



**Manuale per la gestione del protocollo informatico,
dei flussi documentali e degli archivi
del Comune di Nuvolera**

Allegato n. 9

Piano di sicurezza informatica

PIANO DI SICUREZZA INFORMATICA

Gestione dei documenti informatici

Il sistema operativo delle risorse elaborative destinate ad erogare il servizio di protocollo informatico è conforme alle specifiche previste dalla normativa vigente. Il sistema operativo (Linux) del server che ospita i file utilizzati come deposito dei documenti è configurato in maniera da consentire:

- l'accesso esclusivamente al server del protocollo informatico, 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 (logging applicativo). I log di accesso ai sistemi sono conservati in maniera tale da garantire l'integrità degli stessi e conservati per un periodo di tempo di almeno 6 mesi, in compatibilità con le prescrizioni del Garante Privacy in tema di amministratori di sistema.

Il sistema di gestione informatica dei documenti:

- 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;
- 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 dell'archivio adottato.

Componente organizzativa della sicurezza

La componente organizzativa della sicurezza legata alla gestione del protocollo e della documentazione si riferisce principalmente alle attività svolte per l'erogazione del SdP. Nella conduzione del sistema di sicurezza, destinato ad erogare il SdP, le qualifiche funzionali individuate sono le seguenti:

- responsabile ICT;
- responsabile della sicurezza;
- responsabile della tutela dei dati personali;
- operatori di sicurezza sistemi.

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 (sistemi di monitoraggio applicato alle normative sulla sicurezza informatica).

Relativamente alla componente fisica della sicurezza sono stati definiti i seguenti ruoli:

- responsabile della sicurezza;
- responsabile SECOVAL;
- operatori della sicurezza.

Componente fisica della sicurezza

La politica della sicurezza identifica i comportamenti che regolano l'accesso fisico a luoghi in cui sono conservati o custoditi dati personali o sensibili. A tale proposito si può identificare una classificazione degli stessi in:

- ❖ Aree ad accesso non controllato
- ❖ Aree ad accesso controllato
- ❖ Aree ad accesso ristretto

Per ognuna di queste sono state definite delle modalità di gestione degli accessi e delle regole per quanto riguarda l'installazione delle apparecchiature.

Sede Principale

Indirizzo

Video sorveglianza

Allarme antintrusione

Inferriate alle porte o finestre

Vigilanza notturna

Antincendio

Accesso all'edificio (descrizione)

Accesso all'edificio (descrizione)

Distribuzione chiavi registrata

Sede Comunità Montana di Valle Sabbia

Via Gen. Reverberi 2

Esterna sul perimetro dell'edificio

Si collegato a società di vigilanza

No

Si

Estintori - impianto rilevazione incendi con allarme

sonoro in archivio

N° 2 accessi pubblico con porte a vetri attive in orari

di ufficio

Porta ingresso dei dipendenti con badge

Tutti i dipendenti

Sala Server

Accesso

Distribuzione chiavi

Registro interventi

Allarme accesso

Regole Sicurezza

Porta con serratura meccanica ed elettronica

Responsabile sistema informativo e

Operatori Ufficio ICT

In attivazione

Allarme dell'edificio della Comunità Montana

Antincendio

Estintori mantenuti da ditta
specializzata

Impian

A norma

Aria condizionata per raffreddamento de
apparecchiature

Installazione sistemi UPS

Regole di accesso alla SALA SERVER

Di seguito sono sinteticamente riportati i criteri tecnici ed organizzativi per la protezione delle aree e dei locali interessati alle misure di sicurezza, nonché le procedure per controllare l'accesso delle persone autorizzate ai locali medesimi. Le misure riguardano la sala server della Comunità Montana accessibile attraverso una porta dotata di sistema di apertura elettronica tramite badge, in dotazione agli operatori dell'Ufficio ICT.

Una copia delle chiavi di apertura meccanica è custodita dal Responsabile ICT nel caso si debba accedere alla stanza per motivi di emergenza in orari di chiusura degli uffici o in assenza di energia elettrica.

Accesso da parte del personale esterno

Il personale non dipendente che deve accedere all'edificio per la manutenzione degli apparati, degli applicativi software o degli impianti, deve essere autorizzato ed accompagnato dagli operatori dell'Ufficio ICT.

Quando delle persone entrano nella Sala server il loro operato è supervisionato da un collaboratore dell'ufficio informatico, che si preoccupa anche di impartire indicazioni inerenti le regole di accesso ai locali.

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 SdP, è stata realizzata attraverso:

- l'attivazione dei seguenti servizi di sicurezza che prevengono l'effetto "dannoso" delle minacce sulle vulnerabilità del sistema informatico:
 - o identificazione, autenticazione ed autorizzazione degli operatori dell'erogatore del SdP;
 - o riservatezza dei dati;
 - o integrità dei dati;
 - o integrità del flusso dei messaggi;
 - o non ripudio dell'origine (da parte del mittente);
 - o non ripudio della ricezione (da parte del destinatario);
- backup dei sistemi di esercizio.

In base alle esigenze rilevate dall'analisi delle minacce e delle vulnerabilità, è stata implementata una infrastruttura tecnologica di sicurezza con una architettura "a strati multipli di sicurezza" conforme alle best practices correnti.

L'architettura realizza una soluzione centralizzata per l'identificazione, l'autenticazione e l'autorizzazione degli addetti delle AOO e degli operatori dell'erogatore del SdP, con le seguenti caratteristiche:

- server per la gestione dei diritti di accesso ai servizi applicativi;
- unico sistema di repository delle credenziali di accesso degli utenti;
- unico database delle anagrafiche contenente tutti i profili di utenza.

Componente infrastrutturale della sicurezza

Presso la Server Farm dell'erogatore sono disponibili i seguenti impianti:

- estintori antincendio;
- luci di emergenza;
- continuità elettrica;
- controllo degli accessi e dei varchi fisici.

Essendo la server farm, lontana da insediamenti industriali e posta all'interno di un edificio adibito ad uffici, le sue condizioni ambientali per quanto riguarda polvere, temperatura, umidità, vibrazioni meccaniche, interferenze elettriche e radiazioni elettromagnetiche e livelli di inquinamento chimico e biologico, sono tali da non richiedere misure specifiche di prevenzione oltre quelle già adottate per le sedi di uffici di civile impiego.

Gestione delle registrazioni di protocollo e di sicurezza Le registrazioni di sicurezza sono costituite da informazioni di qualsiasi tipo (ad esempio: dati, transazioni), presenti o transitate sul SdP che occorre mantenere, sia dal punto di vista regolamentare, sia in caso di controversie legali, che abbiano ad oggetto le operazioni effettuate sul SdP, sia al fine di analizzare compiutamente le cause di eventuali incidenti di sicurezza.

Ogni registrazione di protocollo viene memorizzata dal Sistema di Gestione Informatica dei Documenti,

unitamente all'identificativo univoco dell'autore che l'ha eseguita e alla data e all'ora della stessa. Eventuali modifiche vengono registrate per mezzo di log di sistema che mantengano traccia dell'autore, della modifica effettuata, nonché della data e dell'ora.

Il Sistema mantiene leggibile la precedente versione dei dati di protocollo, permettendo, in tal modo, la completa ricostruzione cronologica di ogni registrazione. Il Sistema non consente la modifica del numero e della data di protocollo.

Le registrazioni di sicurezza sono costituite:

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

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

- l'accesso alle registrazioni è limitato, esclusivamente, ai sistemisti o agli operatori di sicurezza addetti al servizio di protocollo, come previsto dalle norme sul trattamento dei dati personali;
- i log di sistema sono accessibili ai sistemisti in sola lettura al fine di impedirne la modifica;

Il sistema dell'SdP è ospitato all'interno del DATACENTER di Comunità Montana di Valle Sabbia, strutturato

secondo le specifiche elencate nella scheda tecnica descrittiva allegata al presente piano di sicurezza.

Server e risorse elaborative

Il datacenter ospitato nella Server Farm di Comunità Montana di Valle Sabbia, si compone di una serie di server ed apparati di rete.

L'infrastruttura è composta da tre cluster ed ogni cluster è composto da tre host fisici. Tutti i server sono server virtuali gestiti dall'hypervisor VMWare.

I sistemi operativi installati sui server sono Microsoft Windows Server 2012 e 2016 e diverse

distribuzioniLinux.

Networking

Di seguito viene descritta l'infrastruttura di rete del datacenter.

L'Accesso alla rete internet è gestito dal provider Intred tramite un collegamento in fibra. Il datacenter è dotato di una seconda rete (ridondante) in fibra, fornita dal provider MyNet. Entrambe le connessioni internet sono protette mediante un firewall Sophos. Tutto il traffico verso la WAN è filtrato tramite sistema di Web Security. Tutti i servizi esposti verso internet sono gestiti tramite un Proxy Server.

Tutti gli Enti consorziati sono collegati alla server farm tramite una rete MPLS in fibra a 100 MbitLa rete si basa su servizi di dominio Active Directory. Attraverso i Servizi di dominio Active Directory, la sicurezza è integrata mediante l'autenticazione di accesso e il controllo degli apparati collegati in rete. Con un unico accesso in rete, gli amministratori possono gestire i dati e l'organizzazione della directory dell'intera infrastruttura.

Nella sala server sono installati gli switch del centro stella che sono collegati con gli armati di rete dislocati ai vari piani degli edifici della sede di Comunità Montana. Gli apparati di rete del centro stella sono alimentati con batterie di continuità. In ogni Comune, collegato con il datacenter, sono installati firewall Sophos a monte della rete LAN comunale. Ogni postazione di lavoro (sia dei Comuni che dell'Ente capofila) è dotata di un antivirus Sophos gestito dall'Ufficio ICT a livello centralizzato.

Società e ditte addette alla Manutenzione degli strumenti di Elaborazione, dei software e delle reti informatiche

Nel caso in cui gli Enti richiedano l'intervento di ditte specializzate per interventi di assistenza e manutenzione, questi soggetti devono operare in base a specifica autorizzazione dell'ufficio ICT di Secoval, recante nel dettaglio i compiti da svolgere oppure in ottemperanza delle misure minime di sicurezza.

Backup e ripristino dell'accesso ai dati

Il Backup dei dati contenuti nel Sistema di Gestione Informatica dei Documenti avviene secondo le direttive del Garante Privacy e più precisamente: il salvataggio dei dati e delle configurazioni del server. Il backup viene effettuato tramite procedure automatizzate con l'ausilio del programma *Veeam*.

I dati vengono memorizzati su data domain da 24TB con sistema di deduplica. Il job di backup prevede il retain dei files fino a 7 giorni.

L'operazione viene eseguita tutte le notti 7 giorni su 7.

Al termine dell'operazione di backup viene inviata una mail contenente l'esito completo dell'attività. Un sistema di monitoraggio individua eventuali messaggi di errore ed effettua l'apertura di una segnalazione al sistema di ticketing in uso all'Ufficio ICT.

Il ripristino dell'accesso ai dati, in caso di danneggiamento degli stessi o degli strumenti elettronici, avviene entro 4 ore lavorative in caso di generico malfunzionamento, ed entro 24 ore lavorative in caso di disastro.

Per quanto riguarda le politiche di conservazione a norma dei documenti registrati nell'SdP, si rimanda all'allegato 9 del Manuale di Gestione.

Nome modello	Scheda tecnica misure di sicurezza	
Edizione : 1	Revisione: 0	Data: 04/12/2019

LOGISTICA SALA SERVER	
SISTEMI DI GESTIONE DEGLI ACCESSI	Accesso tramite badge in dotazione ufficio ICT
SISTEMI ANTINCENDIO	Presenza Estintori
SISTEMI DI CONTINUITA'	Presenza UPS
MISURE DI SICUREZZA INFORMATICHE	
<p>SISTEMI SICUREZZA PERIMETRALE E ANTIMALWARE: (Verifica aggiornamenti dei sistemi negli ultimi 6 mesi; configurazione antivirus con aggiornamento quotidiano)</p>	<p>Tutte le sedi sono collegate tramite fibra ottica in MPLS. In ogni sede è dislocato un Firewall Sophos interconnesso con un firewall centrale, localizzato presso la sede di Comunità Montana di Valle Sabbia. L'accesso ad Internet è veicolato attraverso il firewall centrale del centro stella.</p> <p>Il firewall centrale è costituito da 2 nodi in High Availability (1 attivo, l'altro in stand-by che si attiva automaticamente qualora il sistema primario sia indisponibile).</p> <p>Aggiornamenti programmati con cadenza mediamente trimestrale; vengono effettuati aggiornamenti straordinari in caso di aggiornamenti urgenti e critici.</p> <p>Antivirus Sophos con console centralizzata che analizza la situazione dei vari client e distribuisce gli aggiornamenti. Verifica degli aggiornamenti update minacce pianificata ogni 30 minuti, verifica aggiornamento software ogni 60 minuti.</p> <p>Exploit prevention che verifica eventuali processi di cifratura.</p>

<p>AGGIORNAMENTI DEI SISTEMI: (Verifica aggiornamenti dei sistemi negli ultimi 6 mesi)</p>	<p>Sulle postazioni di lavoro è configurato l'aggiornamento automatico. Sui server più rilevanti la verifica dell'aggiornamento è schedulata ogni notte. Sui server con applicazioni secondarie l'aggiornamento è effettuato circa una volta alla settimana.</p> <p>Pianificazione aggiornamenti Socr@web:</p> <ul style="list-style-type: none"> - Lunedì h 20 Mazzano, Nuvolento, Nuvolera - Mercoledì h 23 CMVS e Comune di Salò - Lunedì h 21 tutti gli altri enti
<p>LOGISTICA SALA SERVER</p>	
<p>SISTEMI DI GESTIONE DEGLI ACCESSI</p>	<p>Accesso tramite badge in dotazione ufficio ICT</p>
<p>SISTEMI ANTINCENDIO</p>	<p>Presenza Estintori</p>
<p>SISTEMI DI CONTINUITA'</p>	<p>Presenza UPS</p>
<p>MISURE DI SICUREZZA INFORMATICHE</p>	
<p>SISTEMI SICUREZZA PERIMETRALE E ANTIMALWARE: (Verifica aggiornamenti dei sistemi negli ultimi 6 mesi; configurazione antivirus con aggiornamento quotidiano)</p>	<p>Tutte le sedi sono collegate tramite fibra ottica in MPLS. In ogni sede è dislocato un Firewall Sophos interconnesso con un firewall centrale, localizzato presso la sede di Comunità Montana di Valle Sabbia. L'accesso ad Internet è veicolato attraverso il firewall centrale del centro stella.</p> <p>Il firewall centrale è costituito da 2 nodi in High Availability (1 attivo, l'altro in stand-by che si attiva automaticamente qualora il sistema primario sia indisponibile).</p> <p>Aggiornamenti programmati con cadenza mediamente trimestrale; vengono effettuati aggiornamenti straordinari in caso di aggiornamenti urgenti e critici.</p> <p>Antivirus Sophos con console centralizzata che analizza la situazione dei vari client e distribuisce gli aggiornamenti. Verifica degli aggiornamenti update minacce pianificata ogni 30 minuti, verifica aggiornamento software ogni 60 minuti.</p> <p>Exploit prevention che verifica eventuali processi di cifratura.</p>

<p>AGGIORNAMENTI DEI SISTEMI: (Verifica aggiornamenti dei sistemi negli ultimi 6 mesi)</p>	<p>Sulle postazioni di lavoro è configurato l'aggiornamento automatico. Sui server più rilevanti la verifica dell'aggiornamento è schedulata ogni notte. Sui server con applicazioni secondarie l'aggiornamento è effettuato circa una volta alla settimana.</p> <p>Pianificazione aggiornamenti Socr@web:</p> <ul style="list-style-type: none"> - Lunedì h 20 Mazzano, Nuvolento, Nuvolera - Mercoledì h 23 CMVS e Comune di Salò - Lunedì h 21 tutti gli altri enti
--	---

	<p>Aggiornamenti Halley: eseguiti a richiesta dell'ente tramite ticket</p> <p>Aggiornamenti APKappa: eseguiti a richiesta dell'ente tramite ticket</p> <p>Aggiornamenti portali:</p> <ul style="list-style-type: none"> - Portali gestiti da Internet Soluzioni effettuati dal fornitore - Portali gestiti internamente con Drupal, effettuati dai tecnici secondo necessità
<p>BACKUP: (Versioni disponibili, localizzazione dei supporti, verifica esiti dei backup, mappatura backup dei dati)</p>	<p>Snapshot macchine virtuali</p> <ul style="list-style-type: none"> - Backup giornaliero incrementale (lun-venerdi) - Backup full periodico collegato al numero di restore point (minimo 7, fino a 30 in alcuni casi) <p>Backup applicativi:</p> <ul style="list-style-type: none"> - Dump database Sicr@web effettuato giornalmente, con conservazione di 30 dump.
	<p>Localizzazione dei supporti di backup</p> <ul style="list-style-type: none"> - DATA DOMAIN localizzato in sala server - NAS localizzato in sala server per Enti non ancora migrati nel progetto TESEO <p>Segmentazione della rete che ospita i backup e i Domain Controllers dal resto dell'architettura.</p>
	<p>Verifica esito dei backup</p> <ul style="list-style-type: none"> - Monitoraggio giornaliero dell'esito dei processi di backup tramite email, con segnalazione a monitor dell'eventuale esito fallito del backup; - Verifica settimanale manuale dell'efficacia dei processi di backup.
	<p>Mappatura dei dati sottoposti a backup</p> <ul style="list-style-type: none"> - Effettuata tramite console di Veeam Backup & Restore

<p>UTENTI DI DOMINIO E DEGLI APPLICATIVI: (Utenti “personali”, eventuali eccezioni, disabilitazione utenti più vecchi di 6 mesi)</p>	<p>Utenze di dominio:</p> <ul style="list-style-type: none"> - Presenti utenti standard nominali - Disabilitati utenti inutilizzati da più di 6 mesi <p>Utenze Socr@web, APKappa, Halley:</p> <ul style="list-style-type: none"> - Presenti utenti standard nominali con profilazione
<p>CREDENZIALI AMMINISTRATIVE PREDEFINITE DI SISTEMI ICT (modifica delle default password dei sistemi ICT)</p>	<p>Password di default admin modificate</p>
<p>CARATTERISTICHE DELLE CREDENZIALI (lunghezza delle password, scadenza, codici univoci di identificazione, disattivazione utenti “non tecnici” dopo 6 mesi di inattività)</p>	<p>Password dominio:</p> <ul style="list-style-type: none"> - Minimo 8 caratteri - Almeno 1 lettera, 1 numero, 1 carattere speciale ed una lettera maiuscola - Non possono contenere parte dello username - Cambio ogni 3 mesi <p>Password Socr@web, APKappa, Halley:</p> <ul style="list-style-type: none"> - Policy definita dallo sviluppatore delle applicazioni
<p>GESTIONE RISORSE ASSEGNATE AGLI UTENTI (Processo di autorizzazione)</p>	<ul style="list-style-type: none"> - Richiesta abilitazione risorsa tramite apertura ticket da parte del referente dell’ente richiedente. - Rilascio di credenziali agli utenti: Il rilascio avviene tramite risposta al ticket stesso
<p>ELENCO CONNESSIONI REMOTE (Elenco aggiornato delle connessioni e relative caratteristiche)</p>	<p>Presente elenco delle connessioni remote attive con verifica periodica della necessità di sussistenza.</p>
<p>AMMINISTRATORI DI SISTEMA: (Utenti “personali”, disabilitazione utenti più vecchi di 6 mesi, elenco AdS, utenti impersonali messi in sicurezza)</p>	<ul style="list-style-type: none"> - Prevista gestione utenze impersonali (root, admin, ecc.) con registrazione degli accessi. - Utenti amministratori con credenziali personali. - Presente elenco Amministratori di Sistema, specificamente nominati. - Utente backup dedicato con password. - Lunghezza password AdS almeno 10 caratteri.

<p>LOG AMM.RI DI SISTEMA (Presenza di soluzioni per il tracciamento log AdS)</p>	<p>Log AdS Dominio:</p> <ul style="list-style-type: none"> - Sistema Netwrix <p>Log AdS Sicr@web, APKappa, Halley:</p> <ul style="list-style-type: none"> - Policy definita dallo sviluppatore delle applicazioni -
<p>REPORT DI INTERVENTO (verifica rapporti di intervento redatti)</p>	<p>Gli interventi sono sempre registrati nel sistema di ticketing.</p>