

Camera valdostana delle imprese e delle professioni

Analisi dei Rischi specifici del Sistema Documentale e della Conservazione Allegato al Piano della sicurezza del sistema di conservazione e dei documenti informatici

Asset

Tipologia Asset dei Sistemi di Gestione Documentale e Conservazione	Asset individuati per Camera valdostana delle imprese e delle professioni	Asset Individuati per InfoCamere (x Servizi erogati alla Camera)
Organizzazione	Camera valdostana delle imprese e delle professioni	InfoCamere
Personale coinvolto	Addetti al Sistema di Gestione Documentale (GEDOC)	Addetti al Sistema di Gestione Documentale (GEDOC) e Addetti al Sistema di Gestione Documentale (GEDOC)
Dati (dei Sistemi, di autenticazione e di abilitazione)	Documenti informatici e dati correlati della Camera, profili di abilitazioni del Personale, credenziali del Personale	Dati (i documenti della Camera) conservati nei Database e Storage di InfoCamere e nella strumentazione informatica InfoCamere di supporto alla erogazione dei sistemi di Gestione documentale e della Conservazione, dati relativi alle abilitazioni del Personale, dati relativi alle Credenziali del Personale Camerale e InfoCamere
Infrastrutture IT (Server, Reti, DBMS)	Sistemi (workstation e server di appoggio) nella sede della Camera, Rete IC in Camera, Server di memorizzazione presenti nella sede della Camera e relativo software di gestione e sicurezza (ad esempio: antimalware), in particolare quelli relativi alla erogazione dei Servizi di gestione documentale e conservazione	Server centralizzati in InfoCamere per la gestione dei sistemi di gestione documentale e di conservazione, interconnessi con i servizi web e i sistemi centrali (InfoCamere) su Rete gestita da InfoCamere.
Dispositivi di informatica individuale e firma digitale	Workstation, dispositivi di firma digitale, dispositivi mobili di elaborazione e di memorizzazione removibili del personale addetto alla Gestione Documentale	N/A
Immobili e infrastruttura fisica (sedi e locali, impianti)	Sede di Aosta - Regione Borgnalle, 12	CED di Padova (C.so Stati Uniti 14), Sito di Disaster Recovery di Milano (Via Viserba)
Registro di protocollo	Informazioni connesse con il Protocollo	N/A

Analisi dei Rischi									
Elemento coinvolto	Minaccia o Vulnerabilità	Descrizione minacce e vulnerabilità	Probabilità	Impatto	Rischio attuale	Contromisura	applicazione attuale %	applicazione pianificata %	Rischio Residuo - Descrizione Trattamento
Organizzazione	Errori di processo di gestione documentale e conservazione e dati non corretti. Disallineamenti o alterazioni del protocollo.	I processi di gestione documentale (i.e. classificazione, fascicolazione, inoltro, copia per immagine, metadati inseriti) e conservazione sono formalizzati e rispondenti alla realtà operativa. Il sistema di Gestione Documentale (nella Protocollazione) non consente di cambiare gli allegati dopo la protocollazione, ed è poco possibile una inconsistenza tra protocollo e documento complessivo per comportamenti dolosi o disattenzioni.	B	G	B	Formalizzazione di istruzioni tecniche per il personale.	90	100	Aggiornamento periodico della documentazione. Potenziamento della consapevolezza con un ulteriore intervento formativo organico su tutto il personale addetto in tema di sicurezza delle informazioni e privacy.
	Contenziosi, sanzioni per inadeguatezza Misure minime	L'incompleta o carente formazione in tema di Misure Minime di Sicurezza (riservatezza e cambio periodico delle password, gestione delle credenziali, backup dei dati) può esporre l'Ente al rischio di sanzioni ai sensi della normativa cogente (D.Lgs.196/03 e GDPR, Provvedimenti del Garante Privacy applicabili).	M	M	M	Il rischio residuo è legato essenzialmente alla necessità di adeguate iniziative per aumentare il livello di consapevolezza del personale, (presidio delle postazioni, custodia delle credenziali), in particolare in occasione di cambiamenti organizzativi.	85	100	Potenziamento della consapevolezza con un ulteriore intervento formativo organico su tutto il personale addetto in tema di sicurezza delle informazioni e privacy.
Personale addetto	Danni di immagine per comportamenti fraudolenti del personale	Poiché un documento potrebbe essere accidentalmente o intenzionalmente cancellato, ne consegue che il personale potrebbe essere coinvolto in un procedimento amministrativo o giudiziario; questo accadimento potrebbe provocare un danno all'immagine istituzionale dell'Ente.	B	M	B	Adozione di adeguate regole di sicurezza comunicate al personale, anche in occasione di interventi formativi.	90	100	Potenziamento della consapevolezza con un ulteriore intervento formativo organico su tutto il personale addetto in tema di sicurezza delle informazioni e privacy.
	Accessi non autorizzati ai sistemi con credenziali	Il personale potrebbe non custodire adeguatamente le proprie credenziali di accesso favorendone un uso improprio di terzi. (negligenza)	B	M	B	Disposizioni per la custodia delle credenziali che vanno mantenute riservate da parte del personale addetto.	95	100	Potenziamento della consapevolezza con un ulteriore intervento formativo organico su tutto il personale addetto in tema di sicurezza delle informazioni e privacy.
Dati (dei Sistemi, di Autenticazione e Abilitazione)	Attacco informatico alle stazioni di lavoro dell'Ente	Le postazioni di lavoro potrebbero essere infettate da malware con conseguente compromissione o indisponibilità di dati	M	G	M	La virtualizzazione delle postazioni di lavoro comprende l'esistenza di antivirus. Il personale deve prontamente segnalare gli eventuali incidenti. Il rischio residuo è legato a eventuali comportamenti poco attenti del personale addetto nell'utilizzo di posta e internet.	95	100	Potenziamento della consapevolezza con un ulteriore intervento formativo organico su tutto il personale addetto in tema di sicurezza delle informazioni e privacy. Presidio periodico delle postazioni circa la regolarità di funzionamento dell'Antivirus.
Infrastrutture IT (Server, Reti, DBMS)	Indisponibilità dei Servizi a medio - lungo termine per malfunzioni e/o indisponibilità delle risorse	In caso di malfunzioni o danneggiamenti, anche intenzionali, della infrastruttura IT, il Servizio di gestione documentale e conservazione potrebbero risultare bloccati: nel breve-medio termine (per guasti/malfunzionamenti di lieve entità) o lungo termine (in caso di evento dannoso prolungato o disastro ambientale). In caso di disastro ambientale , l'esistenza di una sola sede non consente spostamenti del personale in altri luoghi di lavoro, ma la virtualizzazione delle postazioni in VDI offre una soluzione tampone efficace, anche in caso di fermi prolungati di altra natura (quali danneggiamento o prolungata assenza di alimentazione elettrica).	B	G	B	Un Piano di emergenza - continuità operativa è predisposto da InfoCamere per la parte "core" e prevalente (asset presenti nel CED di Padova).	90	100	Informativa al personale camerale sulle modalità comportamentali da adottare qualora si verifichi l'evento. Premesso che l'accesso ai servizi è possibile via web, è opportuno adottare una procedura per far fronte all'indisponibilità delle sedi e/o delle workstation.
Dispositivi di informatica individuale e firma digitale	Accessi non autorizzati ad informazioni riservate	Le credenziali di accesso alla rete e i profili di abilitazione assegnati al personale potrebbero essere sovra/sottodimensionati rispetto alle effettive esigenze lavorative; questo accadimento provocherebbe la consultazione di informazioni riservate / l'impossibilità di utilizzare le funzionalità necessarie.	B	G	B	Revisione dei profili di abilitazione in concomitanza di cambiamenti organizzativi. Monitoraggio dei profili di abilitazione: adeguatezza dei profili.	95	100	Le abilitazioni richieste per il personale addetto ai Servizi di Gestione Documentale si rilevano non sotto/sopra/dimensionate; tuttavia è opportuna verifica periodica.
	Accessi non autorizzati alle stazioni di lavoro CCIAA	Accessi non autorizzati alle workstation, cioè durante le pause di lavoro le postazioni di lavoro potrebbero consentire l'interazione con il Sistema da parte di personale non autorizzato.	B	B	B	Disposizione e attuazione di regole di protezione della stazione di lavoro: in caso di assenza blocco delle postazioni con save screen protetto da password o spegnimento. L'inattività comporta comunque disconnessione da molti applicativi in uso.	95	100	Potenziamento della consapevolezza con un ulteriore intervento formativo organico su tutto il personale addetto in tema di sicurezza delle informazioni e privacy.
	Furto o accesso non autorizzato a dispositivi di informatica individuale (workstation, Tablet, PC portatili)	In caso di furto o utilizzo scorretto di dispositivi di elaborazione portatili (workstation, PC portatili) informazioni relative a documenti informatici potrebbero essere rubate o diffuse senza autorizzazione.	B	G	B	Le aree di lavoro della Camera sono protette contro accessi non autorizzati (porta chiusa e reception). L'utilizzo di dispositivi portatili non è normalmente previsto per gli incaricati/addetti alla Gestione Documentale. Ai dipendenti non è consentita la memorizzazione di informazioni Documentali o di Protocollo con l'uso di PC portatili al di fuori della sede. In caso di furto i dipendenti devono segnalare prontamente ai Responsabili l'incidente e si prevede un cambio della password di accesso.	95	100	Un miglioramento previsto è l'ulteriore formazione del personale, da inserire in un contesto formativo di Sicurezza e Privacy .
Immobili e infrastruttura fisica (sedi e locali, impianti)	Accessi non autorizzati ai locali	In caso di accessi non autorizzati agli immobili ed ai locali in cui vengono svolte attività operative inerenti i Servizi di Protocollo e Gestione Documentale possono verificarsi danneggiamenti e utilizzi impropri dei sistemi e degli apparati.	B	G	B	E' controllato l'accesso alla sede.Documenti cartacei danneggiabili restano presenti nei locali del Protocollo in numero estremamente ridotto. Rischio Marginale.	95	100	Richiamo periodico a tutto il personale coinvolto a comportamenti sicuri.