PROVINCIA
DI REGGIO EMILIA

ATTO DI ORGANIZZAZIONE PER LA DEFINIZIONE DELLE LINEE GUIDA PER LA GESTIONE INFORMATIVA DIGITALE della Provincia di Reggio Emilia - ALLEGATO C - Sicurezza della gestione documentale e linee guida per l'acquisizione e manutenzione di strumenti hardware e software.

Il presente allegato specifica le misure di sicurezza adottate per la formazione, la gestione, la trasmissione, l'interscambio, l'accesso e la conservazione dei documenti informatici, in particolare la documentazione tecnico-progettuale, anche in relazione alle norme sulla protezione dei dati personali e alla sicurezza del sistema informativo dell'Ente ed è armonizzato col piano per la sicurezza informatica presente nel *Manuale di Gestione del protocollo informatico, dei documenti e dell'archivio* dell'Ente.

OBIETTIVI DEL PIANO DI SICUREZZA

Il piano di sicurezza garantisce che:

- i documenti e le informazioni trattate siano disponibili, integre e riservate;
- i dati personali comuni, particolari e/o giudiziari 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, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

GENERALITA'

Il Piano per la sicurezza informatica è redatto dal Servizio Sistemi Informativi e Tecnologici ed è formato da una serie di elementi in larga parte contenuti nel "*Disciplinare dei Sistemi Informativi*" in cui ultimo aggiornamento è stato approvato con Decreto del Presidente n. 152/2024 oltre che più in generale nel "*Modello di assessment della postura di sicurezza*" e nel "*Questionario di scoping atto a censire i principali asset e servizi di interesse in ambito cybersecurity*", aderenti al modello del *Framework Nazionale per la Cybersecurity e la Data Protection*, predisposti in fase di adesione al CSIRT (*Computer Security Incident Response Team*) Regionale nel 2024 e periodicamente aggiornati.
In particolare nei documenti sopra indicati, che sono periodicamente aggiornati anche in conseguenza di variazioni normative o organizzative dell'Ente oppure in seguito di eventi gravi, sono definite:

- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- l'analisi dei rischi che incombono sui dati;
- le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
- la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati

personali;
- la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;

ASPETTI GENERALI ATTINENTI ALLA SICUREZZA

Presso gli edifici dell'Ente sono ospitati i soli apparati di rete, la centrale telefonica Voip e le postazioni/dispositivi (*endpoint)*, tutto il resto dell'infrastruttura è ospitata nei datacenter qualificati della società partecipata Lepida Scpa in modalità *IaaS,* oltre ad alcuni servizi software settoriali erogati in modalità *SaaS* da fornitori qualificati da ACN (Agenzia per la Cybersicurezza Nazionale).

In particolare i datacenter di Lepida Scpa sono qualificati da ACN come *infrastruttura qualificata QC1* che risponde ai requisiti per le infrastrutture digitali e i servizi cloud, previsti dal *Regolamento per il Cloud della PA* di AgID del 15 dicembre 2021 e aggiornati con la determina n. 307 di ACN, anche ai fini dell'adeguatezza dell'infrastruttura a trattare sia i dati ordinari sia i dati critici. Lepida inoltre è in possesso della certificazione ISO 14001:2015 per i propri Datacenter che sono anche adeguati alle norme relative al *DNSH (Do No Significant Harm)*.

L'infrastruttura IaaS ospita in linea generale:
- il software CMDBuild per la gestione integrata degli asset, dei software e delle abilitazioni degli utenti del dominio provinciale;
- i software gestionali (protocollo, segreteria, albo pretorio, gestione del personale, sistema contabile, ecc);
- il sistema documentale per la gestione informativa digitale delle costruzioni in ottemperanza all'Art. 43 del Dlgs. n. 36/2023 (c.d. "Codice dei contratti pubblici"), per l'introduzione della metodologia Building Information Modeling (BIM) nell'Ente che fornisce anche la piattaforma per la condivisione dei file controllata, anche con soggetti esterni all'ente;
- la posta elettronica;
- il sistema cartografico;
- la documentazione condivisa e la gestione delle licenze dei software tecnici (CAD e GIS);
- il software di gestione della contabilità dei lavori;
- il file system condiviso;

che ricomprendono in larga parte la gestione documentale amministrativa e tecnica dell'Ente.

Le attività manutentive dell'infrastruttura fisica sono garantite dagli amministratori di sistema di Lepida Scpa, a livello invece di sistema operativi, virtualizzazione e sistemi informativi, le attività sono gestite dagli amministratori di sistema dell'Ente, coadiuvati da alcuni soggetti esterni che operano per conto di imprese fornitrici contrattualizzate dall'Ente, che si occupano di specifici ambiti.
I fornitori che accedono ai server virtuali, vengono nominati *Responsabili* rispetto al trattamento dati, e tale nomina definisce le modalità di accesso, i trattamenti dei dati e le risorse server a cui devono accedere per l'espletamento delle loro attività contrattuali. I profili di accesso sono limitati alle operazioni strettamente necessarie e dichiarate.
I server virtuali che ospitano i file e i dati fisici utilizzati dal sistema gestionale, sono configurati in maniera da garantire che:
- l'accesso diretto ai file e ai dati fisici, al di fuori del sistema di gestione documentale, sia riservato agli amministratori di sistema dell'Ente e al personale incaricato dalle ditte che

erogano assistenza e manutenzione al software, che hanno sottoscritto apposita apposita dichiarazione di responsabilità con l'Ente;
- la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, consentano l'identificabilità dell'utente stesso. Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.

I moduli software di gestione della documentazione amministrativa dell'Ente (protocollo, segreteria e moduli collegati), sono software proprietari, utilizzati in licenza d'uso e la ditta proprietaria garantisce siano realizzati e manutenuti conformemente alla normativa vigente e ai controlli previsti da framework e standard nazionali e internazionali di sicurezza delle informazioni. Relativamente alla gestione dei documenti inoltre:
- garantisce la disponibilità, la riservatezza e l'integrità dei documenti e del registro di protocollo;
- assicura la corretta e puntuale registrazione di protocollo dei documenti in entrata ed in uscita secondo la normativa vigente;
- gestisce la segnatura di protocollo con l'apposizione di un "sigillo elettronico qualificato" che ne garantisce l'integrità e autenticità del profilo *XAdES baseline B level signatures* definito in *ETSI EN 319 132-1 v1.1.1*;
- fornisce informazioni sul collegamento esistente tra ciascun documento ricevuto dall'Amministrazione e gli atti dalla stessa formati al fine dell'adozione del provvedimento finale;
- consente il reperimento delle informazioni riguardanti i documenti registrati;
- consente, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di "privacy", con particolare riferimento al trattamento dei dati sensibili e giudiziari;
- garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato;
- gestisce l'impronta dei file allegati: per ogni allegato ad un documento protocollato viene costruita un'impronta (una codifica hash) che viene memorizzata sul database e collegata al file stesso. La cosiddetta impronta del file permette in qualunque momento di sapere se qualcuno, diverso dal sistema documentale, aggiorni o inserisca allegati sul database senza passare dalla procedura applicativa. Questa attività di verifica vale per tutti gli allegati di un documento e degli eventuali documenti ad esso collegati.

Inoltre le risorse strumentali e le procedure utilizzate per la formazione dei documenti informatici garantiscono:
- l'identificabilità del soggetto che ha formato il documento e l'AOO di riferimento;
- una serie di controlli in fase di protocollazione che ne garantiscono l'integrità e la completezza;
- la sottoscrizione dei documenti informatici, quando prescritta, con firma digitale ai sensi delle vigenti norme tecniche;
- l'idoneità dei documenti ad essere gestiti mediante strumenti informatici e ad essere registrati mediante il protocollo informatico;
- l'accesso ai documenti informatici tramite sistemi informativi automatizzati;
- la leggibilità dei documenti nel tempo;
- l'interscambiabilità dei documenti all'interno della stessa AOO e con AOO diverse.

I moduli software di gestione della documentazione tecnica relativa alle opere pubbliche che

rientrano nella metodologia BIM dell'Ente (ACDat, file share, ecc), sono software sviluppati sul sistema documentale open source Alfresco, in particolare su una componente software modulare che fornisce un ambiente web riservato nel quale gli utenti dell'ente possono svolgere l'editing collaborativo su documenti, classificarli, condividerli, gestire flussi di processo che coinvolgano contenuti digitali di varia natura tra i quali i moduli applicativi specializzati per la gestione documentale per le opere pubbliche, secondo la metodologia progettuale BIM. La soluzione è certificata ACN e possiede i requisiti certificazione ISO 9001:2015, ISO 27017:2015, 27018:2019 e ISO 27001:2013.
Relativamente alla gestione dei documenti inoltre:

- consente di predisporre per ciascuna opera a patrimonio l'aggregazione dei fascicoli informatici nella quale organizzare i documenti informatici dell'opera;
- consente di implementare l' "ambiente di condivisione dei dati (ACDat) richiesto dalla normativa BIM per permettere ai Responsabili Unici di Progetto (RUP) di acquisire, verificare, approvare, condividere ed archiviare tutti i contenuti informatici relativi ad ogni fase progettuale di una opera e più in generale a tutto il ciclo di vita della stessa: il modulo è dotato di tutte le caratteristiche tecniche richieste dalla norma UNI 11337-1, ovvero rappresentare una infrastruttura informatica con condivisione regolamentata da precisi sistemi di sicurezza e tracciabilità (*Journal* per la registrazione automatica degli eventi e della fasi procedurali), successione storica delle operazioni, conservazione temporale, e identificazione delle responsabilità nell'elaborazione dei contenuti;
- permette il trattamento di tutti i documenti in conformità con le vigenti regole tecniche emanate da Agid in tema di documenti informatici;
- consente l'apposizione della 'marcatura' dei file per garantirne la repertazione;
- consentirà di implementare, mediante lo sviluppo di *API* attualmente in progettazione, un modello di interoperabilità con il sistema di protocollo e di gestione degli atti dell'Ente oltre che con il sistema di archiviazione documentale a norma (Parer) e con altre banche dati della pubblica amministrazione, con particolare riferimento al caricamento dei progetti strutturali su AINOP, così da garantire il principio del *once only* nella gestione dei dati relativi all'intero ciclo di vita delle opere pubbliche, anche ai fini del monitoraggio;
- rende disponibili strumenti di visualizzazione integrata dei formati tecnici (DXF. DWG, IFC).

La documentazione tecnica non rientrante nel perimetro BIM sopra descritto, quando non direttamente allegata a protocolli ed atti e quindi contenuta nei fascicoli amministrativi, viene conservata nel sistema di archiviazione connesso alla rete che permette di centralizzare e condividere file tra più utenti e dispositivi che garantisce funzionalità di backup automatico e ripristino veloce delle versioni precedenti dei file, oltre l'ordinario backup notturno dei dati.

COMPONENTE FISICA DELLA SICUREZZA

Il controllo degli accessi fisici ai datacenter di Lepida Scpa risponde ai requisiti minimi di sicurezza previsti per i datacenter pubblici essendo gli stessi qualificati come indicato in premessa, invece l'accesso alle risorse nella sala macchine dell'Ente è regolato secondo i seguenti principi:

- l'Ente è dotato di locali dedicati esclusivamente a ospitare i dispositivi di rete e la centrale telefonica Voip;
- l'accesso a tali locali è consentito soltanto al personale autorizzato realizzato con un sistema di controllo accessi, mediante il badge di servizio;
- visitatori occasionali, i dipendenti di aziende esterne e gli ospiti non possono entrare e trattenersi nell'area protetta se non accompagnati da personale dei sistemi informativi

dell'Ente.

Le procedure comportamentali nell'utilizzo della strumentazione da parte del personale, ai fini della protezione dei documenti sono meglio definite nel '*Disciplinare per utenti dei sistemi informativi della Provincia di Reggio Emilia*', sinteticamente si evidenzia che:

- le postazioni di lavoro, fisse e portatili, o gli strumenti comunque funzionalmente assimilabili, di proprietà dell'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. 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 dell'Ente, non deve pregiudicare il corretto adempimento della prestazione lavorativa, ostacolare le attività dell'Ente o essere destinato al perseguimento di interessi privati in contrasto con quelli pubblici. Gli utenti a cui sono affidate le postazioni di lavoro, sono soggetti a tutte le responsabilità dettate dalla normativa vigente e applicabile. Si sottolineano in particolare le seguenti responsabilità:
  - l'utente è responsabile per la protezione dei dati utilizzati e/o memorizzati nei sistemi in cui ha accesso;
  - l'utente è tenuto a segnalare immediatamente ai referenti informatici ogni sospetto di effrazione, incidente, abuso o violazione della sicurezza;
  - in caso di cessazione del rapporto di lavoro, l'utente deve restituire all'Ente qualsiasi risorsa informatica assegnata e mettere a disposizione ogni informazione di interesse istituzionale;
- l'utente è tenuto a bloccare o a spegnere il personal computer in caso di sospensione o di termine dell'attività lavorativa, assicurandosi di evitarne l'utilizzo improprio da parte di terzi, mediante inserimento di apposite credenziali di accesso. Le postazioni di lavoro o gli strumenti comunque funzionalmente assimilabili, messe a disposizione del personale, non devono essere lasciati incustoditi. Al termine dell'orario di servizio, i computer devono essere spenti prima di lasciare gli uffici. In caso di allontanamento temporaneo, l'utente deve attivare il salvaschermo con sblocco tramite password;
- le credenziali di accesso (generalmente, nome utente e password) sono strettamente personali e ogni attività non regolare effettuata e riconducibile alle stesse è imputata al titolare delle credenziali medesime.

MAPPATURA DI SINTESI DEI RISCHI

Minacce	Sintesi misure adottate
Terremoto	• i Datacenter di Lepida Scpa, o comunque quelli privati che ospitano soluzioni SaaS qualificate ACN, devono garantire di essere stati edificati secondo le norme antisismiche vigenti; • la sala macchine dell'Ente, che ospita gli apparati di rete è in un palazzo storico, che rispetta le norme antisismiche vigenti; • adozione della politica di sicurezza [1];
Inondazione	• il Datacenter di Lepida Scpa, o comunque quelli privati che ospitano soluzioni SaaS qualificate ACN, sono dotati di sistemi di rilevazione monitorati h24 da remoto; • la sala macchine dell'Ente, che ospita gli apparati di rete è sopraelevata rispetto al livello stradale;

	• adozione della politica di sicurezza [1];
Fulmine; *Interruzione di corrente*	• i Datacenter di Lepida Scpa, o comunque quelli privati che ospitano soluzioni SaaS qualificate ACN sono dotati di sistemi di rilevazione monitorati h24 da remoto, hanno linee elettriche ridondate e separate, ciascuna dotata di un sistema UPS e presentano gruppi elettrogeni che garantiscono il funzionamento per 24 ore; • la sala macchine dell'Ente, che ospita gli apparati di rete è dotata di impianto elettrico a norma, separato dall'impianto del resto dell'edificio; • adozione della politica di sicurezza [1];
Fuoco	• i Datacenter di Lepida Scpa, o comunque quelli privati che ospitano soluzioni SaaS qualificate ACN sono dotati di sistemi di rilevazione monitorati h24 da remoto, sono dotati di sistemi antincendio a norma; • la sala macchine dell'Ente, che ospita gli apparati di rete è dotata di impianto antincendio a norma e di sistema di rilevazione che attiva la chiamata ad una serie di numeri di cellulare di presidio; all'esterno della sala macchine, è presente un ulteriore impianto antincendio del palazzo; sono state redatte ed appese nella sala macchine, le note operative per l'intervento del personale in caso di incendio; • adozione della politica di sicurezza [1];
Danno volontario; *Furto;* *Accesso non autorizzato ai locali*	• i Datacenter di Lepida Scpa, o comunque quelli privati che ospitano soluzioni SaaS qualificate ACN sono dotati di sistemi di rilevazione dell'intrusione, oltre a presidi di vigilanza e controllo h24 e sistemi avanzati di controllo degli accessi; • la sala macchine dell'Ente, che ospita gli apparati di rete è dotata di grate alle finestre, videocamera interna visualizzabile da remoto; dotata di sistema di controllo accessi; • adozione della politica di sicurezza [1];
Interruzione di aria condizionata	• i Datacenter di Lepida Scpa, o comunque quelli privati che ospitano soluzioni SaaS qualificate ACN sono dotati di impianti di condizionamento e ridondanza con doppio circuito separato; ridondati anche i motori; • la sala macchine dell'Ente, che ospita gli apparati di rete è dotata di impianto di condizionamento ridondato;
Guasto hardware	• i Datacenter di Lepida Scpa, o comunque quelli privati che ospitano soluzioni SaaS qualificate ACN offrono servizi su hardware ridondato nei componenti principali (alimentatori, scheda di rete, dischi, ventole, ecc); tutti i sistemi sono virtualizzati e costruito per erogare servizi in alta affidabilità; • gli apparati di rete presso la sala macchine dell'Ente sono ridondati, salvo l'apparato di accesso alla rete Lepida; • sono attivi sistemi software di rilevamento guasti su tutta l'infrastruttura in IaaS e sugli apparati di rete; • adozione della politica di sicurezza [1];
Uso non autorizzato dei supporti di memoria	• dipendenti adottano misure di sicurezza per le postazioni assegnate, come da *Disciplinare dei Sistemi Informativi;* • gli uffici sono accessibili soltanto al personale autorizzato; • backup conservati presso i datacenter di Lepida;
Errore del personale operativo o errore di manutenzione	• adozione della politica di sicurezza [1], • revisione completa del cablaggio di rete;

Uso illegale di software	• le applicazioni sulle postazioni possono essere installate dai soli amministratori di sistema; • è presente un sistema di rilevazione dei software non autorizzati installati sui PC e relativa per la rimozione e/o blocco, come da *Disciplinare dei Sistemi Informativi;* • effettuata formazione agli utenti;
Software dannoso	• come da *Disciplinare dei Sistemi Informativi:* ◦ utilizzo di software per prevenire e rimuovere l'installazione di programmi dannosi; ◦ presenza di Antivirus centralizzato; ◦ utilizzo del firewall per il controllo e la restrizione della navigazione Internet ed IPS ispection;
Esportazione/ Importazione illegale di software	• effettuata formazione agli utenti, per responsabilizzarli ed indicazioni specifiche nel *Disciplinare dei Sistemi Informativi*; • misure elencate sopra di monitoraggio e controllo;
Accesso non autorizzato alla rete; *Uso della rete non autorizzato*	• presenza di una DMZ nella topologia della rete e di un reverse proxy per alcuni servizi WWW erogati; • presenza di un sistema di autenticazione e autorizzazione per l'accesso alle risorse condivise e controllo degli accessi alla navigazione Internet; • in fase di implementazione protezione mediante NAC; • adozione della politica di firewalling [2];
Guasto tecnico di provider di rete e danni sulle linee; Guasto dei servizi di comunicazione (rete, apparati)	• contratti di assistenza con i fornitori di connettività che coprono le esigenze di disponibilità del servizio; • connettività principale di rete ridondata su più vie; • presenza di linee di backup; • presenza di meccanismi di segnalazione in caso di guasto; • analisi del traffico di rete;
Sovraccarico di traffico	• adozione di politiche di QoS; • adeguato dimensionamento delle linee che forniscono connettività; • utilizzo di software deputati al monitoraggio degli apparati di rete e dei server della sala macchine;
Analisi del traffico: intercettazione e infiltrazione nelle comunicazioni	• sviluppo della rete interna secondo il principio delle switched network; • adozione della politica di firewalling [2];
Non corretta gestione dei messaggi (spam, ripudio, intercettazione, impersonificazione)	• adozione di strumenti di antispam e antivirus; • utilizzo di PEC e firma digitale;
Errore dell'utente o uso non corretto delle risorse	• presidio costante per l'assistenza agli utenti; • politiche di autorizzazioni minime degli utenti e controllo dei profili • revisione continua dei processi di assegnazione e revoca delle autorizzazioni; • adozione della politica di sicurezza [1];
Guasto software	• contratti di assistenza con i fornitori di applicativi che coprono le esigenze di disponibilità del servizio; • aggiornamento periodico dei sistemi operativi e dei software;

	• adozione della politica di sicurezza [1];
Uso non autorizzato di software da parte degli utenti	• si eseguono scansioni sui client per verificare la presenza di software particolarmente dannosi; • formazione agli utenti ed indicazioni presenti nel *Disciplinare dei Sistemi Informativi;*
Attacchi informatici (hacker, virus, dos)	• implementato un sistema antivirus centralizzato, distribuito su tutte le postazioni dell'Ente che consente di individuare e bloccare virus e malware in tempo reale; • il sistema di protezione controlla in tempo reale i dispositivi esterni alla postazione (chiavette USB, dischi esterni, etc); • sono stati predisposti dal personale dei sistemi informativi script di verifica automatica di rilevazione di eventuali virus in azione atti a crittografare i file (ransomware) o di eventuali attacchi per generare SPAM dai server di posta interno e di frontiera (dmz); • integrata la gestione e monitoraggio degli IoC come da linee guida nazionali;

[1] Politica di disaster recovery e backup/ripristino dei dati: l'Ente adotta una politica di backup frutto di un'analisi (Business Impact Analysis) effettuata sui servizi erogati e sulle tempistiche da garantire in termini di RTO (Recovery Time Objective = la durata accettabile di inattività di un'applicazione o di un sistema e di un processo prima che l'Ente subisca danni significativi; → tempo impiegato per ripristinare l'applicazione e i relativi dati per riprendere le normali attività dopo un problema significativo) e RPO (Recovery Point Objective = il calcolo della quantità di dati che è ragionevolmente accettabile perdere in caso di interruzione dell'attività prima che l'azienda subisca danni significativi, nel periodo fra un evento scatenante e l'ultimo backup dei dati), compatibilmente con le risorse economiche disponibili.
In generale sono presenti sistemi di backup dei dati/file e sistemi di backup delle macchine virtuali, ospitati su datacenter differenti da quelli in cui risiede l'infrastruttura di produzione e tra loro.

[2] Politica di firewalling: l'Ente è dotato di una serie di sistemi di sicurezza per la protezione dei propri sistemi, in particolare è presente un sistema virtualizzato di firewall di ultima generazione e una serie di ulteriori sistemi di controllo, rilevamento e segnalazione lungo il perimetro della rete dell'Ente. I sistemi sono stati integrati con liste di oggetti malevoli distribuiti dal CSIRT regionale, AgID e altre fonti esterne autorevoli, anche mediante il software open MISP (Malware Information Sharing Platform & Threat Sharing), che consentono di proteggere le postazioni anche quando operano in smart working.

COMPONENTE LOGICA DELLA SICUREZZA

La componente logica della sicurezza è ciò che garantisce i requisiti di integrità, riservatezza, disponibilità e non ripudio dei dati, delle informazioni e dei messaggi.
La modalità di gestione dell'accesso ai dati e ai documenti informatici, 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. Periodicamente, e

comunque almeno annualmente, è verificata la sussistenza delle condizioni per il mantenimento dei profili di autorizzazione per il sistema di gestione documentale.

L'architettura realizza una soluzione centralizzata per l'identificazione, l'autenticazione e l'autorizzazione (dominio Active Directory), del personale dell'Ente su cui si basa l'accesso alla rete e alle applicazioni principali (software gestionali, sistemi di gestione documentale, posta elettronica, ecc) che garantisce un unico sistema di repository delle credenziali di accesso degli utenti, protetto con misure minime di sicurezza, secondo la normativa vigente.

GESTIONE DELLE REGISTRAZIONI DI PROTOCOLLO E DI SICUREZZA

Le registrazioni di sicurezza sono costituite:

- dai log di sistema, generati dal sistema operativo;
- dai log dei dispositivi di protezione periferica del sistema informatico, (sensori di rete, firewall, ecc);
- dalle registrazioni degli applicativi, in particolare di gestione documentale, sopra descritti.

Le registrazioni di sicurezza sono soggette alle seguenti misure di sicurezza:

- l'accesso alle registrazioni è limitato, esclusivamente, agli amministratori di sistema dell'Ente a seconda delle tipologie di sistemi a cui sono abilitati (ad esempio ai log della posta accedono i soli amministratori di sistema della stessa);
- relativamente al software di protocollo dell'Ente, gli operatori dell'unità operativa responsabile della gestione documentale hanno un ruolo di amministratori del protocollo;
- le registrazioni sono elaborate tramite procedure automatiche;
- l'accesso dall'esterno da parte di persone non autorizzate non è consentito in base all'architettura stessa del servizio, essendo controllato dal sistema di autenticazione e di autorizzazione e dal firewall;
- l'operazione di scrittura delle registrazioni del protocollo, è effettuata direttamente dagli applicativi.

TRASMISSIONE E INTERSCAMBIO DEI DOCUMENTI INFORMATICI

Al fine di tutelare la riservatezza dei dati personali, i dati, i certificati ed i documenti trasmessi all'interno della AOO o ad altre AOO, contengono soltanto le informazioni relative a stati, fatti e qualità personali di cui è consentita la trasmissione e che sono strettamente necessarie per il perseguimento delle finalità per le quali vengono trasmesse.
Il server di posta certificata del fornitore esterno (provider) di cui si avvale l'AOO, qualificato secondo la vigente normativa nazionale ed europea, oltre alle funzioni di un server SMTP tradizionale, svolge anche le seguenti operazioni:

- accesso alla Certification Autority allo scopo di verificare l'integrità del messaggio e del suo contenuto;
- tracciamento e conservazione per diversi anni delle transazioni e delle ricevute, ma non del loro contenuto;
- gestione automatica delle ricevute di accettazione, consegna, anomalie. Tutte le ricevute sono firmate digitalmente dal gestore e danno garanzia del momento esatto in cui sono avvenute.