COMUNE DI SASSETTA

Politiche di Sicurezza

Misure Minime di Sicurezza – Infrastruttura Informatica - Cyber Security

Premessa

Lo scopo del presente documento è quello di descrivere i principi generali di sicurezza delle informazioni, che il Comune di Sassetta ha fatto propri al fine di realizzare e mantenere un efficiente e sicuro Sistema di Gestione della Sicurezza delle Informazioni.

Tali principi sono concretizzati nelle Policy per la sicurezza delle informazioni, la quale rispecchia le reali esigenze derivanti dalle attività svolte dal Comune di Sassetta .

La sicurezza delle informazioni ha come obiettivo primario la protezione dei dati e degli elementi del sistema informativo responsabile della loro gestione. In particolare, perseguire la sicurezza delle informazioni significa definire, conseguire e mantenere le seguenti proprietà delle stesse:

- riservatezza: assicurare che l'informazione sia accessibile solamente ai soggetti e/o ai processi debitamente autorizzati;
- integrità: salvaguardare la consistenza dell'informazione da modifiche non autorizzate;
- disponibilità: assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architetturali associati quando ne fanno richiesta;
- autenticità: garantire la provenienza dell'informazione;
- non ripudio: assicurare che l'informazione sia protetta da falsa negazione di ricezione, trasmissione, creazione, trasporto e consegna.

La mancanza di adeguati livelli di sicurezza, in termini di riservatezza, disponibilità, integrità, autenticità e non ripudio, può comportare, nell'ambito di una qualsiasi attività del Comune, il danneggiamento dell'immagine del Comune stesso, la mancata soddisfazione dei soggetti utenti, il rischio di incorrere in sanzioni legate alla violazione delle normative vigenti nonché danni di natura economica e finanziaria, il danno alla sfera della privacy dei soggetti coinvolti.

Il presente documento, nel rispetto delle norme vigenti:

- sottolinea l'importanza di garantire la sicurezza delle informazioni, dei dati e degli strumenti atti al trattamento degli stessi;
- è coerente con la volontà espressa dal Comune di garantire la protezione del patrimonio informativo;

- ha come oggetto aspetti fisici, logici ed organizzativi del Sistema di Gestione della Sicurezza delle Informazioni trattate digitalmente.

1 Perimetro organizzativo

La presente policy si applica a tutto il personale dipendente dal Comune e a tutti i soggetti che collaborano con il Comune, nell'ambito della gestione del sistema informativo. La policy si applica inoltre a tutti i processi e più in generale a tutte le risorse coinvolte nella gestione delle informazioni trattate digitalmente dal Comune.

2 Politiche di Sicurezza

2.1 Principi generali

I principi generali cui il Comune si ispira nella gestione della sicurezza delle informazioni sono articolati nelle seguenti aree:

- il rischio informatico e le misure minime
- Gestione della sicurezza fisica
- Identificazione, classificazione e gestione delle risorse
- Gestione sicura degli accessi logici ed accesso dati
- Norme comportamentali per la gestione sicura delle risorse comunali
- Personale e Sicurezza
- Aspetti contrattuali connessi alla sicurezza delle informazioni
- Gestione degli eventi anomali e degli incidenti
- Gestione della continuità operativa
- Politiche di cybersicurezza
- Monitoraggio, tracciamento e verifiche tecniche
- Ciclo di vita dei sistemi e dei servizi
- Rispetto della normativa

Di seguito, si riporta, per ciascuna tematica, l'obiettivo e le linee guida definite dal Comune

2.2 il rischio informatico e le misure minime

Il rischio informatico (o rischio ICT, Information & Communication Technology) è una particolare tipologia di rischio operativo che può comportare la perdita o sottrazione di dati digitali di vitale importanza per le PP.AA.LL.. Tale rischio è palesato in relazione all'utilizzo dell'Information & Communication Technology, dovuto ad eventi suscettibili di compromettere la disponibilità, l'integrità, l'accessibilità e la sicurezza di tali infrastrutture e dei dati. Nel rischio informatico è ricompreso anche il rischio di incorrere in eventi dannosi, quali interruzioni dell'operatività dei sistemi, accesso logico non autorizzato o la compromissione dell'integrità e/o danno alle informazioni, ovvero qualunque atto intenzionale e malevolo sul sistema informativo causato da parti interne, esterne o da terze parti in grado di pregiudicare la Riservatezza, l'Integrità e la Disponibilità delle informazioni e dell'infrastruttura tecnologica.

La Circolare AgID 1/2017, pubblicata in Gazzetta Ufficiale il 17.03.2017, con successivo adeguamento del 18.04.2017 nr. 2/2017, detta le indicazioni sulle misure minime di sicurezza ICT per le Pubbliche Amministrazioni, basata sulla "Direttiva del Presidente del Consiglio dei ministri del 1° agosto 2015", introducendo per le Pubbliche Amministrazioni, rientranti nella definizione ex. art. 1 c.2 d.Lgs. 165/2001, le misure minime di sicurezza del proprio Sistema Informatico.

Queste misure non sono superate o abrogate dal recepimento del regolamento EU 679/2016 (GDPR) con il dlgs 101 del 10 agosto 2018, pertanto rimangono parte integrante del più ampio disegno delle Regole Tecniche per la sicurezza informatica della Pubblica Amministrazione, seppur significativo sia l'impatto del GDPR sul concetto di misure di sicurezza. In estrema sintesi le Misure minime di sicurezza ICT per le pubbliche amministrazioni sono un vademecum ordinato e ragionato di "controlli" predisposto da AgID al fine di fornire alle pubbliche amministrazioni un elenco di azioni puntuali di natura tecnica od organizzativa che costituiscono un riferimento pratico per valutare e innalzare il livello della sicurezza informatica, per le quali

occorre andare oltre, introducendo un approccio basato sul rischio e non su elenco fisso. Si introduce il principio di **misura adeguata al rischio** tenendo conto dello stato dell'arte, dei costi di attuazione nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

Volendo prendere, comunque, le MMS come base di riferimento su cui tessere il proprio approccio alla sicurezza occorre tener di conto come il sistema informatico sia soggetto a continue evoluzioni e pertanto le misure espresse nelle MMS debbano essere sottoposte a successivi aggiornamenti. Con l'allegato al presente documento si provvede alla revisione delle versioni precedentemente approvate. Questo adempimento è propedeutico anche alla comunicazione all'ACN, in caso di eventuale incidente informatico (vedasi riferimento allegato "MMS").

Pur restando valido lo schema composto da schede riassuntive delle modalità di implementazione delle misure minime di sicurezza occorre menzionare le indicazioni dettate dai **piani triennali per l'informatica,** che in alcuni dei propri obiettivi pongono l'accento sul tema della cybesicurezza e per i quali si rimanda alla specifica documentazione e piani redatti dall'ente, nonché le "linee guida per il rafforzamento della protezione delle banche dati rispetto al rischio di utilizzo improprio" pubblicate da ACN, che rappresentano un documento di riferimento per contrastare il rischio di accessi abusivi, sia da parte di insider (insider threats) sia da minacce esterne. Tali documenti offrono un quadro completo delle misure normative esistenti, come quelle definite dal decreto-legge 105/2019 sul Perimetro di sicurezza nazionale cibernetica e della normativa più recente lg 90/2024 e dlgs 138/2024.

Le Misure Minime di Sicurezza si sviluppano su 3 livelli:

- "Minimo", al di sotto il quale nessuna amministrazione può scendere;
- "Standard", che costituisce la base di riferimento nella maggior parte dei casi;
- "Alto", che potrebbe essere un obiettivo a cui tendere pertanto l'ente dovrà adeguarsi almeno alle misure di livello minimo e tendere a rendere il sistema sicuro a seconda della propria situazione contingente.

Si rimanda all'allegato "allegato1_MMS" per la loro consultazione.

2.3 Gestione della sicurezza fisica

Obiettivo: prevenire l'accesso non autorizzato alle sedi ed ai singoli locali e garantire adeguati livelli di sicurezza alle aree e alle attrezzature mediante i quali vengono gestite le informazioni.

- Deve essere garantita la gestione della sicurezza delle aree e dei locali tramite: l'individuazione delle aree e la classificazione dei locali in base alla criticità delle informazioni elaborate; e la definizione dei livelli adeguati di protezione.
- Deve essere garantita la sicurezza delle apparecchiature tramite: la definizione di un'adeguata collocazione delle apparecchiature per l'elaborazione delle informazioni; la messa a disposizione delle risorse necessarie al loro funzionamento; la predisposizione di un adeguato livello di manutenzione.

Questo punto è già oggetto delle MMS e dei paragrafi precedenti

2.3.1 Infrastruttura Informatica Fisica

L'ente è strutturato su una sede centrale (palazzo comunale) e 2 sedi remote (Cimitero e Magazzino Comunale) tutte interconnesse tra loro, più un'altra sede a se stante ma di competenza: ufficio Turistico.

Sede comunale	Via Roma
Magazzino comunale	SP. 18A del Lodano
Cimitero comunale	Via di Castagneto – Piazza S. Rocco
Ufficio turistico	Via di Castagneto

L'infrastruttura (tranne l'ufficio turistico) è collegata ad internet con una connettività nell'ambito SPC ad alta

prestazione in virtù dell'adesione all'accordo quadro regionale RTRT4. L'infrastruttura (schemi allegati) si incentra su un collegamento ad alte prestazioni (1gb/s) ridondato e manutenuto con contratto di assistenza, installato nel centro stella individuato nel palazzo comunale e distribuito verso le sedi remote tramite una rete MPLS. Anche le sedi remote pur nell'ambito della MPLS sono dotate di connessioni ridondate. Questa architettura unita alla presenza di apparati firewall centralizzati, configurati con opportune politiche di traffico e di accesso garantiscono un soddisfacente grado di sicurezza. I firewall sono dotati di opportuni moduli di monitoraggio e controllo del traffico per rilevare attacchi e bloccare potenziali criticità. Anche il firewall del centro stella è ridondato. La strutturazione con MPLS permette un traffico sicuro tra tutte le sedi dell'ente e il palazzo comunale. A completamento della infrastruttura esiste una impianto fisico separato di ponti radio, per veicolare il flusso video delle telecamere distribuite sul territorio comunale.

La lan interna del palazzo comunale ha una dorsale in fibra ed un cablaggio strutturato in rame cat 6, ripartito in 5 armadi di piano. Le connettività e gli apparati di raccordo sono dislocati presso un apposita sala (sala server) ad accesso controllato tramite porta blindata, condizionata, dotata di una fornitura elettrica dedicata e delle necessarie luci di emergenza e dotazioni antincendio. L'accesso alla sala server è consentito soltanto al personale interno ed esterno se autorizzato per motivi di servizio. Ogni persona che accede alle risorse informatiche nella sala è identificato in modo certo.

Alla sala server è ricondotto il raccordo della lan e della connettività tutta, compresa quella dedicata alla telefonia. In essa gli apparati (server e apparati attivi) sono ridondati sia nell'hardware che nell'instradamento dei flussi dati, provvisti di UPS per preservarli da sbalzi di tensione elettrica e consentire una continuità operativa per il tempo necessario al loro eventuale necessario spengimento.

La Sala server ospita, oltre gli apparati dedicati alla lan interna anche quelli dei fornitori di connettività (Telecom in RTRT4) e servizio di telefonia in cloud (Telecom affidamento 2024 sino al 2027).

I sistemi informativi detengono una specifica documentazione per la gestione del complesso sistema informatico della cui struttura si allega un estratto nel documento "**allegato2_infrastruttura**"

2.4 Identificazione, classificazione e gestione delle risorse

Obiettivo: garantire la piena conoscenza delle informazioni gestite nel Comune e la valutazione della loro criticità, al fine di agevolare l'implementazione degli adeguati livelli di protezione, pertanto

- Deve esistere ed essere mantenuto aggiornato, nel corso del tempo un inventario i beni materiali ed immateriali da tutelare (informazioni, hardware, software, documentazioni cartacee e supporti di memorizzazione);
- Ogni risorsa (bene materiale/immateriale) deve essere direttamente associabile ad un responsabile. Le dotazioni dei sistemi centralizzati sono assegnate automaticamente al personale dei sistemi informativi che le supervisiona e manutiene
- Le informazioni devono essere classificate in base al loro livello di criticità, in modo da essere gestite con livelli di riservatezza ed integrità coerenti ed appropriati.

L'ente come già previsto dalle MMS provvede ad inventariare le proprie risorse attribuendone la responsabilità. Tale archivio è manutenuto digitalmente con i software OCS Inventory e Snipe IT: nell'**allegato 3 e 4** si propone una fotografia statica, aggiornata periodicamente, ma per una per avere informazioni più puntuali occorre interrogare direttamente i software di gestione.

Per l'infrastruttura fisico/logica della lan e dei servizi di interconnessione/comunicazione si rimanda all'**allegato2 e allegato5**.

2.4.1 Infrastruttura server e dei servizi

I servizi informatici sono erogati in duplice modalità cloud ed on premise. Quelli erogati in modalità SaaS, su piattaforme certificate ACN, sono:

1. erogazione del gestionale Jente distribuito dalla ditta Municipia SpA
2. servizi di telefonia fissa su piattaforma TIM
3. piattaforma web per l'esposizione del sito istituzionale e di Amministrazione Trasparente (OpenContent)
4. posta elettronica sulla piattaforma Microsoft Office365 Business

5. soluzione Bitdefender di Endpoint Protection Platform & Endpoint Detection and Response
6. SIT: sistema informativo territoriale gestito dalla dil LDP Progetti GIS

L'On Premise, gestito su due host ridondati ed una SAN, è stato strutturato con l'ambiente virtuale VMWare in cui sono state create delle VM ospitanti altrettanti server e servizi con SO Windows e Linux. Ad esso è demandato:

1. le gestione dei servizi prettamente di rete quali la gestione dell'AD, DNSe DHCP e quindi anche delle policy di accesso
2. il repository del file server
3. la gestione dei backup con il software di Veeam
4. software di inventario OCS
5. software snape IT
6. server qgis
7. server coda di stampa
8. server per la gestione degli accessi remoti
9. server per la gestione del ticketing della biblioteca
10. file server Polizia Municipale
11. Server dedicati alla videosorveglianza e lettura targhe

Per garantire l'integrità e la disponibilità del dato l'ente si è dotato, per quanto possibile di una ridondanza fisica e logica dei sistemi nonché di una policy dei backup mirata a garantire il ripristino del dato perso o corrotto.

I sistemi in cloud sono dotati di altrettanti servizi di sicurezza e politiche di ripristino del dato in caso di necessità.

Come per l'infrastruttura fisica si rimanda a specifica documentazione allegata: **Allegato5**

Nell'**allegato4** i software in uso sono stati categorizzati in

- quelli di produzione PC
- Sistemi operativi
- Sistemi di gestione SISTEMISTICA
- Software GESTIONALI

Gli uffici dell'ente fruiscono di stampanti condivise, fornite a noleggio, nel rispetto della razionalizzazione dell'uso e dei consumi.

2.5 Gestione sicura degli accessi logici ed accesso ai dati

Obiettivo: garantire l'accesso sicuro alle informazioni, in modo da prevenire trattamenti non autorizzati delle stesse o la loro visione da parte di utenti che non hanno i necessari diritti.

- L'accesso alle informazioni da parte di ogni utente deve essere limitato alle sole informazioni di cui necessita per lo svolgimento dei propri compiti.
- L'accesso alle informazioni in formato digitale da parte di utenti e sistemi autorizzati deve essere subordinata al superamento di una procedura di identificazione ed autenticazione degli stessi.
- Le autorizzazioni di accesso alle informazioni devono essere differenziate in base al ruolo ed agli incarichi ricoperti dai singoli individui e devono essere periodicamente sottoposte a revisione.
- E' necessario definire un processo di gestione delle credenziali di autorizzazione e dei relativi profili di accesso.
- I sistemi che costituiscono l'infrastruttura ICT devono essere opportunamente protetti e segretati, in modo da minimizzare la possibilità degli accessi non autorizzati.

I software gestionali, siano essi in cloud che on premise sono configurati opportunamente in modo da creare

profili nominativi con privilegi di accesso e operatività alle banche dati, definiti dai responsabili di settore.

Il controllo degli accessi al sistema per la gestione informatica è assicurato utilizzando le credenziali di autenticazione ed un sistema di autorizzazione basato sulla profilazione degli utenti in via preventiva.

La profilazione preventiva consente di definire le abilitazioni/autorizzazioni che possono essere effettuate/rilasciate ad un utente. Queste, in sintesi, sono le abilitazioni/autorizzazioni:

- consultazione;
- inserimento: effettuare una nuova registrazione;
- modifica: modificare i dati opzionali di una registrazione
- annullamento: annullare una registrazione

Il sistema per la gestione informatica di cui dispone il Comune consente il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente, o gruppi di utenti, assicura il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore. Tali registrazioni sono protette da modifiche non autorizzate.

Ciascun utente può accedere solamente ai dati che sono stati assegnati al suo servizio.

Le ACL di accesso sono impostate su più livelli: accesso di primo livello alla rete informatica ed alle sue risorse ed accesso alle banche dati di pertinenza tramite interfacce dei gestionali. Le profilazioni sono impostate in AD e sui singoli gestionali/piattaforme che permettono l'accesso alle proprie banche dati.

L'ente nell'esercizio delle sue funzioni tratta i dati di cui è titolare utilizzando software distribuito e manutenuto da di terze parti. Queste software house hanno necessità di accedere alle piattaforme ospitanti le banche dati elaborate dai loro software, pertanto sono stati stipulati apposite nomine di "responsabile esterno per il trattamento del dato". Tali nomine sono state sottoscritte anche per tutti coloro, che pur avendo ruoli esterni all'ente per i loro compiti istituzionali o tecnici possono utilizzare porzioni delle banche dati o averne la potenziale disponibilità. **Allegato6**: nomine responsabili esterni al trattamento dati.

2.5.1 protezione postazioni e profilazione di rete

L'ente ha n. 72 postazioni di lavoro dislocate presso le sedi di pertinenza, tutte con pc con SO windows11. Le postazioni di lavoro sono corredate di eventuali accessori quali lettori smart card e/o impronte digitali, webcam, monitor (**allegato3**).

Tutte le postazioni sono dotate di antivirus Bitdefender gestito e monitorato centralmente sul cloud.

L'accesso al pc è gestito in AD ed ogni utente è profilato affinché abbia accesso unicamente alle risorse necessarie per lo svolgimento del proprio lavoro.

L'account assegnato all'utente per l'accesso alla rete è costituito da un codice identificativo personale (username o user id) e da una parola chiave (password). La password che viene associata a ciascun utente è personale, non cedibile e non divulgabile.

Le password dovranno avere le seguenti caratteristiche:

- lunghezza minima 8 caratteri;
- caratteri di tipo alfanumerico e contenere almeno un numero, una lettera minuscola e una lettera maiuscola (non si possono usare simboli tipo ? / ! – _ ecc.);
- non deve essere riconducibile a: – nome o cognome proprio, non può essere uguale o riconducibile alla precedente o altri elementi che ne facilitino l'individuazione.

Le postazioni dell'ente sono dotate di autenticazione biometrica con lettura di impronta digitale.

L'utente non può installare software sulle postazioni di lavoro in maniera autonoma, ma ciò è demandato unicamente al personale dei sistemi informatici. A tal riguardo, l'ufficio dietro confronto con gli altri settori dell'ente ha stilato un **elenco di software autorizzati** (**allegato4**). La gestione del parco applicativo è sottoposta a:

- manutenzione dei sistemi
- controllo sul contenuto software dei client al fine di verificare l'assenza di codice malevolo sulle

postazioni di lavoro

- conformità a quanto autorizzato e previsto dalle licenze d'uso

L'utilizzo delle risorse di rete ha le seguenti regole:

- Le cartelle di rete sono aree di disco dello storage, gestito dal SO dei server, messo a disposizione dei vari Settori, Servizi o Uffici. Ogni Settore, Servizio o Ufficio avrà uno spazio la cui dimensione è limitata e determinata in funzione delle proprie esigenze, della disponibilità dell'intero sistema di memorizzazione, del numero di utenti, dei volumi e della tipologia di documenti trattati. I privilegi degli utenti sono determinati in funzione degli incarichi assunti e necessità lavorative, previo autorizzazione dei responsabili;
- le cartelle di rete sono periodicamente salvate con backup centralizzati. Le cartelle di rete sono aree di condivisione di documenti strettamente istituzionali e non possono essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia correlato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità;
- l'organizzazione e la gestione dell'albero delle sottocartelle è demandata al settore dei Sistemi Informatici;
- l'amministratore di sistema, suoi incaricati e la ditta affidataria del servizio di assistenza alle attrezzature informatiche (dietro autorizzazione), nel caso si prefiguri un uso improprio, o che metta a repentaglio la sicurezza del sistema informatico dell'Ente, delle cartelle di rete, ha la facoltà, di procedere alla rimozione di ogni file o applicazione, nonché di inibire temporaneamente l'accesso alle cartelle di rete interessate.

Gli uffici dell'ente fruiscono di stampanti condivise, fornite a noleggio, nel rispetto della razionalizzazione dell'uso e dei consumi.

2.6 Norme comportamentali per la gestione sicura delle risorse informatiche

Obiettivo: garantire che i dipendenti e i collaboratori del Comune adottino modelli di comportamento volti a garantire adeguati livelli di sicurezza delle informazioni.

- Gli ambienti di lavoro e le risorse dell'Amministrazione devono essere utilizzati in modo congruo con le finalità per le quali sono state rese disponibili e garantendo la sicurezza delle informazioni trattate.
- Devono essere definite delle procedure per la gestione ed utilizzo delle informazioni sia su supporto digitale che su supporto cartaceo.
- I sistemi informatici dell'Amministrazione devono essere impiegati da dipendenti e dai collaboratori secondo procedure formalmente definite.

Si faccia rifermento anche ai paragrafi precedenti nonché al "codice di comportamento" approvato con delibera di giunta n.245 del 17/10/2023 (art.17 - **allegato7**).

I principi generali espressi nel presente paragrafo fanno riferimento in particolare ai principali obblighi normativi disposti dal Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati ed a quanto disposto dal Codice dell'Amministrazione digitale (D.Lgs. 82/2005) e provvedimenti collegati.

2.7 Personale e sicurezza

La sicurezza è un obiettivo a cui tendere, integrando tra loro attività multidisciplinari ed ambiti distinti. Se da una parte occorre provvedere ad una infrastruttura fisica e logica adeguata altrettanto importante è garantire che il personale che opera per conto del Comune (dipendenti e collaboratori), abbia piena consapevolezza delle problematiche relative alla sicurezza delle informazioni.

- I dipendenti del Comune che operano nel sistema informativo devono ricevere un'adeguata formazione inerente le tematiche di sicurezza dei dati.

E' in corso la pianificazione di corsi base sui comportamenti essenziali per un comportamento corretto nell'uso delle tecnologie informatiche.

2.8 Aspetti contrattuali connessi alla sicurezza delle informazioni

Obiettivo: assicurare la conformità con i requisiti normativi e con i principi legati alla sicurezza delle informazioni

nei contratti con i fornitori.

- Gli accordi con i fornitori che accedono alle informazioni e/o agli strumenti che le elaborano, devono essere basati su contratti formali contenenti opportuni requisiti di sicurezza.
- Gli accordi con i fornitori ove necessario, devono garantire il rispetto dei requisiti di legge in materia di protezione dei dati personali.

I principi generali espressi nel presente paragrafo fanno riferimento in particolare alle principali richieste provenienti dal Codice in materia di tutela dei dati personali (D.Lgs 196/2003) disposti dal Regolamento (UE) 2016/679 ed a quanto previsto dal Codice dell'Amministrazione digitale (D.Lgs. 82/2005) e provvedimenti successivi ad essi collegati.

I contratti ICT si possono classificare in

- contratti di sviluppo, realizzazione e manutenzione evolutiva di applicazioni informatiche;
- contratti di acquisizione di prodotti (hardware o software);
- contratti per attività di operation e conduzione;
- contratti per servizi diversi da a) e c) (es. supporto, consulenza, formazione, help desk, …);
- contratti per forniture miste, combinazioni delle precedenti tipologie

vi sono tre tipi di azioni a) prima dell'acquisizione b) in corso di procedimento c) dopo la stipula

che si classificano come cogenti laddove la fornitura sia classificabile come critica.

Azioni a):

competenza in tema di sicurezza. Per Sassetta gli approvvigionamenti ICT sono fatti direttamente dal settore deputato secondo:

- raccolta buone prassi
- definire l'asset dei beni informatici (vedere misure minime)
- classificazione dei beni e servizi sotto il profilo della sicurezza
- audit e valutazione dei fornitori in maniera di sicurezza ed interna

Azioni b)

- classificare la fornitura in base a criteri di sicurezza per definire se abbia un impatto critico o meno
- scegliere lo strumento di acquisizione più adeguato

Tutti gli approvvigionamenti di natura informatica o, che ricadano in questa sfera di attività, sono eseguiti dal settore dei Sistemi Informativi ricorrendo alle centrali di committenza nazionali o regionali: Consip/Mepa e Start prediligendo le Convenzioni in essere o gli Accordi Quadro.

2.9 Gestione degli eventi anomali e degli incidenti

Obiettivo: garantire che le anomalie e gli incidenti aventi ripercussioni sul sistema informativo e sui livelli di sicurezza dell'Amministrazione siano tempestivamente riconosciuti e correttamente gestiti attraverso efficienti sistemi di prevenzione, comunicazione e reazione al fine di minimizzare l'impatto sul sistema.

- Tutti i dipendenti e i collaboratori sono tenuti a rilevare e notificare, a chi di competenza, eventuali problematiche legate alla sicurezza delle informazioni.
- Gli incidenti che possono avere un impatto sui livelli di sicurezza devono essere rilevati e gli eventuali danni, potenziali e non, devono essere gestiti, ove possibile, in tempi brevi secondo specifiche procedure.
- Deve essere realizzato un sistema di registrazione e classificazione degli incidenti e degli eventi anomali per effettuare analisi volte al miglioramento dei livelli di sicurezza coerentemente con le reali problematiche riscontrate. Si veda **allegato9.**

2.9.1 Processo di gestione degli incidenti informatici

Gli obiettivi sono:

- minimizzare l’impatto degli eventi malevoli;
- individuare ed attuare in maniera tempestiva idonee misure di contrasto/contenimento;
- individuare ed attuare tutte le attività di ripristino a seguito di un incidente;
- raccogliere dati per produrre statistiche in grado di alimentare il processo di analisi proattiva, finalizzato al rilevamento di eventi sospetti o di pattern comportamentali ripetuti nel tempo;
- attraverso i feedback ricevuti, aumentare all’interno della PA il grado di sensibilità verso le tematiche di sicurezza informatica e il livello di sicurezza delle infrastrutture tecnologiche gestite.

Gli eventi di sicurezza sono classificati in base alla seguente scala gerarchica di importanza:

- evento a basso impatto (non significativo): qualsiasi evento gestito in maniera silente dal sistema di sicurezza della PAL interessata e che non richiede un trattamento ad hoc. Solitamente viene utilizzato a fini statistici;
- evento significativo: qualsiasi evento rilevato nell’ambito dei sistemi e delle infrastrutture ICT, che deve essere analizzato dal personale incaricato delle attività di monitoraggio (quali ad esempio, il rilevamento in tempo reale delle segnalazioni provenienti dai dispositivi di sicurezza, l’analisi dei log prodotti da tali dispositivi, la raccolta e la valutazione di comunicazioni su comportamenti anomali o eventi sospetti) e gestione degli allarmi di sicurezza;
- evento critico: qualsiasi evento significativo che, a seguito delle analisi effettuate dal personale incaricato, potrebbe sottintendere, direttamente o indirettamente, una violazione delle politiche di sicurezza applicate ai sistemi ed alle infrastrutture ICT.

Tutti gli eventi constano di 4 fasi Rilevazione/monitoraggio, Analisi/classificazione, Gestione degli allarmi/incidenti, Ripristino. Si veda **allegato9, allegato11**

2.10 Gestione degli incidenti e della continuità operativa

La gestione della continuità operativa è un di cui della gestione degli incidenti per la quale rappresenta l’estrema ratio.

Si definisce “incidente di sicurezza” qualsiasi evento che comprometta o minacci di compromettere il corretto funzionamento dei sistemi e/o delle reti dell’organizzazione o l’integrità e/o la riservatezza delle informazioni in esse memorizzate od in transito, o che violi le politiche di sicurezza definite o le leggi in vigore.

L’ente classifica gli incidenti, definendone la codifica preventiva e la gestione degli stessi. Il processo di gestione degli incidenti è articolato nelle seguenti fasi:

- Rilevazione/identificazione/classificazione: sono riconosciuti uno o più eventi di sicurezza come incidente e a ogni incidente ne viene assegnato un livello di gravità. Il rilevamento avviene a valle delle segnalazioni provenienti da strumenti automatici o ancora da segnalazioni del personale dell’amministrazione;
- Contenimento: sono attuate le prime contromisure, allo scopo di minimizzare i danni causati dall'incidente. In genere si tratta di azioni temporanee e veloci, di cui effettuare il roll-back dopo la successiva fase di eliminazione;
- Eliminazione: sono eliminate le cause che hanno portato al verificarsi dell'incidente;
- Ripristino: sono effettuate le operazioni necessarie per riparare i danni causati dall'incidente e si effettua il roll-back delle contromisure di contenimento;
- Follow-up: è verificata l'adeguatezza delle procedure di gestione degli incidenti e vengono identificati i possibili punti di miglioramento.

Più in dettaglio, il modello generale che governa il processo di gestione degli incidenti deriva dalle migliori pratiche del framework ITIL secondo la seguente metodologia, suscettibile di miglioramenti ed ottimizzazioni in fase di esercizio in funzione di nuove tipologie di minacce nonché della disponibilità di nuove tecnologie e/o evoluzione di quelle presenti atte a contrastarle e mitigarle:

- analisi del contesto;
- ricezione richiesta/segnalazione da parte dell’utente interno all’Ente, oppure rilevazione non sollecitata

di una necessità a seguito di controlli periodici o segnalazioni automatiche real-time da strumento di monitoring;

- presa in carico della richiesta/segnalazione/necessità;
- analisi preliminare della richiesta/segnalazione/necessità al fine di limitare inefficienze e problemi per non corrette interpretazioni e/o falsi positivi;
- assegnazione all'intervento di un livello di priorità;
- assegnazione dell'intervento ad un tecnico interno/esterno in base a complessità. Gli interventi più complessi saranno affrontati in team;
- pianificazione dell'attività analizzando tutti i fattori ritenuti utili e/o critici (interdipendenze, sinergie tra risorse onsite e/o remote, tempistiche, leveraging esperienziale sulla base di attività analoghe pregresse e di best practice comprovate);
- preparazione dell'intervento attraverso l'analisi di quanto verificatosi in caso di incident/problem, identificazione degli ambiti e degli stakeholder anche esterni, monitoraggio degli SLA, effettuazione di backup delle configurazioni prima dell'intervento;
- attuazione di processi autorizzativi a vari livelli durante l'esecuzione delle attività in base alle classi di intervento concordate;
- esecuzione dell'intervento (in loco, o da remoto, etc.) con particolare attenzione alla definizione concordata dei tempi di intervento e minimizzazione dei tempi di disservizio, completezza, efficienza ed efficacia dell'intervento, comunicazione dell'avvenuta esecuzione agli stakeholder definiti in fase di pianificazione e altri rilevati nel corso dell'intervento, compilazione della documentazione di Knowledge Base quando necessario;
- esecuzione reiterata dell'intervento in caso di mancata risoluzione al primo tentativo con eventuale escalation verso fornitori esterni e/o l'eventuale supporto di figure tecniche specialistiche fino alla completa risoluzione;
- chiusura del case con comunicazione ai soggetti interessati

La gestione degli incidenti è quella di garantire la continuità dell'attività dell'Amministrazione e l'eventuale ripristino tempestivo dei servizi erogati colpiti da eventi anomali di una certa gravità, riducendo le conseguenze sia all'interno che all'esterno del contesto dell'Ente.

Deve essere predisposto un piano di continuità che permetta all'Amministrazione di affrontare, in modo organizzato ed efficiente, le conseguenze di un evento imprevisto garantendo il ripristino dei servizi critici in tempi e con modalità che consentano la riduzione delle conseguenze negative sul funzionamento e sull'erogazione dei servizi da parte dell'Amministrazione.

L'Ente ha redatto un documento in cui si danno indicazioni sugli scenari operativi di applicazione della continuità operativa: allegato10.

2.11 Politiche di cybersicurezza

Consci del fatto che un sistema immune da rischi al 100% non esista, l'obiettivo prefissatosi dell'ente è quello di rendere resiliente l'organizzazione rispetto ad attacchi ed incidenti di cybersicurezza. Nell'allegato12 dedicato a questo aspetto si descrive come l'ente abbia operato e quale struttura si sia dato.

2.12 Monitoraggio, tracciamento e verifiche tecniche

Obiettivo: garantire la rilevazione di eventi anomali, incidenti e vulnerabilità dei sistemi informativi al fine di assicurare la sicurezza e la disponibilità dei servizi e delle relative informazioni.

- I sistemi informativi devono essere periodicamente controllati in modo da valutare il corretto funzionamento dei sistemi di sicurezza, hardware e software implementati, nonché l'eventuale presenza di vulnerabilità non riscontrate o conosciute in passato.
- Sulla base dei I risultati di tutte le attività di monitoraggio, tracciamento e verifica devono essere effettuate periodiche attività di analisi, volte all'identificazione delle aree critiche e delle opportune azioni correttive e migliorative.

Tutti gli apparati predisposti ed utili alla connessione di rete alla elaborazione dati ed i sistemi software sono

acceduti con privilegi di amministratore dal personale dei sistemi informatici. Questi abilitano e danno il consenso ad eventuali tecnici esterni con i quali sono stati preventivamente sottoscritti accordi contrattuali e rispetto del GDPR

2.13 Ciclo di vita dei sistemi e dei servizi

Obiettivo è assicurare che gli aspetti di sicurezza siano inclusi in tutte le fasi di progettazione, sviluppo, esercizio, manutenzione, assistenza e dismissione dei sistemi e dei servizi informatici. I sistemi informativi provvedono ad un monitoraggio costante dei sistemi provvedendo alla sostituzione di apparati o software deprecati e provvedendo a tenere aggiornati i sistemi operativi in uso salvo necessità imposte da sistemi esterni non dismettibili

2.14 Rispetto della normativa

Obiettivo: garantire il rispetto delle disposizioni normative, di statuti, regolamenti e di ogni requisito inerente la sicurezza delle informazioni, riducendo al minimo il rischio di perdita e/o danneggiamento di dati, sanzioni legali o amministrative, danni reputazionali.

- Tutti i requisiti normativi e contrattuali in materia di sicurezza del sistema informativo e aventi impatto sul Sistema di Gestione della Sicurezza delle Informazioni devono essere identificati ed analizzati, al fine di valutarne gli impatti sull'organizzazione e sui sistemi informativi.
- I responsabili dei diversi settori devono assicurarsi, ciascuno nell'ambito di propria competenza, che tutte le politiche, le procedure, gli standard e in generale tutta la documentazione relativa alla sicurezza delle informazioni siano applicati e rispettati

3 Definizione dei ruoli e delle responsabilità

Il Comune secondo quanto dispone il comma 1 dell'articolo 17 del Codice dell'Amministrazione digitale (D.Lgs. 82/2005) ha nominato il Responsabile dell'Ufficio per la transizione alla modalità operativa digitale che ha fra i propri compiti "indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettività, nel rispetto delle regole tecniche".

Alcuni degli allegati richiamati sono in parte riservati perché contenti informazioni tecniche oggetto di cybersicurezza pertanto si riporta il relativo atti di approvazione

Allegati: allegato1_MMS 2026 allegato2_infrastruttura allegato3_elenco pc allegato4_software autorizzati e servizi allegato5_server-vm-banche dati allegato6_elenco nomine trattamento dati allegato7_art17 allegato8_ servizi cloud allegato9_incidenti informatici allegato10_continuità operativa allegato11_backup allegato12_cybersecurity	Determina del responsabile del settore Sistemi Informativi n.2026/464 del 30/04/2026

mentre si allega il "Regolamento per l'uso della strumentazione e servizi ICT" approvato con delibera di Giunta n. 2026/126 del 28/04/2026