dal responsabile del Servizio Informatica), che autorizza la creazione, la modifica, la cessazione delle utenze di concerto con il richiedente.
Periodicamente è verificata a cura del Responsabile della gestione documentale la sussistenza delle condizioni per il mantenimento dei profili di accesso.

Le procedure comportamentali ai fini della protezione dei documenti

Le postazioni di lavoro, da tavolo e portatili, o gli strumenti comunque funzionalmente assimilabili, di proprietà dall'Ente a vario titolo messi a disposizione del personale, sono uno strumento di lavoro e il loro utilizzo è finalizzato allo svolgimento delle attività professionali e istituzionali dell'ASP Ambito 9. Ogni utente adotta comportamenti corretti, tali da preservare il buon funzionamento degli strumenti e da ridurre i rischi per la sicurezza dei sistemi informativi.
In ogni caso, l'utilizzo delle risorse informatiche, non deve pregiudicare il corretto adempimento della prestazione lavorativa, ostacolare le attività dell'ASP Ambito 9 o essere destinato al perseguimento di interessi privati in contrasto con quelli pubblici. Gli utenti a cui sono affidate le postazioni di lavoro dell'Ente, sono soggetti a tutte le responsabilità dettate dalla normativa vigente e applicabile e da quanto previsto dal Regolamento dell'ASP Ambito 9 sulla gestione e organizzazione dei sistemi informativi (IT) approvato con delibera del Consiglio di Amministrazione n. 46 del 29.08.2023.

Conservazione Digitale

In relazione alle procedure di conservazione digitale dei documenti, è possibile fare riferimento al Manuale di gestione documentale ed al Manuale di conservazione dell'ente, per approfondimenti circa l'organizzazione del proprio sistema di conservazione digitale, le tecnologie utilizzate, le misure di sicurezza implementate e la conformità alle normative vigenti.

Misure di sicurezza e di protezione dei dati personali

In questa sezione si descriverà il sistema di gestione documentale e di protocollo informatico adottato, evidenziando l'ispirazione alle norme sulla protezione dei dati personali e al GDPR.4

Applicazione del Regolamento UE 2016/679 – GDPR

L'ASP Ambito 9 in qualità di Titolare del trattamento tratta i dati personali secondo i principi di liceità, correttezza e trasparenza nel rispetto del Reg. UE 2016/679, D.Lgs 196/2003 novellato dal D.Lgs 101/2018.
Le funzioni di titolare generale del trattamento dei dati per l'ASP Ambito 9 sono affidate alla figura del suo Presidente pro tempore. Il Presidente può delegare le relative funzioni al Direttore dell'ASP Ambito 9.
Responsabili interni del Trattamento dei dati sono i Responsabili di ogni singola Unità Operativa e il personale dell'area servizi generali dell'Ambito 9 (dipendenti), ciascuno in relazione ai dati trattati dalle strutture assegnate con i rispettivi atti di incarico.
In applicazione del Regolamento UE 2016/679 è stato nominato il DPO - Data Protection Officer dell'ASP Ambito 9. Per le referenze di contatto si rimanda al sito istituzionale dell'Ente.

Trattamento dei dati personali

Per trattamento di dati personali si intende qualsiasi operazione, o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati, applicate a dati personali o all'insieme di dati personali, anche se non registrati in una banca dati, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'elaborazione, la selezione, il blocco, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, la diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione di dati personali
Per tutto quello che concerne il trattamento dei dati personali, si rimanda all'Informativa Privacy pubblicata sul sito istituzionale dell'Ente.

Procedura in caso di Data Breach

Una violazione dei dati personali, nota come "data breach", si verifica quando, in modo accidentale o illecito, la sicurezza dei dati viene compromessa, comportando la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso indebito ai dati personali trasmessi, conservati o trattati. Questa violazione può essere causata da diverse situazioni, tra cui l'accesso abusivo ai sistemi informatici o il furto o la perdita di dispositivi informatici contenenti dati personali.

- **Scoperta e Notifica:** In caso di sospetta violazione dei dati, è fondamentale inviare immediatamente una notifica al Responsabile della protezione dei dati (DPO) includendo dettagli come la data dell'evento, la tipologia e la quantità di dati coinvolti, le categorie di persone interessate e le modalità di accaduto.

Il competente Responsabile della protezione dei dati, una volta ricevuta la comunicazione sul potenziale data breach, individua il soggetto che esercita le funzioni di titolare che sarà competente per la gestione della eventuale violazione e trasmette senza ritardo la comunicazione ai referenti privacy della struttura individuata

- **Obblighi del Titolare del trattamento in caso di data breach**
    - **Rilevare e inquadrare tempestivamente l'incidente di sicurezza**: il titolare deve verificare se si è verificata una violazione dei dati personali che comporti rischi per i diritti e le libertà degli interessati.
    - **Notificare il data breach all'Autorità Garante entro 72 ore**: il titolare ha l'obbligo di notificare all'Autorità di controllo la violazione dei dati personali, a meno che non sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche. L'eventuale ritardo dovrà essere motivato.

      Comunicare il data breach agli interessati: il titolare, in alcuni casi, deve comunicare senza ingiustificato ritardo la violazione agli interessati coinvolti, qualora la stessa presenti un rischio elevato per i loro diritti e libertà. I motivi per cui tale comunicazione non è richiesta sono disciplinati dall'articolo 34 del GDPR.
    - **Documentare l'evento nel registro dei data breach**: il titolare deve registrare l'evento, documentando le circostanze, le conseguenze e i provvedimenti adottati.
    - **Adottare misure per contenere i rischi e le conseguenze**: il titolare deve mettere in atto strategie per limitare i danni e le eventuali azioni correttive necessarie.
    - **Collaborare con il Responsabile della protezione dei dati**: il titolare deve supportare e coinvolgere adeguatamente il DPO nella gestione del data breach.

- **Obblighi del Responsabile del trattamento in caso di data breach**
    - Informare tempestivamente il titolare del trattamento **non appena viene a conoscenza di una violazione dei dati personali.**
    - Collaborare con il titolare fornendogli tutte le informazioni necessarie **per la notifica del data breach all'Autorità Garante entro 72 ore.**
    - Assiste il titolare nella comunicazione agli interessati coinvolti**, qualora la violazione presenti un rischio elevato per i loro diritti e libertà.**
    - Trattare i dati personali solo su istruzioni documentate del titolare**, anche in caso di subappalto di parte delle sue funzioni.**
    - Documentare le circostanze, le conseguenze e i provvedimenti adottati **nel registro dei data breach, in collaborazione con il titolare.**