SISTEMA DI GESTIONE DOCUMENTALE

PIANO PER LA SICUREZZA INFORMATICA

PERIMETRO DEL SISTEMA

- Funzionalità dell'applicativo: gestione documentale (corrispondenza, atti amministrativi, fatture,…) e workflow documentale
- Classificazione ACN: servizio ordinario
- Categoria ACN: servizi di funzionamento - gestione documentale
- Tipologia applicativo: supporto alle attività amministrative
- Tipologia utenti: interni all'azienda
- Tipologia di dati trattati: dati non personali (aziendali) e dati personali anche particolari

MISURE DI SICUREZZA

Si riportano di seguito le principali misure di sicurezza adottate per la protezione del sistema in oggetto e quindi per garantire la disponibilità, la riservatezza e l'integrità dei documenti gestiti e del registro di protocollo.

LATO APPLICATIVO

- Comunicazioni cifrate (https)
- Tracciatura log accessi e operazioni
- Autenticazione utente:
    - credenziali gestiti dall'Activity Directory aziendale tramite protocollo LDAP

    - Utenze nominative riconducibili a una sola persona (non comuni/condivise)
    - Accesso limitato solo dalle postazioni della rete aziendale – in caso di accesso esterno solo attraverso VPN
    - Imposizione di password robusta
    - Imposizione dell'aggiornamento obbligatorio periodico della password
    - le credenziali delle utenze amministrative vengano sostituite con frequenza (password aging).
    - credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history)
- Autorizzazione utente:
    - Differenziazione delle funzionalità per specifico profilo/ruolo
    - Controllo degli accessi alle aggregazioni documentali
- Gestione del ciclo di vita delle utenze (Provisioning/deprovisioning) tramite sistema specifico aziendale CRED.NET

LATO INFRASTRUTTURALE

Il sistema è ospitato dal datacenter regionale gestito da Regione Umbria-PuntoZero in corso di certificazione ACN.

Il sistema è caratterizzato da **elevata affidabilità**, garantita da:

- **Caratteristiche intrinseche dell'infrastruttura virtuale** che ospita il sistema, basata su VMware vSAN.
  In particolare, la macchina virtuale del sistema in oggetto è ospitata in un cluster composto da n. 9 server fisici.
  VMware VSAN, offre meccanismi di High Availability (HA), tra cui:
    - Se un host va giù, le VM vengono riavviate automaticamente su un altro nodo usando i dati già replicati
    - vSAN offre meccanismi di self-healing: rileva il guasto, marca i componenti come "degraded", ricostruisce automaticamente le repliche mancanti, ristabilisce il livello di affidabilità previsto dalla policy

    - consente di aggiornare host, sostituire hardware, fare manutenzione **senza interrompere i servizi documentali**

- **Replica del sistema su due siti**, primario e secondario (Data Center regionale gestito da PuntoZero, sedi di **Perugia e Terni**).
  In caso di indisponibilità o disastro di uno dei Data Center, la **continuità operativa è garantita tramite il ripristino delle macchine virtuali** presso il Data Center alternativo.

Politiche di backup delle macchine virtuali

I backup delle macchine virtuali seguono le seguenti politiche standard:

- **Macchine Database (DB)**
  Backup giornaliero con 7 punti di ripristino (retention 7 giorni)
- **Macchine Application Server e Web Server**
  Backup settimanale con 4 punti di ripristino (retention 30 giorni)

Politiche di backup del database

- Backup-dump del DB su diversa macchina virtuale (*in corso di attuazione)*

Politiche di mitigazione attacchi

- Attivi sistemi di protezione perimetrali come:
    - Sistemi anti-DDOS
    - Firewall
    - WAF
    - IDS/IPS
- L'infrastruttura virtuale attraverso la rete SDN e le funzionalità di firewall distribuito consente la micro segmentazione del traffico.
- Sono presenti sistemi EDR e XDR attraverso agent e agentless con funzionalità antivirus e anti malware che proteggono ogni sistema virtuale presente in infrastruttura.

Politiche di monitoraggio di corretto funzionamento

- Ogni sistema virtuale viene monitorato il carico computazionale a livello di CPU, RAM e spazio disco oltre a specifici processi e/o servizi attivi sui sistemi. Gli allarmi rilevati inviano mail automatiche al raggiungimento delle soglie di attenzione impostate.

Azioni di miglioramento (in corso)

I meccanismi di replica e Disaster Recovery sono oggetto di un progetto di revisione, nell'ambito del completamento del nuovo datacenter regionale gestito da Regione Umbria-PuntoZero, finalizzato a:

- implementare la **replica delle macchine virtuali** tra i siti;
- superare l'approccio basato esclusivamente sui backup;
- **ridurre i tempi di ripristino (RTO)** e migliorare la continuità operativa complessiva.

ULTERIORI INFORMAZIONI RILEVANTI

- Il sistema in oggetto viene sottoposto periodicamente a **Vulnerability Assessment** e vengono adottate le relative azioni correttive per eliminare o ridurre una vulnerabilità, una non conformità o un rischio individuato
- Connettività:
  - Banda tra datacenter primario e rete aziendale: XXXXXX
  - Banda tra datacenter secondario e rete aziendale: XXXXXX
- Integrazioni applicative:
  - Il sistema dispone di API per la cooperazione applicativa con sistemi terzi – al momento non utilizzate
  - PEC: il sistema è collegato al server di posta elettronica certificato Tinexta-Infocert provider dell'indirizzo PEC aziendale, tramite protocollo SMTP