C O M U N E D I O L B I A

Settore Affari Generali e Provveditorato

Manuale di Gestione del Protocollo
Informatico e dei Documenti Informatici

allegato 10

piano di sicurezza

versione 1.1 del 13/01/2022

Via Dante, 1 – 07026 OLBIA (OT) - Tel 0789-52220

Document History:

Version	***Date***	***Prepared/Modified by***	***Changes comparing to previous versions***
1.0	14/10/2015	Dott. Sebastiano Bellu	First release

Review & Approval

Review Name	***Date***	***Approved***
1.0	14/10/2015	Dott.ssa Annamaria Manca Dott. Sebastiano Bellu

Via Dante, 1 – 07026 OLBIA (OT) - Tel 0789-52220

1 Introduzione

1.1 Obiettivo

Descrizione degli aspetti tecnici e di sicurezza inerenti il Sistema di Gestione Documentale e di Protocollo Informatico del Comune di Olbia.
Il Piano di sicurezza garantisce che:

- i documenti e le informazioni trattati siano resi disponibili, integri e riservati;
- i dati personali comuni, sensibili e/o giudiziari vengano 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.

1.2 Acronimi

SI	Sistema Informativo
ICT	Information and Communication Technology (*Tecnologie dell'informazione e della comunicazione*)
HW	Hardware
SW	Software
PdL	Postazioni di Lavoro: PC + Stampante + UPS
W3C	World Wide Web Consortium
DMZ	**Demilitarized Zone**: è un segmento isolato di LAN (una "sottorete") raggiungibile sia da reti interne sia esterne che permette, però, connessioni esclusivamente *verso* l'esterno: i server attestati sulla DMZ non possono connettersi alla rete aziendale interna.
FTP	**File Transfer Protocol**: protocollo per la trasmissione di grandi quantità di dati tra due computer.
SSL	**Secure Sockets Layer**: è un protocollo che attraverso un sistema di crittografia, assicura che la trasmissione di dati fra un cliente ed un server avvenga in maniera protetta.
FTPs	**File Transfer Protocol on SSL**: è una estensione del protocollo FTP che rende sicuro il trasferimento del dato attraverso la combinazione con il protocollo SSL.

1.3 Glossario

La seguente tabella contiene la definizione di alcuni termini usati nel documento.

Termine	Definizione
Accessibilità telematica ai dati	Proprietà dei sistemi informatici mediante la quale viene data la possibilità, a soggetti esterni all'amministrazione titolare, di fruire attraverso una rete telematica di specifici dati. L'accesso può essere effettuato sia in modalità interattiva da persone sia in modalità automatizzata da sistemi informatici.
Base di dati (o banca dati)	Insieme di dati omogenei, di interesse rilevante per una o più unità organizzative, memorizzati in uno o più archivi informatici, organizzati ed accessibili mediante uno strumento software (ad es., sistemi di gestione di basi di dati, sistemi di information retrieval).
CAD	Codice Amministrazione Digitale
Reg.2016/679 GDPR	Regolamento Generale per la Protezione dei Dati
Cooperazione applicativa	La parte del sistema pubblico di connettività finalizzata all'interazione tra i sistemi informatici delle pubbliche amministrazioni per garantire l'integrazione dei metadati, delle informazioni e dei procedimenti amministrativi (art. 72 CAD).
Dato delle pubbliche amministrazioni	Il dato formato, o comunque trattato da una pubblica amministrazione (art.1 CAD).

Via Dante, 1 – 07026 OLBIA (OT) - Tel 0789-52220

Termine	Definizione
Dato personale	Qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale (art. 4 Codice privacy).
Dato pubblico	Il dato conoscibile da chiunque (art.1 CAD).
Dati sensibili	I dati personali idonei a rilevare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rilevare lo stato di salute e la vita sessuale (art. 4 Codice privacy).
Disponibilità (dei dati)	La possibilità di accedere ai dati senza restrizioni non riconducibili a esplicite norme di legge (art. 1 CAD)
PEC	Posta Elettronica Certificata.
OTP	One-time Password: password che è valida solo per una singola sessione di accesso o una transazione.

1.4 Riferimenti

[1] Sito ufficiale Comune di Olbia: www.comune.olbia.ot.it
[2] Regione Sardegna: www.regione.sardegna.it
[3] Agenzia per l'Italia Digitale: www.agid.gov.it

Via Dante, 1 – 07026 OLBIA (OT) - Tel 0789-52220

2 Descrizione dell'infrastruttura tecnologica

2.1 Analisi dei Rischi

Poichè in questo allegato si fa riferimento ai soli documenti informatici amministrativi gestiti con il sistema documentale e il protocollo informatico dell'Ente, si demanda per tutti gli altri aspetti della sicurezza all'Analisi dei Rischi, in particolare quelli legati alla sicurezza fisica dei luoghi.
Di seguito le principali misure tecniche adottate:

- *Alimentazione elettrica*. Il Data Center, gli apparati di rete, e quasi tutti i personal computer client, sono protetti da UPS (centralizzato e a valle di gruppo elettrogeno), garantendo il corretto spegnimento degli apparati in caso di interruzione della fornitura elettrica;
- *Backup*. Sono stati implementati i sistemi di backup (su LTO8 con CA ArcServe e con UDP ArcServe ridondato su sito secondario) con una retention di 120 giorni mensile, realizzando un sistema di data recovery che garantisca da malfunzionamenti o perdite accidentali. Il backup è criptato.
- *Sistemi di protezione sui sistemi centrali*. I dati dell'amministrazione sono storicizzati sia su cartelle condivise che su DBMS, opportunamente controllati per evitare accessi non autorizzati (policy su ActiveDirectory su unico dominio comuneolbia.it e Grant specifici sulle tabelle dei DB). I Server sono tutti in RAID5; é presente inoltre un appliance Juniper STRM 500II per la memorizzazione dei log di sistema.
- *Contratti di assistenza tecnica*. Al fine di garantire la continuità del servizio e comunque di ridurre al minimo i tempi di fermo macchina, sono attivi contratti di manutenzione HW e SW di primo livello con fornitori qualificati e con livelli di servizio prestabiliti;
- *Sistemi antincendio*. La sede comunale rispetta tutte le normative di legge previste in merito alla sicurezza antincendio, quindi sono dislocati estintori in diversi locali. In paricolare il DataCenter primario è dotato di allarme per la rilevazione di fumi;
- *Accesso alle banche dati e internet.* È previsto ed operante un sistema di autenticazione informatica attraverso gestione delle utenze con Active Directory su un unico dominio di rete. Per ogni applicativo è previsto l'utilizzo di credenziali e profilazione che determina le funzionalità utilizzabili e il livello di visibilità dei dati (scoop).
- È presente un sistema centralizzato di antivirus.
- È presente un Firewall in cluster per il controllo dell'accesso alla rete comunale (IDS, Web Filtering, etc.).

2.2 Architettura della Rete (LAN) Comunale

Di seguito vengono riportati alcuni dati relativi alla infrastruttura informatica del Comune di Olbia.
Tutte le sedi comunali hanno un cablaggio di rete e sono tra loro collegate in Fibra Ottica.
L'accesso a Internet dell'amministrazione avviene in un unico punto con FO 1Gbps simmetrico SPC2, con filtro attraverso il sistema di Firewall in dotazione (Fortinet 1200D).

Viene garantita la gestione della sicurezza per l'uso delle strutture software e hardware presenti nell'amministrazione per una protezione della LAN comunale, attraverso Firewall Fisico in alta affidabilità (con WebFiltering) e sistema di Antivirus.

Viene garantita la sicurezza dei dati oltre che attraverso l'utilizzo di server con sistema di memorizzazione di massa in RAID 5, anche attraverso un backup su disco e su nastro (Arcserve LTO8 e ArcServe UDP ridondato).
È presente un sito secondario di DR con il quale viene replicata la componente elaborativa (i server) e quella dei dati (volumi). Per ulteriori approfondimenti si demanda il PCO-ICT.

È presente una Intranet per l'amministrazione comunale, protetta da accessi esterni non autorizzati, che crea un sistema di informazioni e servizi di utilità generale accessibili della rete interna. Questo permette oggi di avere un supporto all'accesso ai sistemi informativi, ai dati e alle procedure dei sistemi gestionali e di tutti gli altri applicativi nell'amministrazione. Sfruttando la Intranet, è stato realizzato anche un sito interno per la

Via Dante, 1 – 07026 OLBIA (OT) - Tel 0789-52220

pubblicazione di contenuti, si è realizzata in questo modo una comunicazione unidirezionale verso il personale.

E' presente:
- un sito istituzionale su un proprio dominio su server di terze parti (Municipium).
- un Portale dei Servizi OnLine, per la fornitura di servizi per enti esterni, quali le Forze dell'Ordine (Carabinieri, Polizia, Finanza), Agenzia delle Entrate e altri enti pubblici.
- un sistema di posta elettronica su proprio dominio su server di terze parti.
- esistono più caselle di Posta Elettronica Certificata.

Il sistema di autenticazione utilizzato è il Dominio Windows Active Directory, attraverso il quale si autorizzano gli utenti interni all'uso delle risorse (cartelle, file, stampanti, etc..) condivise nella rete comunale (LAN) e, in un'ottica SSO, anche all'accesso di alcuni applicativi.

La rete Comunale è segmentata logicamente in una LAN e una DMZ. Nella DMZ sono attestati i Server che permettono l'esecuzione di applicazioni attraverso le quali si forniscono servizi verso l'esterno.

2.3 Tipologie di collegamenti fra le sedi Comunali

Nella **Figura2**, si riporta la configurazione degli uffici comunali localizzati su sedi distaccate nelle strette vicinanze alla sede principale di Via Dante 1 (a parte San Pantaleo e Berchideddu situati a circa a 20Km).

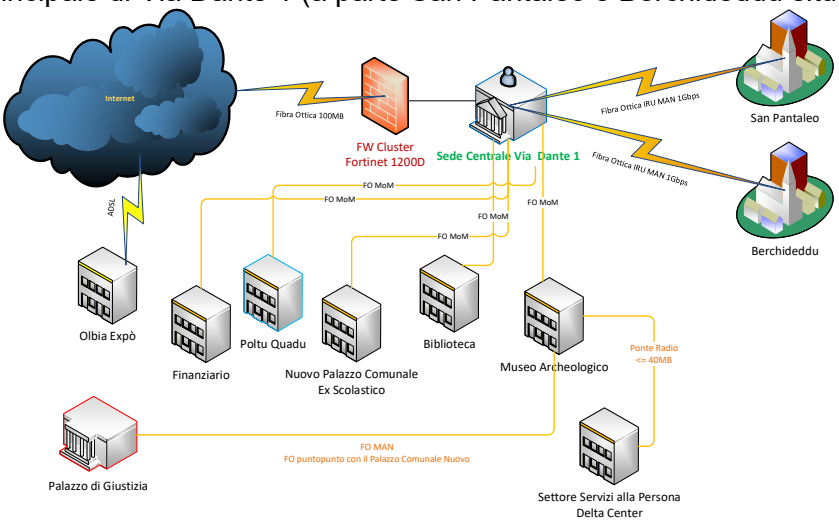

Figura 1: *Siti del Comune di Olbia e tipologia di collegamenti.*

Via Dante, 1 – 07026 OLBIA (OT) - Tel 0789-52220

3 Criteri Tecnici sulle modalità di accesso.

L'accesso al Sistema di Gestione Documentale e di Protocollazione Informatica (in seguito "Sistema"), è reso disponibile attraverso la rete Intranet ed apposita suite applicativa HyperSIC.NET. Il Sistema è garantito da un Application Server e un DB Server virtuali (VMware Enterprise Plus) configurato nella sottorete LAN.
L'accesso avviene mediante autenticazione (Login e Password) dell'utente. Tali credenziali vengono rilasciate dal Servizio ICT del Comune, utilizzando l'applicazione "Amministratore" della suite HyperSIC.NET. L'applicazione web che realizza il sistema in questione, non permette più accessi contemporanei da postazioni fisiche/virtuali distinte, utilizzando le stesse credenziali; per tale ragione il sistema prevede anche una password di sblocco per poter terminare una sessione di consultazione aperta su un'altra postazione.
Il sitema fornisce la funzionalità che restituisce un report di tutti gli utenti abilitati con i relativi profili funzionali.
Al primo accesso al sistema informatico, gli utenti abilitati al sistema, devono sostituire la password provvisoria loro assegnata con una di loro scelta, il tutto in confirmità alle prescrizione del GDPR. Il sistema chiederà il **rinnovo della password dopo 6 mesi** e, comunque, trascorsi 6 mesi senza che sia utilizzata, la credenziale stessa sarà automaticamente bloccata (in tal caso l'utente dovrà richiederne lo sblocco).
In caso di cessazione di un utente dall'incarico, il Servizio ICT provvede a disabilarlo da futuri accessi.

3.1 Regole minime di Sicurezza

Il Responsabile del SI da disposizioni agli utenti affinché la password sia mantenuta **segreta**, venga conservata adeguatamente e non venga né comunicata né divulgata. La password dovrà essere modificata alle scadenze temporali suggerite dall'applicativo.
Il collegamento è consentito agli utenti abilitati esclusivamente durante lo svolgimento della propria attività lavorativa.

Al fine di consentire agli operatori l'accesso alle sole informazioni pertinenti e non eccedenti rispetto al proprio profilo e alla finalità istituzionale perseguita, l'accesso ai dati sarà consentito attraverso la segmentazione degli stessi.
Il Comune è legittimato a registrare tutti gli accessi sul proprio sistema informativo memorizzando gli accessi effettuati, al fine di prevenire o correggere malfunzionamenti del sistema e garantire l'efficienza dello stesso, mettendo tali informazioni a disposizione dell'autorità giudiziaria, qualora vengano richieste, nonché di effettuare controlli a scadenza almeno semestrale, anche per verificare eventuali accessi anomali.

In particolare, come misure di sicurezza:

a. il Comune garantisce le misure minime di sicurezza come emanate da AgID, al fine di adempiere agli obblighi sulla sicurezza e sulla fruibilità dei dati.
b. le postazioni da cui si effettua il collegamento al sistema, sono collocate in luogo non accessibile al pubblico e, comunque, poste sotto la responsabilità dell'operatore designato e connesse alla rete IP locale dell'Ente stesso.
c. la procedura di registrazione dell'incaricato al trattamento, viene effettuata utilizzando i dati che vengono dichiarati dall'Uffico del Personale.
d. le regole di gestione delle credenziali di autenticazione prevedono:
   • le credenziali di accesso vengono rilasciate direttamente all'utente abilitato.
   • le credenziali di accesso sono costituite da username e password.
e. per le credenziali username/password, sono adottate le seguenti politiche di gestione delle password:
   • al primo accesso l'applicazione web richiede obbligatoriamente la modifica della password iniziale; successivamente viene richiesta la modifica ogni 6 mesi; il sistema prevede che in caso di modifica la nuova password sia diversa dalle ultime 9 utilizzate;
   • l'applicazione web vincola le password ai seguenti requisiti di complessità: almeno otto caratteri, almeno una lettera maiuscola, almeno una lettera minuscola, almeno un numero, almeno un carattere speciale;
   • la sessione di lavoro viene bloccata dopo 30 min. di inattività (timeout);
   • le credenziali vengono bloccate a fronte di 10 reiterati tentativi falliti di autenticazione.
f. il Comune dispone di un firewall in cluster (full-tollerance) per la protezione perimetrale del sistema informatico; accessi esterni direttamente sul sistema informatico vengono effettuati dagli amministratori

Via Dante, 1 – 07026 OLBIA (OT) - Tel 0789-52220

tecnici, oppure da dipendenti in SmartWorking, attraverso l'utilizzo di reti private virtuali (VPN) gestite dal firewall.

g. i sistemi software, i programmi utilizzati e la protezione antivirus del comune sono costantemente aggiornati sia sui server che sulle postazioni di lavoro.
h. il Servizio ICT verifica annualmente le misure di sicurezza, al fine di adeguarle ai progressi tecnici e all'evoluzione dei rischi.
i. il Sistema Documentale e Protocollo Informatico garantisce che la procedura di autenticazione dell'utente viene protetta dal rischio di intercettazione delle credenziali. Questo a livello di database, dove le password vengono memorizzate in maniera criptata (AES_256) nelle relative tabelle.
j. il Sistema Documentale e Protocollo Informatico, attraverso una funzionalità di configurazione della applicazione web, controlla che gli accessi siano effettuati in ore e/o giorni prestabiliti, sulla base delle esigenze d'ufficio.
k. il Sistema Documentale e Protocollo Informatico esclude la possibilità di effettuare accessi contemporanei con le medesime credenziali da postazioni diverse.
l. tutte le operazioni eseguite sul Sistema Documentale e Protocollo Informatico, anche relative al trattamento di dati personali, che vengono effettuate dalle varie utenze, comprese le utenze di tipo applicativo e sistemistico (amministratori), sono tracciate dal Sistema stesso.

L'accesso in lettura e scrittura alle directory di rete (volume U del DB-Server) utilizzate come deposito dei documenti indicizzati dal Sistema Documentale e Protocollo Informatico, è effettuato dal processo server dell'applicativo, mai dalle stazioni di lavoro. Il Responsabile del Servizio ICT garantisce la puntuale esecuzione delle operazioni di backup sia del DB che dei documenti informatici (su Nastro con LTO8, su doppio sistema di backup ArcServe UDP, con replica VMware su sito di DR). Ogni operazione di manutenzione o di backup effettuata sul sistema che ospita la base documentale e sul sistema di protocollo informatico è registrata su un file di log.
Il Sistema 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.

3.2 Sottoscrizione e Datazione di un Documento Informatico

La sottoscrizione dei documenti informatici è eseguita con una Firma Digitale (in seguito FD), basata su un certificato rilasciato da Actalis SpA, accreditato presso AgID. Tale FD è generata con un dispositivo sicuro. Per i documenti informatici che non necessitano di sottoscrizione con FD, l'identificazione dei soggetti che li producono è assicurata della sistema informatico di gestione dei documenti (login/password) oppure dal sistema di posta elettronica certificata, o, nei casi previsti, dal sistema di posta elettronica.

Per attribuire una data certa al documento informatico ci si avvale del riferimento temporale contenuto nella segnatura di protocollo di cui all'art. 9 del decreto del Presidente del Consiglio dei Ministri, 31 ottobre 2000, pubblicato nella Gazzetta Ufficiale 21 novembre 2000, n. 272. Altra data certa è fornita dal Conservatore esterno PaRER.

3.3 Livelli di Servizio e Modalità di Assistenza

In caso di interruzioni programmate (normalmente per permettere gli aggiornamenti software), il CED informa gli utenti, dei tempi previsti di interruzione e del ripristino del servizio.
Il CED assicura l'intervento entro quarantotto (48) ore dalla segnalazione. Gli addetti al CED garantiscono l'assistenza tutti giorni dal Lunedì al Venerdì, dalle 08:00 alle 14:00 e dalle 15:30 alle 18:30.

Via Dante, 1 – 07026 OLBIA (OT) - Tel 0789-52220