UNIONE MONTANA ALTO ASTICO

Sede : Via Europa 22 – 36011 Arsiero (VI)
Tel. 0445740529 - Fax 0445741797
C.F. 83002610240 – P.IVA 03013720242
e-mail: protocollo@altoastico.it
P.E.C.: um.altoastico.vi@pecveneto.it

Allegato sub B alla Deliberazione di Giunta n. 11 del 15/03/2023

PIANO DELLA SICUREZZA INFORMATICA

Sommario

1 Il piano di sicurezza informatica

1.1 Definizione

Il ricorso alle tecnologie dell'informazione e della comunicazione intrapreso dall'Unione Montana Alto Astico per lo snellimento, l'ottimizzazione e una maggiore efficienza dei procedimenti amministrativi comporta una serie di rischi che, se non adeguatamente affrontati, potrebbero comportare gravi conseguenze sull'affidabilità dei dati e dei servizi. Tali rischi sono imputabili a due fattori caratteristici della tecnologia in questione: la non garanzia di corretto funzionamento sia nelle componenti hardware che in quelle software e l'esposizione alle intrusioni informatiche. In termini più operativi è bene intendere la sicurezza del Sistema Informativo non solo come "protezione del patrimonio informativo da rilevazioni, modifiche o cancellazioni non autorizzate per cause accidentali o intenzionali" ma anche come "limitazione degli effetti causati dall'eventuale occorrenza di tali cause".
Si evidenzia che la sicurezza del Sistema Informativo non dipende solo da aspetti tecnici ma anche, se non principalmente, da quelli organizzativi, sociali e legali. La sicurezza del Sistema Informativo è pertanto vista come caratteristica "globale", in grado di fornire dinamicamente, con l'evolversi temporale delle necessità e delle tecnologie, il desiderato livello di disponibilità, integrità e confidenzialità delle informazioni e dei servizi erogati.
Il presente Piano descrive le misure di sicurezza adottate per la formazione, la gestione, la trasmissione, l'interscambio, l'accesso e la conservazione dei documenti informatici, nel rispetto anche di quanto disposto dal D. Lgs. 196/2003, "Codice in materia di protezione dei dati personali**,** recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE**",** del relativo Allegato B "Disciplinare tecnico in materia di misure minime di sicurezza" e dal Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27.04.2016.
Sono elencate inoltre le strategie ed i controlli adottati per assicurare al Sistema Informativo dell'ente un adeguato livello di sicurezza.

1.2 Obiettivi

Scopo del presente documento è descrivere la strategia che l'ente intende adottare per poter soddisfare i seguenti requisiti di sicurezza:

- **CONFIDENZIALITÀ**: l'accesso e la divulgazione delle informazioni presenti nel sistema, indipendentemente dal formato in cui si trovano, deve poter essere effettuato solo da entità autorizzate. Devono essere ridotte al minimo, compatibilmente con i limiti delle tecnologie e risorse impiegate, la probabilità che un'informazione riservata sia resa pubblica.
- **INTEGRITÀ**: la modifica o la distruzione di informazioni presenti nel sistema, indipendentemente dal formato in cui si trovano, devono poter essere effettuate solo da entità autorizzate. Devono essere ridotte al minimo, compatibilmente con i limiti delle tecnologie e risorse impiegate, le probabilità che l'informazione sia in qualche modo modificata. Devono essere altresì garantiti sia l'origine del dato (non ripudiabilità) che la sua conformità all'originale (autenticità).
- **DISPONIBILITÀ**: l'accesso all'informazione e ai sistemi deve essere sempre affidabile e tempestivo. Una perdita di disponibilità si verifica quando a fronte di un'intrusione un sistema diventa non più accessibile da parte degli utenti.

- **TRACCIABILITÀ**: tutte le azioni che un'entità compie nell'ambito del sistema sono memorizzate in modo tale da poter essere, in tempi successivi, ricondotte in maniera inequivocabile all'entità stessa.

L'adozione di idonee e preventive misure di sicurezza garantisce che il trattamento dei dati personali comuni identificativi, sensibili e/o giudiziari venga effettuato in modo da ridurre al minimo 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.

Il Piano per la sicurezza informatica si basa attualmente sull'analisi dei rischi a cui è esposto il sistema informatico, i relativi dati e documenti in esso contenuti e sulle direttive strategiche stabilite dal vertice dell'Ente.

Il presente Piano è soggetto a revisione, in funzione dell'estensione del sistema, dell'evoluzione tecnologica, della variazione degli obiettivi dell'organizzazione e del manifestarsi di nuovi o mutati rischi per la sicurezza. In caso di eventi straordinari il Piano è soggetto ad una revisione estemporanea.

2 Il sistema informativo dell'ente

2.1 Tipologia di servizi offerti

Il Sistema Informativo dell'Unione Montana Alto Astico è rivolto a soddisfare tutte le esigenze di carattere informativo-informatico, sia dal punto di vista delle esigenze "interne" cioè sostanzialmente provenienti dai servizi interni all'amministrazione stessa sia, quasi sempre indirettamente, provenienti dall'utenza esterna all'amministrazione.
Nell'uno e nell'altro caso l'esigenza può essere soddisfatta o da un sistema effettivamente interno, fisicamente residente presso sistemi informativi dell'ente, oppure tramite un sistema esterno, reso disponibile da altri enti e all'ente stesso accessibile con le opportune modalità.

2.2 Servizio informativo

2.2.1 Organizzazione

Nel contesto del Sistema Informativo ogni dipendente dell'Unione Montana Alto Astico deve collaborare, secondo le proprie specifiche funzioni, alla gestione del Sistema Informativo e alla gestione generale della sicurezza.

Tipologia Utenti	**Compiti/Responsabilità**
Addetti società assistenza hardware e software	• attuazione e messa in opera delle politiche di sicurezza informatica (sistemi antivirus, firewalling, backup, politiche relative alle utenze, …); • verifiche sull'attuazione delle politiche;
Dipendenti dell'Unione Montana Alto Astico (generici)	• rispetto delle norme relative alla Sicurezza Informatica; • rispetto delle norme inerenti il trattamento dati;

2.3 Infrastruttura tecnologica

2.3.1 Struttura fisica

La struttura è costituita da rete interna CAT.5e (cablaggio strutturato) che serve 15 PC client in dominio Windows. Tutti i PC client hanno sistemi operativi Windows 10/11.
Il server di dominio, che svolge anche funzione di file server per gestione dell'area documentale dell'Ente, è in cloud presso il Centro Servizi Territoriale(CST) della Regione Veneto PASUBIO TECNOLOGIA, allocato in datacenter certificato a norme ISO 27017 e 27018.
Il cablaggio interno fa capo a centro stella in armadio rack in locale accessibile al solo personale autorizzato ove risiedono switch 24 porte e router/firewall.
Non sono presenti server interni, né sono previsti backup PC client.
La sicurezza dei dati all'interno del server in cloud è garantita dal fornitore del servizio che opera in conformità alle norme ISO per garantire la disponibilità del dato a fronte di qualsiasi evento o incidente di sicurezza).
Tutto il software applicativo e gestionale è fruito in cloud in modalità Saas (software as a service) dai rispettivi fornitori su piattaforme certificate per la PA. Anche in questo caso la sicurezza delle

informazioni è garantita dal fornitore del servizio, ivi compresa la cifratura dei dati nelle comunicazione tra Pc locale e cloud service remoto.

Caratteristiche sede

- Ubicazione: Via Europa n. 22 – 36011 Arsiero (VI)
- Videosorveglianza: Non presente
- Allarme: Non presente
- Antincendio: Presidi manuali

Caratteristiche Uffici

Denominazione	Accesso	Armadi chiusi a chiave	Cassaforte
Segreteria	Porta chiusa a chiave	Sì	Una a muro
Servizi sociali 1	Porta chiusa a chiave	Sì	
Servizi sociali 2	Porta chiusa a chiave	Sì	
Servizi sociali 3	Porta chiusa a chiave	Sì	
Università Popolare	Porta chiusa a chiave	Sì	
Ragioneria 1	Porta chiusa a chiave	Sì	
Ragioneria 2	Porta chiusa a chiave	Sì	
Sala Giunta	Porta chiusa a chiave	Sì	
Ufficio di Piano Sviluppo Multiservizi	Porta chiusa a chiave	Sì	
Servizi sociali 4	Porta chiusa a chiave	Sì	

Gli estintori sono presenti in numero totale di 4 nel vano scale (2 al piano terra, 1 al primo e 1 al secondo), oltre a 1 nel locale caldaia.

Caratteristiche armadio di rete

- Ubicazione: Secondo piano
- Accesso: chiuso a chiave
- UPS: Sì
- Raffreddamento: Aria
- Ignifugo: Sì
- Posizione: Vano tecnico

Caratteristiche connettività

Linea primaria (Fibra ottica)

- Gestore: Axera-Telemar
- Tipologia: FTTH 1000-300 Mbps

Linea secondaria (Wifi)

- Gestore: Axera-Telemar
- Tipologia: Wi-Fi 30/6 con banda garantita 40%

Caratteristiche centralino

- Marca e modello: ALCATEL OmniPCX Office 50
- Linee: n°3 ADSL
- Ubicazione: piano terra
- UPS: No

2.3.3 Sistema di Conservazione

Per quanto concerne il sistema di conservazione si fa rimando a quanto dettagliato nel Manuale di Gestione.

3 Politiche organizzative della sicurezza

3.1 Generalità

La definizione e l'applicazione delle politiche di sicurezza all'interno dell'ente richiedono l'individuazione di un insieme di regole che fanno riferimento alle tecnologie usate, alle metodologie, alle procedure d'implementazione e ad altri elementi specifici dell'ambiente e del sistema informativo. L'applicazione delle politiche di sicurezza all'interno dell'ente richiede, inoltre, la definizione di processi che descrivano gli specifici passi operativi che le persone devono seguire per raggiungere gli obiettivi che sono stati stabiliti. I processi sono indispensabili per la gestione di tutti gli oggetti legati alla sicurezza.
Attualmente, l'individuazione della politica di sicurezza determina il modello logico della sicurezza fissandone gli obiettivi. L'individuazione degli obiettivi di sicurezza si traduce in obiettivi del sistema informativo, sostanziandosi con la formalizzazione di norme organizzative e standard di riferimento. Inoltre, la sicurezza viene considerata, da tutto il personale, una componente integrante dell'attività quotidiana, finalizzata alla protezione delle informazioni e delle apparecchiature da manomissioni, uso improprio o distruzione. Un sistema di sicurezza, per poter raggiungere i migliori risultati funzionali, va visto globalmente, negli aspetti fisici, logici e organizzativi, come un insieme di misure e strumenti hardware, software, organizzativi e procedurali integrati fra loro, volti a ridurre la probabilità di danni a un livello accettabilmente basso e ad un costo ragionevole.

3.1.1 Backup e Disaster Recovery

Non esiste un "local backup" perché i dati sono centralizzati sul server in cloud. Il fornitore si occupa della gestione della sicurezza per garantire la disponibilità dei dati secondo quanto previsto dalle regole del sistema di certificazione e dalla normativa vigente. Il fornitore è CST Regionale della Regione Veneto per la Provincia di Vicenza.

3.2 Sicurezza logica

3.2.1 Introduzione

La sicurezza logica si occupa della protezione dell'informazione, dei dati, dei documenti, delle applicazioni, dei sistemi e reti, sia in relazione al loro corretto funzionamento ed utilizzo, sia in relazione alla loro gestione e manutenzione nel tempo. La realizzazione della sicurezza logica è pensata in termini architetturali e ciò comporta l'individuazione di tutti i sistemi hardware e software che implementano le attività dei vari servizi dell'ente, in modo tale da garantirne la fruibilità nel tempo, che deve essere nel contempo aperta a tutti gli operatori necessari, ma limitata alle funzioni ad essi attribuite in un determinato momento.

3.2.2 Sistema di autenticazione

Le credenziali di autenticazione consistono in un codice per l'identificazione dell'Incaricato (utente), associato a una parola chiave riservata e conosciuta solamente dal medesimo. La parola chiave è composta da almeno otto caratteri (numeri e lettere) e non contiene riferimenti agevolmente riconducibili all'Incaricato, il quale provvederà a modificarla al primo utilizzo. Le credenziali di autenticazione sono affidate al controllo del Server, che garantisce l'applicazione delle politiche di protezione e sicurezza in forma centralizzata ed automatizzata. La politica di centralizzazione del sistema informativo si appoggia al sistema integrato di *active directory* ("insieme di servizi di rete - *account* utente, *account computer*, cartelle condivise, stampanti, *etc*. -

adottati dai sistemi operativi organizzati in modo da consentirne la condivisione da parte dei *client*") tramite apposita profilazione degli utenti (gestione dei profili di autorizzazione). Ad integrare la protezione sul sistema informativo, i *software* dell'Ente e gli applicativi *web* sono dotati di apposite procedure di accesso tramite *username* ("nome con il quale l'utente viene riconosciuto da un *computer*, da un programma o da un *server*") e *password* ("sequenza di caratteri alfanumerici utilizzata per accedere in modo esclusivo ad una risorsa informatica"). Lo *username* è un identificativo che, insieme alla *password*, rappresenta le credenziali per accedere alle risorse informatiche o ad un sistema.

3.2.3 Antivirus e similari

Tutti i PC client hanno antivirus gestito ed aggiornato dal sistema operativo Windows 10/11, aggiornato dal fornitore Microsoft, mediante *Windows Update* con le opportune *patch* di sicurezza ("programma o parte di programma che aggiorna e corregge un *software*").
Per quanto riguarda la posta elettronica, antivirus, antispam ecc sono integrati nelle piattaforme di aziende certificate (nel caso dell'Ente, Axera, pluricertificata) che sono fornitori di servizio.
Regolarmente e costantemente i Responsabili aggiornano, vigilano e controllano.
Gli aggiornamenti dei programmi per elaboratore volti a prevenire la vulnerabilità degli strumenti elettronici e a correggerne difetti sono stati correttamente installati. I programmi sono stati impostati in modo da scaricare e aggiornare automaticamente le loro funzionalità garantendone quindi sempre la massima efficacia di funzionamento.
Al fine di prevenire intrusioni dall'esterno è stato installato e configurato un *firewall hardware* e su ciascun elaboratore è stato attivato il *firewall software* integrato nel sistema operativo *"Windows"*. Periodicamente sono stati eseguiti e verranno effettuati, nei tempi previsti dalla normativa, gli aggiornamenti sui sistemi di protezione.

4 Documenti e Banche dati

4.1 Sistema di gestione informatica dei documenti

Il DPR 445/2000, all'art. 1, comma 1, lett. r) definisce il Sistema di Gestione Informatica dei Documenti come *"l'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle amministrazioni per la gestione dei documenti"*. Tale sistema è attivato dall'ente su tutte le postazioni di lavoro degli uffici e le abilitazioni all'utilizzo delle sue funzionalità sono stabilite e aggiornate a cura dei Responsabili.

Per quanto concerne i software attraverso i quali viene registrato e gestito il patrimonio documentale dell'ente si fa riferimento alle indicazioni contenute nel manuale di gestione così come anche per i seguenti argomenti:

- Protocollo informatico;
- Formazione dei documenti;
- Formati adottati;
- Sottoscrizioni;
- Validazione temporale;
- Metadati;
- Trasmissione dei documenti;
- Conservazione.