

1. Registro asset informativi

Registro asset informativi

Il Registro degli asset informativi rappresenta uno strumento fondamentale per DNS Informatica SAS nella gestione sistematica e conforme ai requisiti di ISO9001 (clausole 7.1.3, 8.1) e ISO/IEC 27001 (clausole 8.1, A.8) degli elementi informativi rilevanti per l'erogazione dei servizi ICT e di consulenza. Tale registro consente di identificare, classificare, proteggere e monitorare gli asset informativi, garantendo la riservatezza, integrità e disponibilità delle informazioni critiche per l'azienda e i suoi clienti.

1. Scopo e ambito di applicazione

Il registro copre tutti gli asset informativi utilizzati nei processi di DNS Informatica SAS, inclusi hardware, software, dati, documentazione, infrastrutture di rete e servizi cloud. L'ambito comprende sia le risorse fisiche presso le sedi di Romentino (NO) e Trecate (NO), sia le risorse virtuali e i servizi erogati in outsourcing o in hosting. Il registro supporta la conformità ai requisiti normativi e contrattuali, nonché la gestione del rischio informativo.

2. Responsabilità e ruoli

La responsabilità primaria della gestione del registro asset informativi è attribuita al Responsabile ICT, che coordina l'identificazione, la classificazione e l'aggiornamento degli asset in collaborazione con il Referente per la Sicurezza delle Informazioni. Il management aziendale garantisce le risorse necessarie per mantenere il registro aggiornato e integrato con le attività di valutazione del rischio e controllo interno. Tutti i dipendenti sono tenuti a segnalare variazioni o anomalie relative agli asset di cui sono utenti o custodi.

3. Metodologia di identificazione e classificazione

Gli asset informativi sono censiti mediante un processo strutturato che prevede la raccolta di informazioni dettagliate quali: tipologia, ubicazione, proprietario, valore aziendale, livello di riservatezza, requisiti di protezione, stato di manutenzione e ciclo di vita. La classificazione segue criteri basati sull'impatto potenziale in caso di compromissione in linea con la valutazione del rischio prevista da ISO/IEC 27001 (clausola 6.1.2). Il registro distingue tra asset critici, strategici e di supporto, facilitando la prioritizzazione delle misure di sicurezza.

4. Struttura e contenuti del registro

Campo |

Descrizione |

Note operative |

ID Asset |

Codice univoco di identificazione |

Generato secondo schema interno per tracciabilità |

Nome Asset |

Denominazione chiara e descrittiva |

Es. Server Cloud, Database Clienti, Laptop Tecnico |

Tipologia |

Hardware, Software, Dato, Servizio, Documentazione |

Classificazione funzionale |

Proprietario |

Responsabile aziendale dell'asset |

Individua il referente per la gestione e sicurezza |

Ubicazione |

Luogo fisico o virtuale |

Sede legale, operativa o cloud provider |

Valore aziendale |

Importanza strategica e operativa |

Valutazione qualitativa e quantitativa |

Classificazione di sicurezza |

Livello di riservatezza e criticità |

Confidenziale, interno, pubblico |

Stato |

Attivo, in manutenzione, dismesso |

Indica la disponibilità e integrità |

Data ultima revisione |

Data dell'ultimo aggiornamento del record |

Garantisce la freschezza delle informazioni |

5. Procedure di aggiornamento e controllo

Il registro è soggetto a revisione periodica almeno annuale, con aggiornamenti tempestivi in caso di modifiche significative quali acquisizioni, dismissioni, migrazioni o incidenti di sicurezza. Le modifiche sono documentate tramite un sistema di controllo delle versioni e approvate dal Responsabile ICT. Le attività di verifica includono audit interni e controlli incrociati con i registri di manutenzione inventario hardware/software e report di sicurezza.

6. Integrazione con la gestione del rischio e la sicurezza delle informazioni

Il registro asset informativi alimenta direttamente il processo di valutazione e trattamento del rischio previsto da ISO/IEC 27001 (clausola 6.1.2), consentendo di identificare le vulnerabilità e definire le contromisure più efficaci. La classificazione degli asset guida la definizione delle politiche di accesso, backup, cifratura e monitoraggio, in coerenza con le esigenze di riservatezza, integrità e disponibilità. Eventuali non conformità rilevate durante gli audit sono gestite secondo la procedura di miglioramento continuo.

7. Evidenze documentali e indicatori di performance

Il registro costituisce documentazione controllata e deve essere conservato in formato digitale protetto, con backup regolari e accesso riservato. Le evidenze di aggiornamento includono log di modifica, report di audit e verbali di riunioni di revisione. Gli indicatori di performance correlati comprendono la percentuale di asset aggiornati entro i termini previsti, il numero di anomalie riscontrate e il tempo medio di risoluzione delle non conformità. Tali indicatori sono oggetto di monitoraggio periodico e revisione da parte della Direzione.

8. Interfacce e relazioni con altri processi aziendali

Il registro interagisce con i processi di gestione delle risorse IT, manutenzione, sicurezza informatica, gestione dei fornitori e formazione del personale. La corretta alimentazione del registro richiede la collaborazione tra i reparti tecnici, amministrativi e di sicurezza. Le modifiche agli asset devono essere comunicate tempestivamente per garantire coerenza tra i sistemi di gestione e la documentazione associata. Il processo di audit interno verifica la congruenza e l'efficacia di tali interfacce.

[Placeholder per diagrammi di flusso del processo di gestione del registro asset informativi, inclusivo delle fasi di identificazione, classificazione, aggiornamento, controllo e integrazione con la gestione del rischio]