Piano della Sicurezza dei documenti informatici

Versione 1
Allegato al Regolamento Privacy

Redatto: VR Solutions srl

Validato: ISIA Roma Design

Roma 21.09.2018

Indice

1 INTRODUZIONE AL DOCUMENTO 3
1.1 Scopo e campo di applicazione del documento 3
1.2 Livello di riservatezza 3
1.3 Precedenti emissioni 3
1.4 Riferimenti normativi 4
1.5 Riferimenti documentali 4
1.6 Termini e definizioni 4

2 ORGANIZZAZIONE DELLA SICUREZZA DELLE INFORMAZIONI 5
2.1 Analisi del rischio IT 5
2.2 Formazione del Personale 10
2.3 Continuità operativa 11
2.3.1 Continuità operativa del Servizio 11
2.3.2 Continuità Operativa del Sistema 11
2.4 Ripristino del Servizio 11
2.5 Livelli di servizio 11
2.6 Comunicazione con il fornitore apposita Ditta 12
2.7 Monitoraggio dell'infrastruttura IT 12
2.7.1 Procedure operative 12
2.7.2 Strumenti 12
2.7.3 Gestione dei log 12

3 POLITICHE DI SICUREZZA 13
3.1 Politica di gestione della sicurezza dei sistemi 13
3.1.1 Inventario degli asset IT 13
3.1.2 Installazione dei sistemi 13
3.1.3 Resource Capacity Management 14
3.1.4 Configurazione dei sistemi 14
3.1.5 Backup 14
3.1.6 Amministratori di Sistema 14
3.2 Politica per l'inserimento dell'utenza e per il controllo degli accessi logici 15
3.2.1 Gestione delle credenziali di accesso 15
3.2.2 Utilizzo delle password 16
3.2.3 Responsabilità degli utenti 16
3.2.4 Servizi informatici forniti da apposita Ditta 16
aggiornamenti del software 17
limitazione della connettività a supporti esterni 17
modifica delle impostazioni 17
configurazione delle postazioni di lavoro 17
3.3 Politica di gestione, dismissione e smaltimento degli apparati mobili e dei supporti 17
3.4 Politica di protezione dal malware 18

1 INTRODUZIONE AL DOCUMENTO

1.1 Scopo e campo di applicazione del documento

Il Piano di sicurezza garantisce che:

- i documenti e le informazioni trattati dalla AOO (Aerea Organizzativa Omogenea) siano resi disponibili, integri e riservati;
- i dati personali comuni, sensibili e/o giudiziari vengano custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, 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 presente documento chiarisce la gestione informatica del dato in seguito agli adempimenti derivati dalla normativa vigente e dal regolamento privacy adottato .

1.2 Livello di riservatezza

	Livello	Ambito di diffusione consentito
	Pubblico	Il documento può essere diffuso **all'esterno** dell'ISIA.
	Uso interno	Il documento può essere diffuso solo **all'interno** dell'ISIA. E' consentito darne comunicazione a Terzi con clausola di non diffusione.
	Riservato	Il documento **non può essere diffuso** all'interno dell'ISIA La sua visibilità è limitata ad un gruppo ristretto di Persone. L'indicazione "Riservato" DEVE essere riportata anche nel Piè-di-pagina del documento.

1.3 Precedenti emissioni

Prima emissione

Versione:	n. 1	Data Versione:	21/09/2018
Descr. modifiche:	Non Applicabile		
Motivazioni :	Non Applicabile		

1.4 Riferimenti normativi

CAD CO	Codice dell'Amministrazione Digitale, Decreto legislativo 7 marzo 2005, n. 82, art. 50 bis
LG AGID DR	Linee Guida AgID per la disaster recovery delle Pubbliche Amministrazioni - ai sensi del comma 3, lettera b) dell'art. 50bis del Codice dell'Amministrazione Digitale (aggiornamento 2013)
TESTO UNICO	Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa

1.5 Riferimenti documentali

CAD CO	Codice dell'Amministrazione Digitale, Decreto legislativo 7 marzo 2005, n. 82, art. 50 bis
LG AGID DR	Linee Guida AgID per la disaster recovery delle Pubbliche Amministrazioni - ai sensi del comma 3, lettera b) dell'art. 50bis del Codice dell'Amministrazione Digitale (aggiornamento 2013)
MANUALE	Manuale di Gestione documentale dell'ISIA
MCF CLIENT	Configurazione della postazione di lavoro
TESTO UNICO	Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa

1.6 Termini e definizioni

SGQ	Sistema di Gestione della Qualità

2 ORGANIZZAZIONE DELLA SICUREZZA DELLE INFORMAZIONI

La conversione del Decreto Legge n. 5 del 9 febbraio 2012 (c.d. Decreto semplificazioni), avvenuta con la Legge 4 aprile 2012 n. 35, conferma definitivamente la soppressione dell'obbligo – in capo ai Titolari di trattamento di dati sensibili e giudiziari effettuato mediante strumenti elettronici – di redigere, e quindi di tenere aggiornato, il Documento Programmatico sulla Sicurezza (DPS). I Titolari del trattamento sono, tuttavia, ancora tenuti ad osservare tutti gli accorgimenti tecnici e organizzativi idonei a garantirne protezione, privacy e riservatezza.

2.1 Analisi del rischio IT

Individuazione degli asset

asset	descrizione
Personale coinvolto	utenti del Sistema
servizio	il Servizio di Gestione Documentale offerto agli Utenti
documenti	documenti gestiti dal Sistema
dati personali	dati personali presenti nei documenti, registrazioni di protocollo, metadati
metadati relativi alle registrazioni di protocollo ed ai documenti	informazioni associate a documenti e fascicoli informatici tramite l'adozione di regole, procedure e tecnologie idonee a garantirne le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità.
registro di protocollo	registro su cui si annota in ordine cronologico la corrispondenza in arrivo e in partenza
credenziali di accesso	identificativo di accesso, profilo di abilitazione associato, password
processi di gestione documentale	processi e attività di gestione della protocollazione e dei flussi documentali
processi: protocollazione	attribuzione al documento di un numero progressivo
processi: classificazione	attribuzione al documento della classifica prevista dal titolario di archivio
processi: fascicolazione	inserimento del documento in un fascicolo informatico
processi: inoltro	assegnazione del documento all'Ufficio competente
processi: copia per immagine su supporto informatico di documenti analogici	inserimento nel sistema informatico di un documento analogico tramite scansione e attestazione di conformità all'originale cartaceo
infrastruttura IT	infrastruttura tecnologica che ospita il Sistema
postazioni di lavoro	personal computer / altri apparati mobili tramite i quali gli Utenti accedono al sistema
dispositivi di firma	dispositivi di firma digitale

Analisi delle minacce e vulnerabilità

Le minacce e vulnerabilità che insistono sugli asset sono:

asset	minacce e vulnerabilità	P (probabilità)	I (impatto)
Personale coinvolto	Poiché il Sistema informatico è di recente adozione, ne consegue che il Personale potrebbe incontrare difficoltà nell'utilizzo e questo accadimento provocherebbe una perdita di efficienza e di motivazione all'utilizzo.	M	A
	Poiché il Sistema informatico è di recente adozione, ne consegue che i profili di abilitazione assegnati al Personale potrebbero essere sovra /sottodimensionati rispetto alle esigenze lavorative; questo accadimento provocherebbe la consultazione di informazioni riservate / impossibilità di utilizzare le funzionalità necessarie.	M	A
documenti	Poiché la classificazione e fascicolazione dei documenti è un'operazione complessa, ne consegue che un documento potrebbe venir fascicolato in modo non corretto e questo accadimento provocherebbe difficoltà nelle successive ricerche.	M	M
	Poiché un documento potrebbe essere accidentalmente / 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'ISIA.	mB	mA
dati personali	Poiché il Sistema informatico è di recente adozione, ne consegue che i profili di abilitazione assegnati al Personale potrebbero essere sovradimensionati rispetto alle esigenze lavorative; questo accadimento provocherebbe la consultazione di informazioni personali da parte di Personale non incaricato.	M	mA
metadati relativi alle registrazioni di protocollo ed ai documenti	i metadati inseriti potrebbero essere incoerenti con le registrazioni di protocollo o i documenti archiviati	mB	A
registro di protocollo	il registro di protocollo potrebbe risultare danneggiato	mB	mA
	il registro di protocollo potrebbe venire alterato	mB	mA
credenziali di accesso	le credenziali potrebbero diventare non allineate alle effettive necessità	B	B
processi di gestione documentale	i processi di gestione documentale potrebbero essere poco conosciuti al Personale	B	A
processi: protocollazione	un eventuale malfunzionamento del sistema può ritardare la protocollazione dei documenti	M	M
processi: classificazione	un errore di classificazione può incidere sui tempi di conservazione di un fascicolo/documento	M	mA

processi: fascicolazione	la fascicolazione non corretta di un documento provocherebbe difficoltà nelle successive ricerche	M	M
processi: inoltro	l'inoltro non corretto può creare disguidi e rallentare l'attività lavorativa	M	B
processi: copia per immagine su supporto informatico di documenti analogici	una errata scansione fa sì che il documento informatico non sia leggibile, ma il sistema prevede l'attestazione della conformità del file al documento analogico e quindi un controllo	mB	mB
processi	nel tempo i processi di gestione documentale potrebbero discostarsi dalle prassi effettive	B	M
infrastruttura IT	Poiché l'infrastruttura IT potrebbe essere coinvolta da malfunzionamenti, ne consegue che il Servizio di gestione documentale potrebbe essere non disponibile e questo accadimento provocherebbe un blocco dei processi.	M	A
	poiché potrebbe accadere un evento disastroso nel sito di erogazione dei servizi di apposita Ditta, ne consegue che l'infrastruttura IT potrebbe venire distrutta e questo accadimento provocherebbe l'indisponibilità del servizio per un lunghissimo periodo.	mB	mA
postazioni di lavoro	le postazioni di lavoro potrebbero essere infettate da malware	M	mA
	durante le pause di lavoro le postazioni di lavoro potrebbero consentire l'interazione con il Sistema da parte di Personale non autorizzato	M	A
	le postazioni di lavoro potrebbero essere inadeguate rispetto alle caratteristiche richieste dal Sistema	mB	M
dispositivi di firma	il dispositivo di firma può non funzionare impedendo la firma del documento in tempo utile	M	mA

Individuazione delle contromisure

asset	minacce e vulnerabilità	contromisure	grado di copertura
Personale coinvolto	Poiché il Sistema informatico è di recente adozione, ne consegue che il Personale potrebbe incontrare difficoltà nell'utilizzo e questo accadimento provocherebbe una perdita di efficienza e di motivazione all'utilizzo.	- Piano di formazione adeguato - Incontri individuali con il Personale che ne manifesti la necessità per raccogliere le problematiche e individuare soluzioni condivise	100%
	Poiché il Sistema informatico è di recente adozione, ne consegue che i profili di abilitazione assegnati al Personale potrebbero essere sovra / sottodimensionati rispetto alle esigenze lavorative; questo accadimento provocherebbe la consultazione di informazioni riservate / l'impossibilità di utilizzare le funzionalità necessarie.	- Verifica periodica dell'adeguatezza dei profili (anche intervistando il Personale)	100%

asset	minacce e vulnerabilità	contromisure	grado di copertura
documenti	Poiché la classificazione e fascicolazione dei documenti è un'operazione complessa, ne consegue che un documento potrebbe venir classificato e fascicolato in modo non corretto e questo accadimento provocherebbe difficoltà nelle successive ricerche.	- Piano di formazione adeguato - Incontri individuali con i responsabili ufficio per raccogliere le problematiche e individuare soluzioni condivise	100%
	Poiché un documento potrebbe essere accidentalmente / 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'ISIA.	- Verifica della tracciatura delle operazioni	100%
dati personali	Poiché il Sistema informatico è di recente adozione, ne consegue che i profili di abilitazione assegnati al Personale potrebbero essere sovradimensionati rispetto alle esigenze lavorative; questo accadimento provocherebbe la consultazione di informazioni personali da parte di Personale non incaricato.	- Verifica periodica dell'adeguatezza dei profili (anche intervistando il Personale)	100%
infrastruttura IT	Poiché l'infrastruttura IT potrebbe essere coinvolta da malfunzionamenti, ne consegue che il Servizio di gestione documentale potrebbe essere non disponibile e questo accadimento provocherebbe un blocco dei processi.	- Verifica del livello di disponibilità garantito da apposita Ditta per il Sistema di gestione documentale	100%
	Poiché potrebbe accadere un evento disastroso nel sito di erogazione dei servizi di apposita Ditta, ne consegue che l'infrastruttura IT potrebbe venire distrutta e questo accadimento provocherebbe l'indisponibilità del servizio per un lunghissimo periodo.	- Verifica che il Sistema di gestione documentale sia inserito nella soluzione di Disaster Recovery di apposita Ditta	100%

Calcolo del Rischio

asset	minacce e vulnerabilità	rischio intrinseco	rischio residuo
Personale coinvolto	Poiché il Sistema informatico è di recente adozione, ne consegue che il Personale potrebbe incontrare difficoltà nell'utilizzo e questo accadimento provocherebbe una perdita di efficienza e di motivazione all'utilizzo.	Alto	Basso
	Poiché il Sistema informatico è di recente adozione, ne consegue che i profili di abilitazione assegnati al Personale potrebbero essere sovra / sottodimensionati rispetto alle esigenze lavorative; questo accadimento provocherebbe la consultazione di informazioni riservate / l'impossibilità di utilizzare le funzionalità necessarie.	Alto	Alto
documenti	Poiché la classificazione e fascicolazione dei documenti è un'operazione complessa, ne consegue che un documento potrebbe venir classificato e fascicolato in modo non corretto e questo accadimento provocherebbe difficoltà nelle successive ricerche.	Medio	Basso
	Poiché un documento potrebbe essere accidentalmente / 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'ISIA.	Medio	Basso
dati personali	Poiché il Sistema informatico è di recente adozione, ne consegue che i profili di abilitazione assegnati al Personale potrebbero essere sovradimensionati rispetto alle esigenze lavorative; questo accadimento provocherebbe la consultazione di informazioni personali da parte di Personale non incaricato.	Altissimo	Altissimo
infrastruttura IT	Poiché l'infrastruttura IT potrebbe essere coinvolta da malfunzionamenti, ne consegue che il Servizio di gestione documentale potrebbe essere non disponibile e questo accadimento provocherebbe un blocco dei processi.	Alto	Basso

	Poiché potrebbe accadere un evento disastroso nel sito di erogazione dei servizi di apposita Ditta, ne consegue che l'infrastruttura IT potrebbe venire distrutta e questo accadimento provocherebbe l'indisponibilità del servizio per un lunghissimo periodo.	Medio	Basso

Trattamento del rischio residuo

asset	minacce e vulnerabilità	rischio residuo	strategia di risposta	azione di trattamento
Personale coinvolto	Poiché il Sistema informatico è di recente adozione, ne consegue che il Personale potrebbe incontrare difficoltà nell'utilizzo	Basso	Accettazione	Formazione mirata sulla base delle difficoltà manifestate
	Poiché il Sistema informatico è di recente adozione, ne consegue che i profili di abilitazione assegnati al Personale potrebbero essere sovra / sottodimensionati	Alto	Mitigazione	Sei mesi dopo l'avvio verifica dell'adeguatezza dei profili (anche intervistando il Personale e i Responsabili). Successivamente, verifica annuale.
documenti	Poiché la classificazione e fascicolazione dei documenti è un'operazione complessa il Personale potrebbe incorrere in errore	Basso	Accettazione	Controllo da parte dei responsabili ufficio
	Poiché un documento potrebbe essere accidentalmente intenzionalmente cancellato o sostituito. Tuttavia il sistema ne mantiene traccia.	Basso	Accettazione	Controllo da parte dei responsabili ufficio
dati personali	Poiché il Sistema informatico è di recente adozione, ne consegue che i profili di abilitazione assegnati al Personale potrebbero essere sovradimensionati ...	Altissimo	Rimozione	Sei mesi dopo l'avvio, verifica dell'adeguatezza dei profili (anche intervistando il Personale e i Responsabili). In seguito, verifica annuale.
infrastruttura IT	L'infrastruttura IT potrebbe essere coinvolta da malfunzionamenti ...	Basso	Accettazione	Si individuano soluzioni condivise con i Fornitori dei servizi
	Poiché potrebbe accadere un evento disastroso nel sito di erogazione dei servizi di apposita Ditta	Basso	Accettazione	Si individuano soluzioni condivise

2.2 Formazione del Personale

Con riferimento al Piano di Formazione del Personale, relativamente alla Gestione Documentale Informatica del dato Personale, l'ISIA garantisce che:

- le iniziative di formazione/aggiornamento siano finalizzate al mantenimento e sviluppo del patrimonio delle conoscenze dell'ISIA in un'ottica di formazione continua in grado di recepire le esigenze formative e le evoluzioni normative, istituzionali e tecnologiche;
- la formazione di ogni Persona avvenga sulla base di una pianificazione che tenga conto del percorso formativo seguito, della figura professionale di appartenenza e quindi delle attività che la Persona svolge o dovrà svolgere oltreché delle competenze e potenzialità espresse.

La formazione viene pianificata ed attuata, di concerto con il Responsabile della Gestione Documentale, secondo le attività:

- analisi dei bisogni formativi
- pianificazione
- diffusione delle informazioni sui corsi
- effettuazione degli interventi formativi
- valutazione degli interventi.

Continuità operativa

2.2.1 Continuità operativa del Servizio

La gestione della Continuità Operativa del Servizio di Gestione Documentale di protocollo e conservazione dell'ISIA è affidata ad apposita Ditta.

2.2.2 Continuità Operativa del Sistema

Il Sistema di Gestione Documentale, ospitato su infrastruttura IT di apposita Ditta, è inserito:

- nell'ambito del Sistema di Gestione della Continuità Operativa di apposita Ditta:
- nell'ambito della soluzione tecnologica di Disaster Recovery di apposita Ditta; tale soluzione è dotata di una infrastruttura tecnologica dedicata e delle necessarie caratteristiche di ridondanza geografica.

MONITORAGGIO E CONTROLLI

2.3 Ripristino del Servizio

Il Responsabile del Servizio di Gestione documentale cura che le funzionalità del sistema, in caso di guasto o anomalia, siano ripristinate entro ventiquattro ore dal blocco delle attività e, comunque, nel più breve tempo possibile [art. 61, comma 3 del TESTO UNICO]

2.4 Livelli di servizio

In coerenza con il paragrafo precedenti, apposita Ditta garantisce che il Servizio sia erogato con i seguenti livelli di servizio:

orario di servizio	08:00 – 21:00 Lunedì – Venerdì 08:00 – 14:00 Sabato
disponibilità del servizio	migliore del 99%
RTO	72 ore

RPO	24 ore

LEGENDA

orario di servizio
Intervallo temporale entro il quale è garantita al cliente l'erogazione del "servizio" sulla base di quanto previsto da regolamento con il Comparto AFAM o da contratti in essere con il Cliente.
È uno degli elementi che concorrono al calcolo dell'indicatore sulla disponibilità del servizio.
Al di fuori di tale orario, il sistema è comunque disponibile ai Clienti senza garanzia del livello di servizio.

2.5 Comunicazione con il fornitore

L'apposita Ditta incaricata rende disponibile uno speciale servizio di assistenza al quale il Personale dell'ISIA può accedere attraverso l'apertura di una segnalazione (ticket) per chiedere la risoluzione di eventuali anomalie emerse durante la fruizione del servizio.

In caso d'anomalia o malfunzionamento del Servizio, l'apposita Ditta è tenuta a comunicare il problema riscontrato al Responsabile del Servizio; la comunicazione deve essere effettuata (anche tramite email) entro due ore all'interno dell'orario di servizio dal lunedì al venerdì.

2.6 Monitoraggio dell'infrastruttura IT

Il Sistema di Gestione Documentale:
- è ospitato su infrastruttura IT di apposita Ditta;
- viene mantenuto sotto controllo da apposita Ditta per quanto attiene l'infrastruttura IT tramite i processi e gli strumenti sotto descritti.

2.6.1 Procedure operative

La Procedura di Operation & Event Management di apposita Ditta:
- assicura il monitoraggio ed il controllo del corretto funzionamento dell'infrastruttura IT del Sistema di Gestione Documentale;
- descrive le attività necessarie affinché ai sistemi ed alle procedure applicative siano rese disponibili le risorse necessarie al corretto funzionamento;
- è focalizzata al supporto 24 ore x 365 giorni.

2.6.2 Strumenti

La strumentazione per il monitoraggio infrastrutturale del servizio erogato da apposita Ditta è essenzialmente costituita dalle componenti:
- sistemi di rilevazione;
- registrazione degli eventi;
- console;
- segnalazioni generate automaticamente.

2.6.3 Gestione dei log

La Ditta incaricata mantiene sotto controllo gli eventi anomali legati a:

- malfunzionamenti;
- performance;

registrandoli ai fini di:

- riesame;
- audit.

I log sono classificati nelle seguenti tipologie:

- log infrastrutturali: riguardano le componenti software (acquisite da Fornitori) e i sistemi hardware che compongono l'infrastruttura IT;
- log applicativi: riguardano le applicazioni software (sviluppate da apposita Ditta) con rilevanza dal punto di vista di monitoraggio delle funzionalità.

A seconda della tipologia dei log e della loro importanza, sono definite appropriate modalità di registrazione, accesso, archiviazione e cancellazione.

POLITICHE DI SICUREZZA

2.7 Politica di gestione della sicurezza dei sistemi

Poiché il Sistema di Gestione Documentale è ospitato su infrastruttura IT di apposita Ditta ed è gestito dal punto di vista infrastrutturale della stessa, le politiche di sicurezza descritte nel presente paragrafo riguardano il Fornitore e per quanto di possibile conoscenza da parte dell'ISIA di Roma.

2.7.1 Inventario degli asset IT

Gli asset associati ad informazioni e a strutture di elaborazione delle informazioni sono identificati; un inventario di questi asset deve essere pubblicato e mantenuto aggiornato.

Gli asset devono essere censiti, catalogati e valutati in relazione alla loro importanza per il business; devono essere quindi assegnati ad un Responsabile. La valutazione deve essere effettuata in base al valore, alle normative cui sono assoggettati, ai requisiti di riservatezza, integrità e disponibilità, alla criticità per l'organizzazione.

2.7.2 Installazione dei sistemi

L'integrità dei sistemi di produzione è un requisito di sicurezza essenziale per la Ditta incaricata; pertanto devono essere attuate procedure per controllare l'installazione del software sui sistemi di produzione.
Devono inoltre essere stabilite e attuate regole (limitazioni) per il governo dell'installazione del software da parte degli Utenti.

cambiamento

Le modifiche alle componenti di software applicativo, hardware e software di sistema devono essere gestite applicando, a seconda dei casi, dei processi di governo del cambiamento relativi alla pianificazione, progettazione, sviluppo, test e rilascio delle nuove funzionalità o di quelle modificate, includendo gli opportuni passi di verifica ed autorizzazione.

documentazione

I cambiamenti apportati all'infrastruttura IT devono essere opportunamente documentati.

2.7.3 Resource Capacity Management

Per poter garantire che l'infrastruttura tecnologica sia in grado di soddisfare i livelli di servizio richiesti, tutte le componenti hardware e software devono essere tenute sotto controllo; si devono fare proiezioni sui futuri requisiti di capacità per assicurare le prestazioni di sistema richieste.

Il Processo è strutturato nelle seguenti fasi:

- analizzare i piani aziendali a breve e lungo termine;
- osservare l'attuale performance di ciascuna componente coinvolta, identificando ogni "collo di bottiglia" e verificando il carico di lavoro attuale e la sua evoluzione prevista per il futuro;
- valutare la crescita del carico di lavoro nel tempo;
- avviare l'eventuale attività di approvvigionamento delle risorse in esame.

2.7.4 Configurazione dei sistemi

Nel tempo deve essere mantenuto un modello dell'infrastruttura IT attraverso l'identificazione, il controllo, la manutenzione e l'aggiornamento delle informazioni di configurazione; tali informazioni vanno gestite in un apposito archivio.

2.7.5 Backup

Devono essere effettuate copie di backup delle informazioni, del software e delle immagini dei sistemi; le copie devono essere sottoposte a test periodici di restore.

Il Processo che regola l'esecuzione del backup garantisce che la modalità di salvataggio sia selezionata in base ai seguenti parametri: tipologia del dato (dato di produzione / non produzione, dato strutturato / non strutturato), frequenza, ubicazione copie, periodo di retention, supporto fisico, ambiente tecnologico.
Le copie di backup dei dati di produzione sono replicate nel datacenter secondario (Disaster Recovery).

2.7.6 Amministratori di Sistema

Devono essere minimizzati i rischi di:

- violazione alla compliance relativa agli Amministratori di Sistema;
- danneggiamento di dati e sistemi informatici derivanti da accessi non autorizzati o non adeguatamente controllati ai sistemi ed alle applicazioni da parte dei medesimi Amministratori.

La nomina degli Amministratori di Sistema va effettuata, da parte dei Responsabili delle competenti S.O. aziendali (Servizi Operativi), previa attenta valutazione delle caratteristiche soggettive, ovvero: è necessaria una valutazione dell'esperienza, della capacità e dell'affidabilità del Soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza.
Inoltre la designazione quale Amministratore di Sistema deve essere in ogni caso individuale e deve recare l'elencazione degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti, anche da parte del Garante della Privacy.

L'operato degli Amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei Titolari o dei Responsabili del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

Politica per l'inserimento dell'utenza e per il controllo degli accessi logici

La politica per il controllo degli accessi logici si applica anche al caso specifico del Servizio di Gestione Documentale Informatico; pertanto anche in tale ambito si deve limitare l'accesso alle informazioni ed ai servizi di elaborazione delle informazioni ai cosiddetti "need to access" ovvero alle effettive e legittime necessità operative, è considerato obiettivo fondamentale della Sicurezza delle Informazioni nell'ISIA.

Tutto il Personale dell'ISIA e le terze parti interessate devono essere informati sulla esistenza di una politica specifica per la gestione ed il controllo degli accessi logici alle risorse e devono essere vincolati, in dipendenza delle loro responsabilità o competenze, a rispettarne le prescrizioni.
La strumentazione e le istruzioni per il controllo degli accessi devono essere mantenute costantemente adeguate alle esigenze dei servizi offerti dall'ISIA e alle esigenze di sicurezza degli accessi, anche in relazione alle evoluzioni organizzative e tecnologiche.

2.7.7 Gestione delle credenziali di accesso

Assegnazione, riesame e revoca degli accessi degli utenti

Riguardo al Servizio di Gestione Informatico:

- l'accesso alle informazioni e funzioni di sistemi applicativi deve essere limitato alle effettive necessità;
- rimozione o adattamento dei diritti di accesso: i diritti di accesso di tutto il Personale e degli utenti di parti esterne a informazioni e strutture di elaborazione delle informazioni devono essere rimossi al momento della cessazione del rapporto di lavoro, del contratto o accordo, oppure adattate ad ogni variazione;
- a fronte della cessazione, verranno disattivati gli identificativi di accesso del Personale non più in servizio e dei consulenti non più operativi;
- nessun identificativo di accesso dovrà essere cancellato ma dovranno essere eliminate le abilitazioni;
- gli identificativi-utenti assegnati una volta non potranno più essere assegnati successivamente a persone diverse;
- gestione dei diritti di accesso privilegiato: l'assegnazione e l'utilizzo delle utenze e dei privilegi amministrativi deve essere ristretto e controllato;
- nel caso sia necessario accedere "in emergenza" a specifici dati/sistemi da parte di Personale non ancora abilitato si deve richiedere un'abilitazione temporanea;
- a fronte della definizione di nuove credenziali di accesso / modifica delle esistenti, viene inviata una notifica all'Interessato; egli accede al sistema informativo aziendale nel quale consulta le credenziali assegnate e registra la propria accettazione.

L'attuazione del processo organizzativo è di responsabilità delle figure designate dall'ISIA; le relative richieste sono effettuate alla Ditta incaricata ed all'Amministratore di Rete che provvedono, tramite gli opportuni strumenti tecnici, a soddisfarle e a fornire il relativo riscontro ai richiedenti.

Richieste effettuate al fornitore

I processi organizzativi e la strumentazione tecnica utilizzata da apposita Ditta per la gestione delle richieste dell'ISIA relative alle credenziali di accesso al sistema di gestione dei documenti, sono coerenti con la politica ed i processi dell'ISIA.

2.7.8 Utilizzo delle password

Riguardo al Servizio di Gestione Documentale informatica:

- l'utilizzo e la gestione delle credenziali deve garantire di evitare utilizzi impropri delle password e delle credenziali di autenticazione;
- le regole relative alla costruzione ed utilizzo delle password si applicano a tutto il Personale ed alle terze parti che ne fanno uso per accedere agli asset dell'ISIA;
- l'utilizzo delle password ed in genere delle credenziali utente deve essere controllato con un processo di gestione formale, anche automatizzato, fin dove possibile;
- le credenziali sono personali e non cedibili, devono essere assegnate in base alla necessità di accedere ai dati o ai sistemi aziendali e devono essere gestite contemporaneamente alle abilitazioni, sulla base del principio del "minimo privilegio";
- le password devono essere 'robuste', ovvero costruite in modo da non essere facilmente 'indovinabili' (password guessing) e custodite con cura, nonché variate periodicamente;
- analoghe regole valgono per i cosiddetti PIN dei dispositivi con a bordo certificati digitali (smart card, ecc.).

2.7.9 Responsabilità degli utenti

Le credenziali sono personali e non cedibili.
Ogni utente è Responsabile della corretta gestione della propria password, dei dispositivi di riconoscimento, delle informazioni per l'accesso ai sistemi e ai dati.
Le credenziali e i dispositivi di riconoscimento devono essere conservati adeguatamente e non essere mai lasciati incustoditi.

La responsabilità delle azioni compiute nella fruizione del Servizio di Gestione Documentale è dell'utente fruitore del servizio.

La responsabilità delle operazioni compiute tramite un'utenza è sempre del legittimo Titolare, anche se compiute in sua assenza.

2.7.10 Servizi informatici forniti da apposita Ditta incaricata.

La strumentazione tecnica utilizzata dalla Ditta incaricata per la gestione delle password di accesso ai servizi forniti, è coerente con la politica dell'ISIA in quanto:

- i sistemi di gestione delle password sono interattivi e assicurano password di qualità;
- i sistemi di autenticazione impongono il rispetto della password policy.

Esecuzione degli accessi

Il Sistema di Gestione Documentale realizzato su infrastruttura IT della Ditta incaricata e da questa gestito, è dotato di:

- procedure di log-on sicure. L'accesso a sistemi e applicazioni è essere controllato da procedure di log-on sicure;
- controllo degli accessi alle applicazioni ed alle informazioni. L'accesso alle informazioni ed alle funzionalità dei sistemi applicativi da parte degli utenti e del Personale di supporto è progettato e realizzato in base al principio di necessità;
- password di accesso. La strumentazione tecnica utilizzata da apposita Ditta per la gestione delle password di accesso ai servizi forniti, è coerente con la politica.

Politica di gestione delle postazioni di lavoro

La politica si applica anche al caso specifico del Servizio di Gestione Documentale; pertanto devono essere rispettate le seguenti regole:

Aggiornamenti del software

- l'ISIA deve mantenere adeguato il livello di aggiornamento del software installato sulle postazioni di lavoro;
- il Personale, da parte sua, non deve inibire gli eventuali strumenti di aggiornamento automatico o centralizzato previsti dall'ISIA.

limitazione della connettività a supporti esterni

L'utilizzo improprio di dispositivi rimovibili può aumentare il rischio di fuga di dati riservati; pertanto il Personale:

- non deve consentire ad altro Personale il collegamento di dispostivi rimovibili alla propria postazione;
- non deve connettere alla propria postazione dispositivi rimovibili e lasciarli incustoditi;
- non deve lasciare incustodito il dispositivo all'esterno del perimetro aziendale.

Modifica delle impostazioni

Il Personale ha la responsabilità di non modificare le configurazioni standard (sia software che hardware) impostate al momento dell'installazione iniziale nelle postazioni di lavoro, dispositivi mobili o supporti rimovibili affidati in dotazione individuale, senza specifica autorizzazione delle funzioni di sicurezza.

Configurazione delle postazioni di lavoro

Il sistema di gestione documentale, lato utente, è reso disponibile in modalità di navigazione sul web; le postazioni di lavoro ed i browser devono pertanto essere configurati secondo le specifiche tecniche riportate nel Manuale di configurazione fornito dal fornitore dei servizi.

Postazioni di lavoro virtuali

Quale elemento primario per la razionalizzazione delle risorse strumentali, progressiva riduzione delle spese di esercizio ed incremento delle caratteristiche di sicurezza, viene previsto l'utilizzo delle tecnologie di virtualizzazione del desktop.

2.8 Politica di gestione, dismissione e smaltimento degli apparati mobili e dei supporti

La politica si applica anche al caso specifico del Servizio di Gestione Documentale Informatico; pertanto devono essere rispettate le seguenti regole:

gestione apparati e supporti informatici

Gli apparati e i supporti informatici devono essere protetti da accessi non autorizzati, utilizzi impropri, manomissioni, danneggiamento o furti:

- durante il loro utilizzo all'interno e all'esterno delle sedi dell'ISIA;
- durante il trasporto;
- durante i periodi di inattività.

Riguardo alla postazioni di lavoro mobili:
in genere le postazioni di lavoro mobili sono assegnate personalmente al Personale, in alcuni casi possono essere intestate ad una Postazione Operativa ed utilizzate dal Personale ad essa appartenente.
Il Personale deve essere preventivamente autorizzato a portare con sé al di fuori delle sedi dell'ISIA gli apparati mobili assegnati.
La memorizzazione di dati personali non aziendali da parte del Personale su apparati mobili non è ammessa a meno di esplicita autorizzazione da parte dell'ISIA (esempio: smartphone in comodato d'uso).

Dismissione apparati e supporti informatici

Tutti gli apparati e i supporti informatici devono essere controllati per assicurare che ogni dato critico sia rimosso o sovrascritto in modo sicuro prima della dismissione o del riutilizzo.

Gestione supporti cartacei

In generale le informazioni presenti sui supporti cartacei (documenti, appunti) non dovrebbero mai essere lasciate dal Personale in luoghi al di fuori del proprio controllo.
Nello specifico, le informazioni rilevanti o riservate presenti sui supporti cartacei non devono mai essere lasciate dal Personale al di fuori del proprio controllo.

Sulle scrivanie degli uffici, sui tavoli delle sale riunioni, o in altri luoghi, al termine del lavoro o al termine delle riunioni non deve essere lasciata documentazione riservata.
Sui dispositivi di stampa, fotocopia, acquisizione ottica delle immagini e nelle loro vicinanze non deve essere lasciata documentazione riservata.
A maggior ragione la documentazione riservata deve essere gestita con particolare cura all'esterno delle sedi dell'ISIA.

Dismissione supporti cartacei

Le informazioni rilevanti o riservate presenti sui supporti cartacei che non si intende più utilizzare, devono essere distrutte o rese non consultabili.
Nel caso di cessato utilizzo di documenti cartacei riservati, essi devono essere triturati con gli appositi apparecchi.

2.9 Politica di protezione dal malware

La politica si applica anche al caso specifico del Servizio di Gestione Documentale Informatico; pertanto devono essere rispettate le seguenti regole:

- le informazioni di proprietà dell'ISIA o da essa gestite e le infrastrutture IT preposte alla loro elaborazione devono essere protette contro il malware;
- debbono essere previsti ed attuati controlli di individuazione, di prevenzione e di ripristino relativamente al malware;
- deve essere formato e promosso un idoneo grado di consapevolezza degli utenti per prevenire le minacce e le vulnerabilità derivanti dal malware.

Contromisure per la protezione dal malware

La strumentazione software per la protezione dal malware (c.d. antivirus) è installata su tutte gli apparati con sistema operativo Windows, siano essi server dedicati ad erogare servizi che postazioni di lavoro dalle quali si accede ai servizi; l'antivirus è installato sia sui sistemi fisici (server, personal computer) che virtuali utilizzati dall'ISIA.

Nei sistemi "endpoint" su cui è installato, l'antivirus è sempre attivo e la scansione opera in tempo reale su ogni movimentazione di file, proteggendo così l'apparato dal malware.

Le componenti sopra descritte sono periodicamente aggiornate per assicurare adeguate misure di protezione.

Contromisure per la protezione dallo spamming

I sistemi che gestiscono la posta elettronica utilizzano una strumentazione software per la protezione dallo spamming; le finalità della strumentazione sono:

- controllare le informazioni di provenienza dei messaggi;
- a seconda della correttezza di tali informazioni, eliminare, inserire in quarantena o consegnare i messaggi al destinatario;
- eliminare dai messaggi ricevuti eventuali programmi eseguibili in essi contenuti;
- inviare ai Destinatari l'elenco dei messaggi inseriti in quarantena.

Il Personale dell'ISIA, qualora ritenga che un messaggio ricevuto sia indesiderato, lo può inviare al sistema che aumenta così la base di conoscenza per l'individuazione dello spamming.

Le componenti sopra descritte sono periodicamente aggiornate per assicurare adeguate misure di protezione.

Scrivania e schermo puliti

La politica si applica anche al caso specifico del Servizio di Gestione Documentale; pertanto devono essere rispettate le seguenti regole:

debbono essere adottate e rispettate le politiche di "scrivania pulita" per i documenti ed i supporti di memorizzazione rimovibili e di "schermo pulito" per i servizi di elaborazione delle informazioni.
Tali regole sono essenziali per proteggere tutti gli apparati di elaborazione delle informazioni sia in utilizzo individuale (postazioni di lavoro) sia condiviso (console di sistemi di controllo, server, cartelle di rete, etc.).

Le regole debbono essere rispettate dal Personale dell'ISIA, dai Fornitori e dalle terze parti.

Scrivania pulita

Le regole di "scrivania pulita" sono essenziali per proteggere le informazioni su supporto cartaceo e su supporti rimovibili di memorizzazione: al termine del lavoro o durante lunghe pause, sulle scrivanie non deve essere lasciata alcuna documentazione riservata cartacea o su supporti rimovibili.

Schermo pulito

Non lasciare accessibile la postazione di lavoro durante la propria assenza: bloccarla, prevedendo lo sblocco con password e attivare comunque un "savescreen" automatico protetto da password che pulisca la videata entro alcuni minuti in caso di inutilizzo.
Sullo schermo della postazione, anche durante lo svolgimento della propria attività, non debbono essere facilmente visibili o accessibili informazioni riservate inutili per la corrente sessione di lavoro (ad esempio: lasciare aperto inutilmente un documento contenente informazioni sensibili, che possono essere inopportunamente lette da terzi durante o alla ripresa della sessione).