PIANO DI SICUREZZA INFORMATICA

UNIONE DI COMUNI MONTANA AMIATA GROSSETANA	MANUALE GESTIONE PROTOCOLLO **ALLEGATO 2** **PIANO DI SICUREZZA INFORMATICA**	

Premessa

Il presente piano di sicurezza informatica è definito ai sensi dell'articolo 4 comma 3 lettera c del DPCM 3 dicembre 2013 recante le regole tecniche di protocollo.

Il presente piano di sicurezza è pienamente conforme a quanto previsto dal "Disciplinare tecnico in materia di misure minime di sicurezza" Allegato B al D.Lgs. 196/2003 Codice in materia di protezione dei dati personali.
Alla data di approvazione del Manuale non sono state emanate le regole tecniche di cui al comma 1 dell'articolo 51 del D.Lgs. 82/2005, come modificato dal D.Lgs. 179/2006, con le quali saranno individuate "le modalità che garantiscono l'esattezza, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati, dei sistemi e delle infrastrutture ". Quando tali regole tecniche entreranno in vigore il presente piano, se necessario, dovrà essere opportunamente adeguato.

Nella Gazzetta ufficiale del 5 maggio 2017 è stata pubblicata la circolare dell'Agenzia per l'Italia Digitale (AgID) n° 2 del 18 aprile 2017, recante le "Misure minime di sicurezza ICT per le pubbliche amministrazioni", in attuazione della Direttiva del Presidente del consiglio dei ministri 1° agosto 2015. Il documento che fa parte integrante delle Linee guida per la sicurezza ICT nelle PPAA costituisce una "anticipazione urgente della regolamentazione in corso di emanazione " per fornire un riferimento utile a stabilire un livello di protezione …..
Il presente piano di sicurezza è allineato ai controlli ABSC previsti dalle "Misure minime" secondo il livello minimo di applicazione "livello sotto il quale nessuna amministrazione può scendere " (controlli obbligatori).

1 Obbiettivi del piano di sicurezza

Il presente documento riporta le misure di sicurezza adottate per la formazione, la gestione, la trasmissione, l'interscambio, l'accesso e la conservazione dei documenti informatici e delle aggregazioni informatiche, anche in relazione alle norme sulla protezione dei dati personali.

Il piano di sicurezza garantisce che:

- i documenti e le informazioni trattate dal sistema per la gestione informatica dei documentisono disponibili, integre e riservate;
- i dati personali comuni, sensibili 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.

2 Generalità

Il piano di sicurezza:

- si articola in due componenti: una di competenza del responsabile del servizio informatico (responsabile del sistema informativo) una di competenza del responsabile della gestione documentale (RGD);
- si basa sui risultati dell'analisi dei rischi a cui sono esposti i dati e i documenti trattati,
- si fonda sulle direttive strategiche di sicurezza stabilite dall'Amministrazione (Politiche di sicurezza);
- definisce:
- le modalità di accesso al sistema per la gestione informatica dei documenti e al Programma Informatico di protocollo (PIP)

✓ gli aspetti operativi della sicurezza, con particolare riferimento alle "Misure minime di sicurezza ICT per le pubbliche amministrazioni"circolare AgID n° 2/2017 e alle misure minime di sicurezza, di cui al Disciplinare tecnico

richiamato nell'allegato B) del D.lgs. 196/2003 - Codice in materia di protezione dei dati personali;
- ✓ i piani di formazione degli addetti;
- ✓ le modalità esecutive del monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza.

Il piano è soggetto a revisione formale con cadenza periodica e può essere modificato a seguito di eventi gravi.
I dati personali registrati nel log del sistema operativo, del sistema di controllo degli accessi e delle operazioni svolte con il sistema per la gestione informatica dei documenti, saranno conservati dal responsabile del sistema informativo secondo le vigenti norme e saranno consultati solo in caso di necessità

3 Formazione dei documenti informatici: aspetti attinenti la sicurezza

Le risorse strumentali e le procedure utilizzate per la formazione dei documenti informatici garantiscono:
- l'identificabilità del soggetto che ha formato il documento e il servizio di riferimento;
- 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 dell'Amministrazione e con le altre PA.

I documenti informatici sono formati dall'Amministrazione secondo quanto previsto dal capitolo 2 del MdG .
Per attribuire in modo certo la titolarità del documento, la sua integrità e, se del caso, la riservatezza, il documento è sottoscritto con firma digitale.
Per attribuire una data certa a un documento informatico prodotto all'interno della AOO, si applicano le regole per la validazione temporale e per la protezione dei documenti informatici previste dalla normativa vigente.

4 Gestione dei documenti informatici

Il **sistema operativo** delle risorse elaborative del sistema per la gestione informatica dei documenti è conforme alle specifiche previste dalla normativa vigente.
Il sistema operativo del server che ospita i file utilizzati come deposito dei documenti è configurato in maniera da consentire:
- l'accesso esclusivamente al server del PIP in modo che qualsiasi altro utente non autorizzato non possa mai accedere ai documenti al di fuori del sistema di gestione documentale;
- la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantire l'identificabilità dell'utente stesso. Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.

.
Il sistema per la gestione informatica dei documenti
- garantisce la disponibilità, la riservatezza e l'integrità dei documenti, del registro di protocollo e degli altri registri particolari;
- assicura la corretta e puntuale registrazione di protocollo dei documenti in entrata ed in uscita;

- 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.

5 Componente organizzativa della sicurezza

Nella conduzione del sistema di sicurezza, dal punto di vista organizzativo, sono state individuate le seguenti funzioni specifiche:

- ✓ sicurezza informatica si occupa principalmente della definizione dei piani di sicurezza e della progettazione dei sistemi di sicurezza;
- ✓ sicurezza operativa ha il compito di realizzare, gestire e mantenere in efficienza le misure di sicurezza così da soddisfare le linee strategiche di indirizzo definite dalla funzione sicurezza informatica;
- ✓ revisione ha il compito di controllare le misure di sicurezza adottate, verificandone l'efficacia e la coerenza con le politiche di sicurezza.

Nell'Unione le tre funzioni sono affidate al responsabile dei sistemi informativi (responsabile del sistema informativo) che si coordina, per gli aspetti di loro competenza con il responsabile della gestione documentale, il responsabile della conservazione dei documenti informatici ed il responsabile del trattamento dei dati personali.
Il responsabile del sistema informativo nella definizione del piano di sicurezza e nella progettazione dei sistemi di sicurezza potrà avvalersi del responsabile del sistema informativo, ove necessario, di soggetti dotati delle necessarie competenze tecniche interni o esterni all'amministrazione.
Il responsabile del sistema informativo per la realizzazione di quanto attiene alla sicurezza operativa potrà avvalersi del responsabile del sistema informativo dei servizi specialistici dei fornitori di hardware e software dell'amministrazione o di altri soggetti interni o esterni qualificati.

6 Componente fisica della sicurezza

La componente fisica della sicurezza riguarda, data la struttura del sistema informatico dell'Unione, l'accesso alla sala macchine nella quale sono collocate le risorse elaborative.
Il controllo degli accessi fisici alla sala macchine è regolato secondo i seguenti principi:

- l'accesso è consentito soltanto al personale, interno ed esterno, autorizzato per motivi di servizio;
- i visitatori occasionali, i dipendenti di aziende esterne e gli ospiti devono esplicare la procedura di registrazione; essi non possono entrare e trattenersi se non accompagnati da personale dell'Unione autorizzato;
- ogni persona che accede alle risorse informatiche nella sala macchine è identificata in modo certo.
- gli accessi alla sede sono registrati e conservati ai fini della imputabilità delle azioni conseguenti ad accessi non autorizzati;

Il controllo degli accessi fisici alle risorse della sala macchine è regolato secondo i principi stabiliti dal responsabile del sistema informativo.

7 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.

Tale componente, nell'ambito del sistema per la gestione informatica dei documenti, è stata realizzata attraverso l'attivazione dei seguenti servizi di sicurezza che prevengono l'effetto "dannoso" delle minacce sulle vulnerabilità del sistema informatico:

- identificazione, autenticazione ed autorizzazione degli utenti;
- riservatezza dei dati;
- integrità dei dati;
- integrità del flusso dei messaggi;
- non ripudio dell'origine (da parte del mittente);
- non ripudio della ricezione (da parte del destinatario);
- audit di sicurezza;

8 Componente infrastrutturale della sicurezza

Il locale che ospita la parte centrale del sistema informatico (sala macchine) deve essere dotata delle necessarie infrastrutture di sicurezza:

- protezione degli accessi (porte e finestre accessibili) con adeguate strutture,
- impianto antincendio;
- impianto di condizionamento;•
- luci di emergenza;
- apparato per la continuità elettrica.

9 Gestione delle registrazioni di protocollo e di sicurezza

Le registrazioni di sicurezza sono costituite da informazioni di qualsiasi tipo, presenti o transitate sul PIP che occorre mantenere, sia dal punto di vista regolamentare, sia in caso di controversie responsabile del sistema informativo e legali che abbiano ad oggetto le operazioni effettuate sul PiP, sia al fine di analizzare compiutamente le cause di eventuali incidenti di sicurezza.

Le registrazioni di sicurezza sono formate:

- dai log di sistema, generati dal sistema operativo,
- dai log dei dispositivi di protezione periferica del sistema informatico (intrusion detection system-IDS, sensori di rete e firewall),
- dalle registrazioni dell'applicativo PIP

Le registrazioni di sicurezza devono essere effettuate tramite una specifica procedura.

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

- l'accesso alle registrazioni è limitato, esclusivamente, agli amministratori di sistema agli operatori di sicurezza addetti al servizio di protocollo, come previsto dalle norme sul trattamento dei dati personali;
- le registrazioni del PIP sono elaborate tramite procedure automatiche da parte degli operatori di sicurezza;
- l'accesso dall'esterno da parte di persone non autorizzate non è consentito essendo controllato dal sistema di autenticazione e di autorizzazione e dal firewall

;
I supporti con le registrazioni di sicurezza sono conservati all'interno di un idoneo contenitore (esempio armadio blindato ignifugo) in un locale diverso dalla sala macchine

10 Trasmissione e interscambio di documenti informatici

Gli addetti dell'Unione alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi, a qualsiasi titolo,

informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni che, per loro natura o per espressa indicazione del mittente, sono destinate ad essere rese pubbliche.
Come previsto dalla normativa vigente, i dati e i documenti trasmessi per via telematica sono di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario.
Al fine di tutelare la riservatezza dei dati personali, i dati, i certificati ed i documenti trasmessi contengono soltanto le informazioni relative a stati, fatti e qualità personali di cui è consentita la diffusione e che sono strettamente necessarie per il perseguimento delle finalità per le quali vengono trasmesse.

11 Accesso ai documenti informatici

Il controllo degli accessi al sistema per la gestione informatica dei documenti 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 del servizio di protocollo e gestione documentale. Queste, in sintesi, sono le abilitazioni/autorizzazioni:

- consultazione visualizzare in modo selettivo registrazioni già presenti nel PIP;
- inserimento effettuare una nuova registrazione di protocollo e associare i documenti;
- modifica modificare i dati opzionali di una registrazione
- annullamento annullare una registrazione di protocollo, può essere autorizzata solo dal RGD.

Il sistema per la gestione informatica dei documentidi cui dispone l'Unione 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.
Ad ogni documento, all'atto della registrazione nel sistema di protocollo informatico, viene associata una Access Control List (ACL) che consente di stabilire quali utenti, o gruppi di utenti, hanno accesso ad esso (sistema di autorizzazione o profilazione utenza).
Ciascun utente può accedere solamente ai documenti che sono stati assegnati al suo servizio.
I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell'archivio o di una ricerca full text.

UTENTI INTERNI
I livelli di abilitazione/autorizzazione alle funzioni del sistema per la gestione informatica dei documenti sono disposti dai RDS per il proprio ambito di competenza.
I livelli di abilitazione/autorizzazione alle funzioni del PIP sono disposti dai RGD.

La gestione delle abilitazioni/autorizzazioni è realizzata dal sistema in modo che gli utenti creati non sono mai cancellati ma, eventualmente, disabilitati.

12 Conservazione di documenti informatici
Gli aspetti di sicurezza relativi al sistema di conservazione dei documenti informatici saranno trattati nel "Manuale di conservazione di cui all'articolo 8 del DPCM 3 dicembre 2013 "Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005".

13 Politiche di sicurezza

Le politiche di sicurezza, riportate nell'allegato 3, stabiliscono, sia le misure preventive per la tutela e l'accesso al patrimonio informativo, sia le misure correttive per la gestione degli incidenti informatici.
È compito del responsabile del sistema informativo e del responsabile della tutela dei dati personali procedere al perfezionamento, alla divulgazione, al riesame e alla verifica delle politiche di sicurezza.
Il riesame delle politiche di sicurezza è conseguente al verificaresponsabile del sistema informativo di incidenti attinenti alla sicurezza, di variazioni tecnologiche significative, di modifiche all'architettura di sicurezza che potrebbero incidere sulla capacità di mantenere gli obiettivi di sicurezza o portare alla modifica del livello di sicurezza complessivo, ad aggiornamenti delle prescrizioni minime di sicurezza o a seguito dei risultati delle attività di audit
.
In ogni caso, tale attività è svolta almeno con cadenza annuale

14 Misure minime di sicurezza AgID 2016

Integrazione del piano con quanto previsto dalla circolare AgID 1/2017 "Misure minime per la sicurezza ICT nelle pubbliche amministrazioni – aprile 2016", si fa riferimento ai controlli AgID Basic Security Control(s) (ABSC) secondo il livello minimo di applicazione "livello sotto il quale nessuna amministrazione può scendere " (controlli obbligatori).
I controlli che seguono in parte sono riconducibili a quelli già previsti nei paragrafi precedenti, altri sono introdotti ex novo

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

1.1.1	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4
1.3.1	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.
1.4.1	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.

ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

2.1.1	Stilare un elenco di software autorizzati e relative veresponsabile del sistema informativooni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diveresponsabile del sistema informativo usi. Non consentire l'istallazione di software non compreso nell'elenco.
2.3.1	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato

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

3.1.1	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.

3.2.1	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di si-stemi usati dall'organizzazione.
3.2.2	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.
3.3.1	Le immagini d'installazione devono essere memorizzate offline.
3.4.1	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).

ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

4.1.1	Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.
4.4.1	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.
4.5.1	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni
4.5.2	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air -gapped, adottando misure adeguate al loro livello di criticità.
4.7.1	Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.
4.8.1	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.).
4.8.2	Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche

ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

5.1.1	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.
5.1.2	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.
5.2.1	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia

	debitamente e formalmente autorizzata
5.3.1	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.
5.7.1	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).
5.7.3	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).
5.7.4	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).
5.10.1	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.
5.10.2	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconduci-bili ad una sola persona.
5.10.3	Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.
5.11.1	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.
5.11.2	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

8.1.1	Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.
8.1.2	Installare su tutti i dispositivi firewall ed IPS personali.
8.3.1	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.
8.7.1	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.
8.7.2	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.

8.7.3	Disattivare l'apertura automatica dei messaggi di posta elettronica.
8.7.4	Disattivare l'anteprima automatica dei contenuti dei file.
8.8.1	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione
8.9.1	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destina-tario, prevedendo anche l'impiego di strumenti antispam.
8.9.2	Filtrare il contenuto del traffico web.
8.9.3	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).

ABSC 10 (CSC 10): COPIE DI SICUREZZA

10.1.1	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni stretta-mente necessarie per il completo ripristino del sistema.
10.3.1	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.
10.4.1	Assicuraresponsabile del sistema informativo che i supporti contenenti almeno una delle copie non siano permanentemente ac-cessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

13.1.1	Effettuare analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli cui va applicata la protezione crittografica.
10.3.1	Bloccare il traffico verso url presenti in una black list.

15 Revisione e controllo

Il responsabile del sistema informativo dispone la tenuta e l'aggiornamento del registro dei guasti e del malfunzionamenti del sistema informatico; nel quale vengono annotati gli eventi riguardanti la sicurezza informatica.
Nel registro vengono riportate:

- la data e l'ora della [eventuale] segnalazione di guasto o malfunzionamento e la sintetica descrizione dell'evento di sicurezza;

- la descrizione dell'intervento effettuato per contenere e/o risolvere l'evento di sicurezza;
- la data e l'ora della soluzione dell'evento di sicurezza.

Il responsabile del sistema informativo almeno una volta all'anno pianifica e realizza una attività di controllo delle misure di sicurezza oggetto del presente Piano, attraverso:

a) l'esame del registro dei guasti e malfunzionamenti;
b) l'individuazione di specifiche misure di sicurezza che devono essere verificate e le modalità di verifica delle stesse;
c) la verifica delle misure di sicurezza di cui al punto precedente.

L'esito dell'attività di verifica deve essere verbalizzato e sottoscritto dal responsabile del sistema informativo.
A seguito dell'esito delle attività di controllo o del verifica responsabile del sistema informativo di rilevanti eventi di sicurezza il responsabile del sistema informativo può proporre la revisione del Piano,