Camera di commercio di Torino

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 CCIAA di TORINO	Asset Individuati per InfoCamere (x Servizi erogati alla CCIAA)
Organizzazione	Camera di commercio di Torino	InfoCamere
Personale coinvolto	Addetti al Sistema di Gestione Documentale (GEDOC) e Addetti al Sistema di Conservazione a norma (CNIP-FOR)	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 CCIAA, Profili di abilitazioni del Personale, Credenziali del Personale	Dati (i documenti della CCIAA) conservati nei DB 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) dislocati nelle sedi CCIAA, Rete IC in CCIAA, Server di memorizzazione presenti nelle sedi CCIAA 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 ed alla Conservazione	N/A
Immobili e infrastruttura fisica (sedi e locali, impianti)	Sedi CCIAA di Torino (Palazzo Affari, Palazzo Birago, via Pomba 23, via Giolitti 15)	CED di Padova (C.so Stati Uniti 14), Sito di Disaster Revovery di Milano (Via Viserba)
Registro di protocollo	Informazioni connesse con il Protocollo	N/A

Analisi dei Rischi

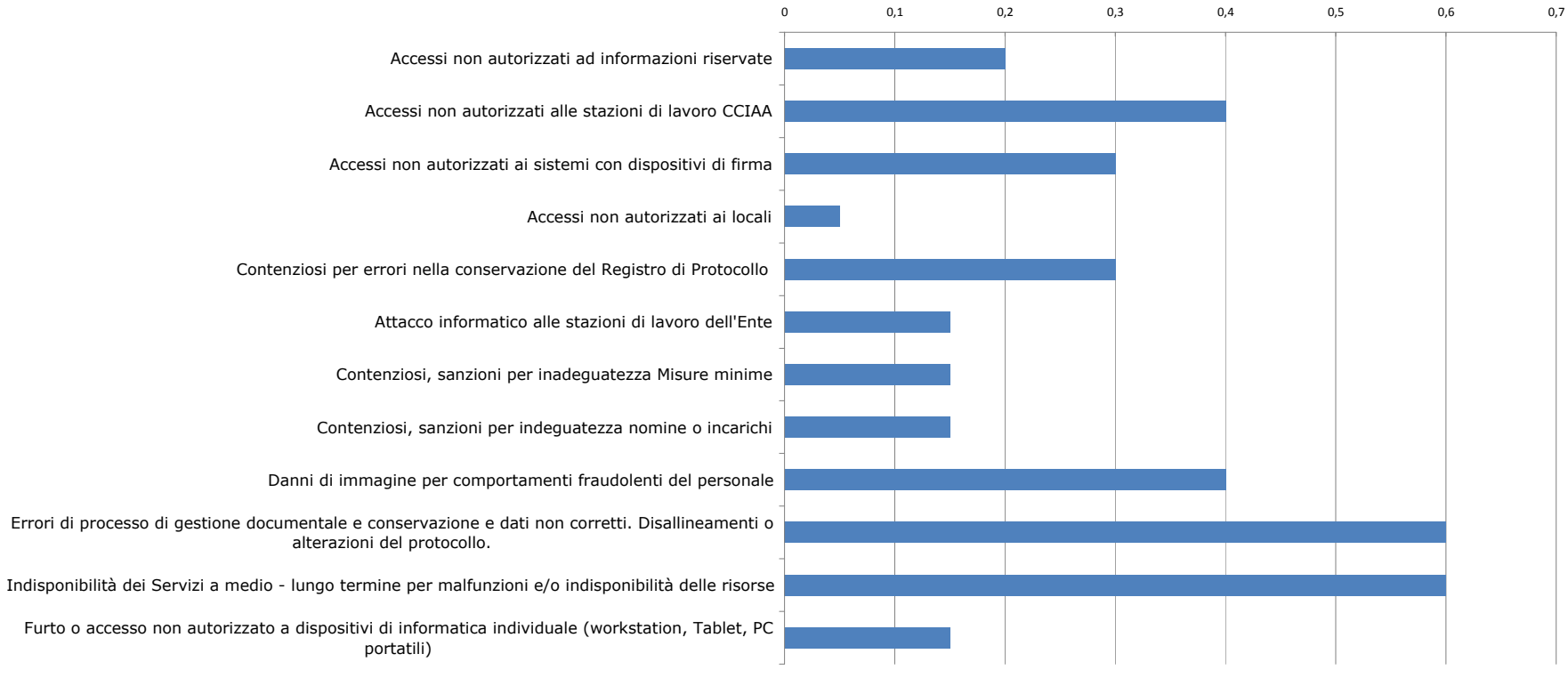
Asset	Minaccia o Vulnerabilità	Descrizione minacce e vulnerabilità	Probabilità (P)	Impatto (I)	Rischio attuale (P x I)	Contromisura	applicazione attuale %	applicazione pianificata %	Rischio Residuo - Descrizione Trattamento	Rischio Residuo
Organizzazione	Contenziosi, sanzioni per indeguatezza nomine o incarichi	La formulazione carente o errata degli incarichi al personale e delle nomine ai fornitori potrebbe portare a impatti normativi ed esporre la CCIAA al rischio di sanzioni.	**2**	**4**	**3**	Formalizzazione di incarichi al personale e fornitori con riferimento ai trattamenti consentiti ed alle misure di sicurezza da adottare nel trattamento, in particolare in occasione di cambiamenti organizzativi.	95	100	Adozione di un sistema di formalizzazione degli incarichi, alternativo al D.P.S. non più aggiornato. Verifica sistematica e puntuale degli eventi.	**0,15**
	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 incoerenti con le registrazioni di protocollo) e conservazione sono poco formalizzati o scarsamente rispondenti alla realtà operativa. Inoltre, il sistema di Gestione Documentale (nella Protocollazione) consente di cambiare gli allegati dopo la protocollazione, è possibile una inconsistenza tra protocollo e documento complessivo per comportamenti dolosi o disattenzioni.	**4**	**4**	**4**	Formalizzazione di istruzioni tecniche per il personale. Valutare l'opportunità di modifiche al sistema per 'blindare' il documento dopo la sua protocollazione ovvero un alert al responsabile.	85	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.	**0,6**
	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 Provvedimenti del Garante Privacy applicabili).	**2**	**4**	**3**	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.	95	100	Potenziamento della consapevolezza con un ulteriore intervento formativo organico su tutto il personale addetto in tema di sicurezza delle informazioni e privacy.	**0,15**
Personale coinvolto	Danni di immagine per comportamenti fraudolenti del personale	Poiché un documento potrebbe essere accidentalmente o intenzionalmente cancellato o sostituito, 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.	**3**	**4**	**4**	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. Verificare che la soluzione proposta soddisfi ai requisiti di tracciatura delle operazioni.	**0,4**
	Accessi non autorizzati ai sistemi con dispositivi di firma	Il personale potrebbe non custodire adeguatamente i dispositivi di firma e il PIN favorendone un uso improprio di terzi. (negligenza)	**2**	**5**	**3**	Disposizioni per la custodia dei dispositivi di firma e lavoro in aree sicure; il PIN va mantenuto riservato da parte del personale addetto.	90	100	Potenziamento della consapevolezza con un ulteriore intervento formativo organico su tutto il personale addetto in tema di sicurezza delle informazioni e privacy.	**0,3**
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	**2**	**4**	**3**	Il sistema antivirus, gestito su server CCIAA, attivo su tutte le stazioni di lavoro, è aggiornato automaticamente e non deve essere disattivato. 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.	**0,15**
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**, essendo le sedi camerali a breve distanza fra esse, e quindi soggetti a rischi analoghi, l'Ente valuterà l'opportunità di eventuali spostamenti del personale in altre sedi (non camerali), tenendo comunque in considerazione che le dotazioni di dispositivi mobili e l'architettura di rete possono offrire soluzioni tampone efficaci. In caso di **fermi prolungati** di altra natura (quali danneggiamento o prolungata assenza di alimentazione elettrica), l'Ente valuterà l'opportunità di uno spostamento di personale tra le sedi camerali disponibili, sfruttando la flessibilità e ridondanza di postazioni. Se un evento disastroso (naturale o doloso) impattasse solo sulla sede di **Palazzo Affari,** sede	**2**	**5**	**3**	Un Piano di emergenza - continuità operativa è predisposto da InfoCamere per la parte "core" e prevalente (asset presenti nel CED di Padova).	80	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, anche ricorrendo al *mobile* .	**0,6**
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.	**3**	**4**	**4**	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 e Conservazione si rilevano non sotto/sopra/dimensionate; tuttavia è opportuna verifica periodica, almeno annuale.	**0,2**
	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.	**4**	**4**	**4**	Disposizione e attuazione di regole di protezione della stazione di lavoro: in caso di assenza blocco delle postazioni con save screen protetto da password.	90	100	Potenziamento della consapevolezza con un ulteriore intervento formativo organico su tutto il personale addetto in tema di sicurezza delle informazioni e privacy.	**0,4**
	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, Tablet) informazioni relative a documenti informatici potrebbero essere rubate o diffuse senza autorizzazione, potrebbe verificarsi un utilizzo scorretto delle credenziali di accesso alla rete informatica.	**3**	**3**	**3**	Le aree di lavoro della CCIAA sono protette contro accessi non autorizzati (servizio di porteneria e di allarme). L'utilizzo di dispositivi portatili non è normalmente previsto per gli incaricati/addetti alla Gestione Documentale ed alla Conservazione. Ai dipendenti è vietata la memorizzazione di informazioni Documentali o di Protocollo con l'uso di PC portatili al di fuori delle sedi CCIAA. Sono comunque impartite istruzioni per la loro attenta custodia in caso di trasporto al di fuori delle sedi. 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 e, da valutare, la cifratura automatica di alcune aree dati del PC.	**0,15**
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 operartive inerenti i Servizi di Protocollo e Gestione Documentale possono verificarsi danneggiamenti e utilizzi impropri dei sistemi e degli apparati.	**1**	**2**	**1**	E' controllato l'accesso agli immobili. Accessi promiscui al Protocollo sono evitati dalla dislocazione in locali separati e distinti ed è presente un servizio di guardia all'esterno; documenti cartacei danneggiabili restano presenti nei locali del Protocollo in numero estremamento ridotto sino alla completa dematerizziazione. Rischio Marginale.	95	100	Richiamo periodico a tutto il personale coinvolto a comportamenti sicuri e, nel caso del Protocollo, celere completamento della dematerializzazione.	**0,05**
Registro di protocollo	Contenziosi per errori nella conservazione del Registro di Protocollo	Il Registro di Protocollo andrebbe inviato giornalmente in conservazione. La configurazione della CCIAA attuale lascia il compito al Responsabile del Protocollo, anziché, come peraltro possibile, automatizzarlo.	**2**	**4**	**3**	Pronta segnalazione degli incidenti da parte del personale addetto. Automazione dell'invio.	90	100	Automazione dell'invio in valutazione. Non vi sono marcati rischi di compliance.	**0,3**

Il calcolo del rischio e rischio residuo è normalizato sulla scala 0:1.

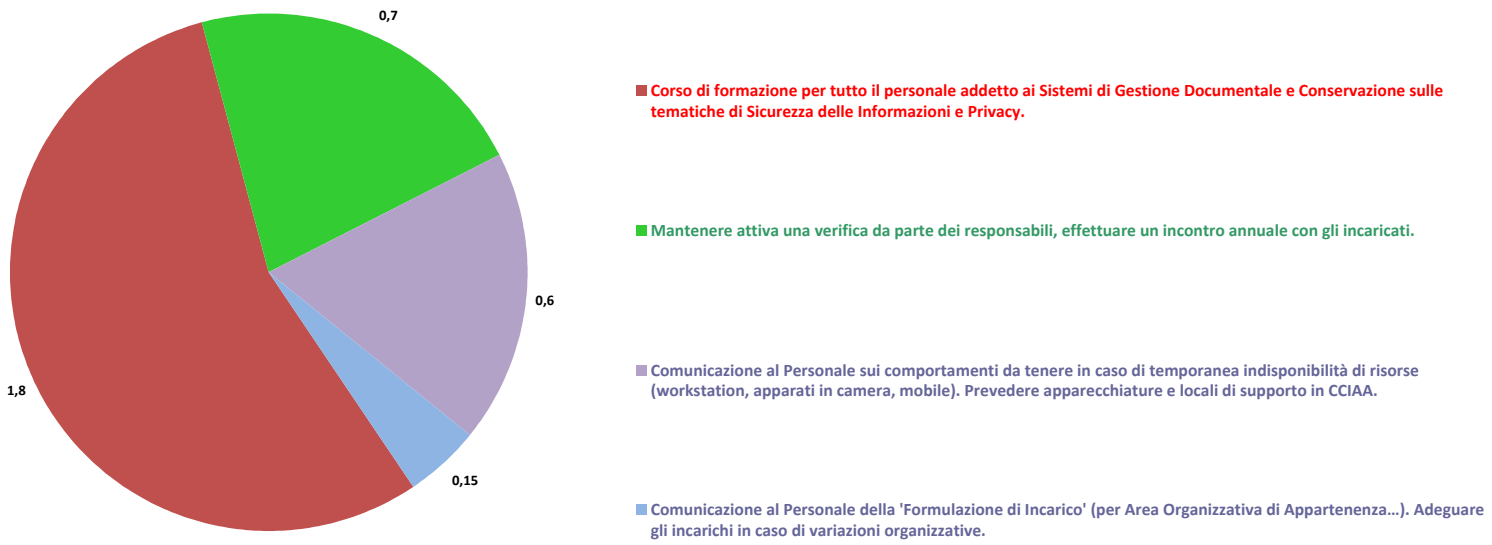
Piano di Trattamento del Rischio

Minaccia o Vulnerabilità	Rischio Residuo (contromisura R.R.)	Valore R.R.	Ulteriore trattamento del Rischio	ID. Piano	Responsabile attività	Entro
Accessi non autorizzati ad informazioni riservate	Revisione dei profili di abilitazione in concomitanza di cambiamenti organizzativi. Monitoraggio dei profili di abilitazione: adeguatezza dei profili.	0,2	Mantenere attiva una verifica da parte dei responsabili, effettuare un incontro annuale con gli incaricati.	1		N/A
Accessi non autorizzati ai locali	E' controllato l'accesso agli immobili. Accessi promiscui al Protocollo sono evitati dalla dislocazione in locali separati e distinti ed è presente un servizio di guardia all'esterno; documenti cartacei danneggiabili restano presenti nei locali del Protocollo in numero estremamento ridotto sino alla completa dematerizziazione. Rischio Marginale.	0,05	Mantenere attiva una verifica da parte dei responsabili, effettuare un incontro annuale con gli incaricati.	1		N/A
Attacco informatico alle stazioni di lavoro dell'Ente	Il sistema antivirus, gestito su server CCIAA, attivo su tutte le stazioni di lavoro, è aggiornato automaticamente e non deve essere disattivato. 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.	0,15	Mantenere attiva una verifica da parte dei responsabili, effettuare un incontro annuale con gli incaricati.	1		N/A
Contenziosi per errori nella conservazione del Registro di Protocollo	Pronta segnalazione degli incidenti da parte del personale addetto. Automazione dell'invio.	0,3	Mantenere attiva una verifica da parte dei responsabili, effettuare un incontro annuale con gli incaricati.	1		N/A
Accessi non autorizzati alle stazioni di lavoro CCIAA	Disposizione e attuazione di regole di protezione della stazione di lavoro: in caso di assenza blocco delle postazioni con save screen protetto da password.	0,4	Corso di formazione per tutto il personale addetto ai Sistemi di Gestione Documentale e Conservazione sulle tematiche di Sicurezza delle Informazioni e Privacy.	2		15-ott-17
Accessi non autorizzati ai sistemi con dispositivi di firma	Disposizioni per la custodia dei dispositivi di firma e lavoro in aree sicure; il PIN va mantenuto riservato da parte del personale addetto.	0,3	Corso di formazione per tutto il personale addetto ai Sistemi di Gestione Documentale e Conservazione sulle tematiche di Sicurezza delle Informazioni e Privacy.	2		15-ott-17
Contenziosi, sanzioni per inadeguatezza Misure minime	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.	0,15	Corso di formazione per tutto il personale addetto ai Sistemi di Gestione Documentale e Conservazione sulle tematiche di Sicurezza delle Informazioni e Privacy, richiami formativi in occasione di variazioni organizzative.	2		15-ott-17
Danni di immagine per comportamenti fraudolenti del personale	Adozione di adeguate regole di sicurezza comunicate al personale, anche in occasione di interventi formativi.	0,4	Corso di formazione per tutto il personale addetto ai Sistemi di Gestione Documentale e Conservazione sulle tematiche di Sicurezza delle Informazioni e Privacy, richiami formativi in occasione di variazioni organizzative.	2		15-ott-17
Errori di processo di gestione documentale e conservazione e dati non corretti. Disallineamenti o alterazioni del protocollo.	Formalizzazione di istruzioni tecniche per il personale. Valutare l'opportunità di modifiche al sistema per 'blindare' il documento dopo la sua protocollazione ovvero un alert al responsabile.	0,4	Corso di formazione per tutto il personale addetto ai Sistemi di Gestione Documentale e Conservazione sulle tematiche di Sicurezza delle Informazioni e Privacy, richiami formativi in occasione di variazioni organizzative.	2		15-ott-17
Furto o accesso non autorizzato a dispositivi di informatica individuale (workstation, Tablet, PC portatili)	Le aree di lavoro della CCIAA sono protette contro accessi non autorizzati (servizio di porteneria e di allarme). L'utilizzo di dispositivi portatili non è normalmente previsto per gli incaricati/addetti alla Gestione Documentale ed alla Conservazione. Ai dipendenti è vietata la memorizzazione di informazioni Documentali o di Protocollo con l'uso di PC portatili al di fuori delle sedi CCIAA. Sono comunque impartite istruzioni per la loro attenta custodia in caso di trasporto al di fuori delle sedi. In caso di furto i dipendenti devono segnalare prontamente ai Responsabili l'incidente e si prevede un cambio della password di accesso.	0,15	Corso di formazione per tutto il personale addetto ai Sistemi di Gestione Documentale e Conservazione sulle tematiche di Sicurezza delle Informazioni e Privacy, richiami formativi in occasione di variazioni organizzative.	2		15-ott-17
Contenziosi, sanzioni per indeguatezza nomine o incarichi	Formalizzazione di incarichi al personale e fornitori con riferimento ai trattamenti consentiti ed alle misure di sicurezza da adottare nel trattamento, in particolare in occasione di cambiamenti organizzativi.	0,15	Comunicazione al Personale della 'Formulazione di Incarico' (per Area Organizzativa di Appartenenza…). Adeguare gli incarichi in caso di variazioni organizzative.	3		15-mar-17
Indisponibilità dei Servizi a medio - lungo termine per malfunzioni e/o indisponibilità delle risorse	Un Piano di emergenza - continuità operativa è predisposto da InfoCamere per la parte "core" e prevalente (asset presenti nel CED di Padova).	0,6	Comunicazione al Personale sui comportamenti da tenere in caso di temporanea indisponibilità di risorse (workstation, apparati in camera, mobile). Prevedere apparecchiature e locali di supporto in CCIAA.	4		15-mar-17

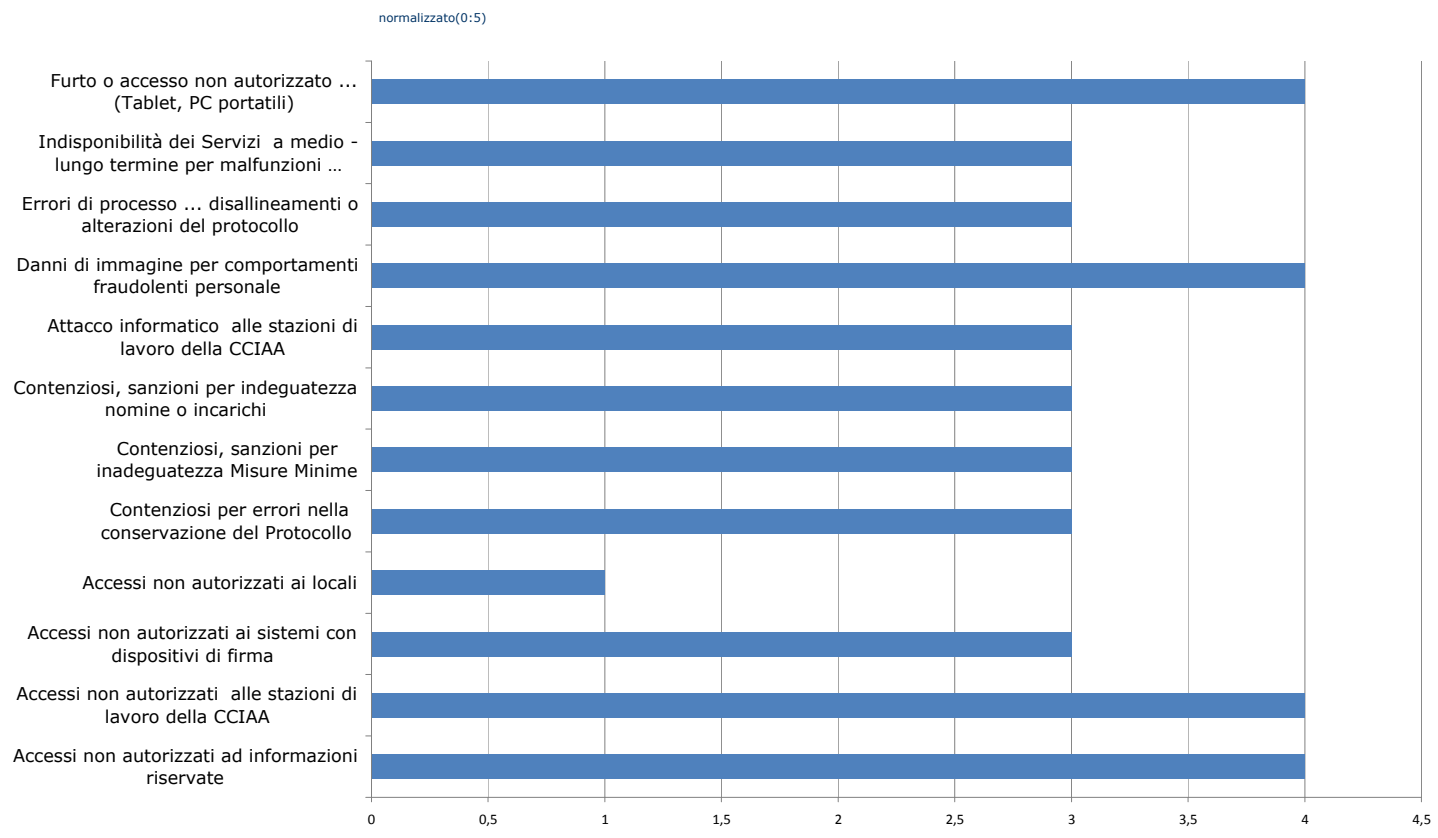
Rischio Residuo



Rischio Residuo coperto per Piano di Trattamento



Rischio intrinseco (P x I)



Linee Guida e Tabelle di codifica utilizzate

Linea GUIDA: Calcolare il rischio "intrinseco" che ogni minaccia o vulnerabilità comporta per l'asset; tale rischio esiste indipendentemente dalle contromisure applicate: rischio intrinseco = probabilità X impatto. Nel caso di scala "mB / B / M / A / mA" utilizzare la seguente tabella che associa ai valori di probabilità e impatto il corrispondente valore di rischio:

Probabilità x Impatto	***Rischio***
mB.mB	*Basso*
mB.B	*Basso*
mB.M	*Basso*
mB.A	*Basso*
mB.mA	*Medio*
B.mB	*Basso*
B.B	*Basso*
B.M	*Medio*
B.A	*Medio*
B.mA	*Alto*
M.mB	*Basso*
M.B	*Medio*
M.M	*Medio*
M.A	*Alto*
M.mA	*Altissimo*
A.mB	*Basso*
A.B	*Medio*
A.M	*Medio*
A.A	*Alta*
A.mA	*Altissimo*
mA.mB	*Medio*
mA.B	*Medio*
mA.M	*Alto*
mA.A	*Altissimo*
mA.mA	*Altissimo*

Linea GUIDA: Calcolo rischio "residuo": rischio che permane considerando l'efficacia delle contromisure in essere.Per il calcolo utilizzare una tabella simile alla seguente:

rischio intrinseco	*grado di copertura*	*rischio residuo*
Altissimo	*100%*	*Basso*
Alto	*100%*	*Basso*
Medio	*100%*	*Basso*
Basso	*100%*	*Basso*
Altissimo	*parziale*	*da valutare caso per caso*
Alto	*parziale*	*da valutare caso per caso*
Medio	*parziale*	*da valutare caso per caso*
Basso	*parziale*	*da valutare caso per caso*
Altissimo	*0%*	*Altissimo*
Alto	*0%*	*Alto*
Medio	*0%*	*Medio*
Basso	*0%*	*Basso*

Tabelle di codifica utilizzate riportando i valori a numerici - normalizzazione dei valori (1:5)

Probalità X Impatto valori	RISK VALUES	Probabilità per impatto significato	Significato
1	1	***mB.mB***	***Basso***
2	1	***mB.B***	***Basso***
3	2	***mB.M***	***Basso***
4	2	***mB.A***	***Basso***
5	2	***mB.mA***	***Medio***
6	2	***B.mB***	***Basso***
7	2	***B.B***	***Basso***
8	3	***B.M***	***Medio***
9	3	***B.A***	***Medio***
10	3	***B.mA***	***Alto***
11	4	***M.mB***	***Basso***
12	4	***M.B***	***Medio***
13	4	***M.M***	***Medio***
14	4	***M.A***	***Alto***
15	4	***M.mA***	***Altissimo***
16	4	***A.mB***	***Basso***
17	5	***A.B***	***Medio***
18	5	***A.M***	***Medio***
19	5	***A.A***	***Alta***
20	5	***A.mA***	***Altissimo***
21	5	***mA.mB***	***Medio***
22	5	***mA.B***	***Medio***
23	5	***mA.M***	***Alto***
24	5	***mA.A***	***Altissimo***
35	5	***mA.mA***	

Tabelle di codifica utilizzate riportando i valori a numerici - normalizzazione dei valori (1:5)

% copertura del Rischio Intrinseco (efficacia delle contromisure)	Significato Valori di Probabilità e Impatto Minaccia - Normalizzato (5 valori)	Probabilità Minaccia	Rischio Intrinseco	Valore di Rischio
90-100	Altissimo	5	>16	5
70-90	Alto	4	11:16	4
60-70	MedioAlto	3	5:10	3
30-60	Medio_Basso	2	3:4	2
1-30	Basso_MoltoBasso	1	1:2	1

Diagramma valori risultante

Probabilità x Impatto	5	4	2	1	1
5	***25***	*20*	10	5	5
4	*20*	*16*	8	4	4
3	15	12	6	3	3
2	10	8	4	2	2
1	5	4	2	1	1
1	5	4	2	1	1