CREDEMTEL

Documento della

POLITICA SULLA SICUREZZA DELLE INFORMAZIONI

del Sistema di Conservazione
(ex. comma 1 dell'art. 3 del DPCM 3 dicembre 2013)

INDICE

REVISIONI

3	15/12/2017	Documento adeguato in seguito a modifiche organizzative, piccole revisioni di processi e recepimento nuove normative; aggiornato il glossario.
2	31/05/2017	Documento adeguato per recepire modifiche apportate a Manuale procedure interne (in particolare eliminazione allegati del MdQ, revisione della gestione degli incidenti di sicurezza ecc.). Aggiornato il glossario.
1	03/05/2016	Documento adeguato in seguito a modifiche organizzative, aggiornato glossario e organigramma. Sostituito il riferimento al "Manuale di utilizzo delle risorse informatiche" col nuovo "Disciplinare per l'uso dei dispositivi informatici e dei sistemi di comunicazione elettronica e disposizioni di carattere generale in materia di risorse informatiche",
0	30/04/2015	Prima stesura
Rev.	**data**	**causale**

Terminologia ed abbreviazioni

AD	=	Amministratore Delegato
AGL	=	Funzione Affari Generali e Legale
Agorà	=	Intranet comune a tutto il gruppo CREDEM con aree dedicate ad ogni singola società
AMMCO	=	Servizio Amministrazione Controllo e Servizi
Asset	=	Risorsa materiale o immateriale di Credemtel Spa che porta valore all'azienda (es. persone, edifici, hardware, software, apparati di rete ecc.)
BCM	=	*Business Continuity Manager*
BCPLAN	=	*Business Continuity Plan*
Business Continuity Manager	=	Esponente aziendale con posizione gerarchico-funzionale adeguata al quale è assegnata dalla Direzione la responsabilità dello sviluppo, della manutenzione e delle verifiche del *BCPLAN*.
Business Continuity Plan	=	Piano di continuità operativa dei processi critici per il business aziendale contenente le indicazioni metodologiche, tecniche ed organizzative per presidiare le situazioni di crisi.
CEDACRI	=	Outsourcer del sistema informativo del gruppo CREDEM
Codice utente	=	Codice univoco di accesso ad un sistema informatico. Di norma ad un utente viene assegnato un solo Codice Utente stabilito in base alla matricola di registrazione (se dipendente) o ad una diversa codifica se esterno.
Comitato di Crisi	=	L'organo responsabile della gestione della crisi nell'ambito del *Business Continuity Plan*.
Comitato Sicurezza	=	Organo collegiale gestito dal DG.
COMME	=	Servizio Commerciale
Credenziali	=	Codice utente aziendale e relativa password
CS	=	Capo Servizio
CU	=	Capo Ufficio
DBA	=	Ufficio DataBase Application e Altro di Credemtel Spa
DIR	=	Direzione
DG	=	Direttore Generale
DRF	=	Applicazione di CREDEM presente sulla intranet di gruppo che gestisce il workflow approvativo delle richieste di modifica delle abilitazioni o di sblocco/riassegnazione di nuova password a SEISLO. Le abilitazioni alle funzioni autorizzative del DRF sono stabilite dall'ufficio SIL e possono essere derogate su richiesta specifica a SEISLO.
GES	=	Ufficio Gestione delle persone di CREDEM.
HDI	=	Ufficio Help Desk Interno di CREDEM.
Incidente di sicurezza	=	Qualsiasi evento che comprometta o minacci di compromettere il corretto funzionamento dei sistemi e/o delle reti dell'organizzazione o la disponibilità, l'integrità e/o la riservatezza delle informazioni in esse memorizzate od in transito, o che violi le politiche di sicurezza definite o le leggi in vigore (con particolare riferimento al D.lgs. 196/2003, al Regolamento UE 2016/679, alla L. 547/1993 ed alla L. 38/2006)

Incidente IT	=	Grave disservizio tecnico che compromette l'erogazione di un sistema informatico in ambiente di produzione
INTEC	=	Servizio Information Technology
MQ	=	Manuale della Qualità e sicurezza informatica
NC	=	Non Conformità.
Outsourcer	=	Azienda che fornisce servizi in Outsouring (Es. CEDACRI)
Outsourcing	=	Affidamento della gestione, in tutto in parte, di uno o più sistemi o servizi ad aziende esterne denominate Outsourcer
PERMUTE	=	Procedura di gestione dei permessi utente presente sulla intranet di gruppo. Consente ai *RdF* di visionare e/o revocare i permessi associati al personale dei i servizi e/o uffici di competenza.
PM	=	Il Product Manager è colui che ha la responsabilità del prodotto/servizio dal punto di vista commerciale.
RAQ	=	Responsabile Assicurazione Qualità e sicurezza
RDC	=	Referente della Conservazione, funzione di Credemtel Spa composta dalle seguenti figure professionali previste dalla normativa AgID per la gestione di un Sistema di Conservazione: • Responsabile del servizio di conservazione • Responsabile della funzione archivistica di conservazione • Responsabile della sicurezza dei sistemi per la conservazione • Responsabile del trattamento dati personali • Responsabile dello sviluppo e della manutenzione del sistema di conservazione • Responsabile manutenzione e sviluppo del sistema di conservazione • Delegati di tutte le figure precedentemente elencate eventualmente nominati.
RdF	=	Responsabile di Funzione (*CS* e *CU*)
RS	=	Responsabile di Sistema, un Amministratore di Sistema con specifiche responsabilità di gestione e manutenzione tecnica del sistema stesso (elenco puntuale in TIME, si rimanda alla PRO06 per maggiori dettagli).
RSS	=	Responsabile del Sistema SECURITY (Sicurezza logica e fisica) di Credemtel Spa e Responsabile della sicurezza dei sistemi per la conservazione.
SEI	=	Ufficio Servizi Esterni e Interni della capogruppo CREDEM
Sistema di Conservazione	=	Sistema di conservazione dei documenti informatici di cui all'articolo 44 del Codice dell'Amministrazione Digitale (Decreto Legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni)
SIF	=	Ufficio Sicurezza Fisica della Capogruppo CREDEM.
SIL	=	Ufficio Sicurezza Logica della capogruppo CREDEM
SEISLO	=	Sicurezza Logica Operativa; reparto dell'ufficio SEI (Servizi Esterni e Interni) della capogruppo CREDEM.
SGSI	=	Sistema per la Gestione della Sicurezza delle Informazioni
Telelavoro	=	In caso di necessità e per periodi predefiniti, sono rilasciate autorizzazioni ad incaricati identificati per il telelavoro; a questi Credemtel Spa assegna le autorizzazioni e le istruzioni in forma scritta e riservata che l'incaricato deve sottoscrivere per accettazione. Le modalità di accesso al telelavoro, sono definite nel **Disciplinare per l'uso dei dispositivi informatici e dei sistemi di comunicazione elettronica e disposizioni di carattere generale in materia di risorse informatiche** allegato alla procedura **PRO20 Gestione sicurezza logica**. Per connettersi in telelavoro sul PC portatile del dipendente deve essere richiesto all'ufficio *HDI* l'installazione di uno specifico programma software che consente di effettuare l'Accesso remoto alla rete aziendale.
Sistema	=	Per sistema, ai sensi del provvedimento del garante sulla Privacy del 27 novembre 2008 sugli amministratori di Sistema, si intende una Rete di computer, un Database o altro sistema software complesso. Un sistema può essere anche un prodotto ed il relativo servizio erogato.

Workflow	=	Programma informatico che gestisce gli stati di una o più attività ognuna delle quali rappresenta un lavoro da svolgere per giungere a un obiettivo comune consentendo a più operatori di intervenire sullo stato delle varie attività solo quando di loro pertinenza per passarle dallo stato corrente solo ad uno di quelli definiti e consentiti dal disegno del workflow stesso.

1. Politica e standard di sicurezza (Security Policy)

1.1. L'obiettivo è quello di fornire le direttive per la gestione delle informazioni sulla sicurezza informatica.

La gestione in sicurezza delle infrastrutture informatiche ha l'obiettivo di garantire che i sistemi, le postazioni di lavoro, le applicazioni, i servizi di rete, i servizi elaborativi forniscano le prestazioni elaborative ai livelli e con i requisiti di sicurezza definiti:

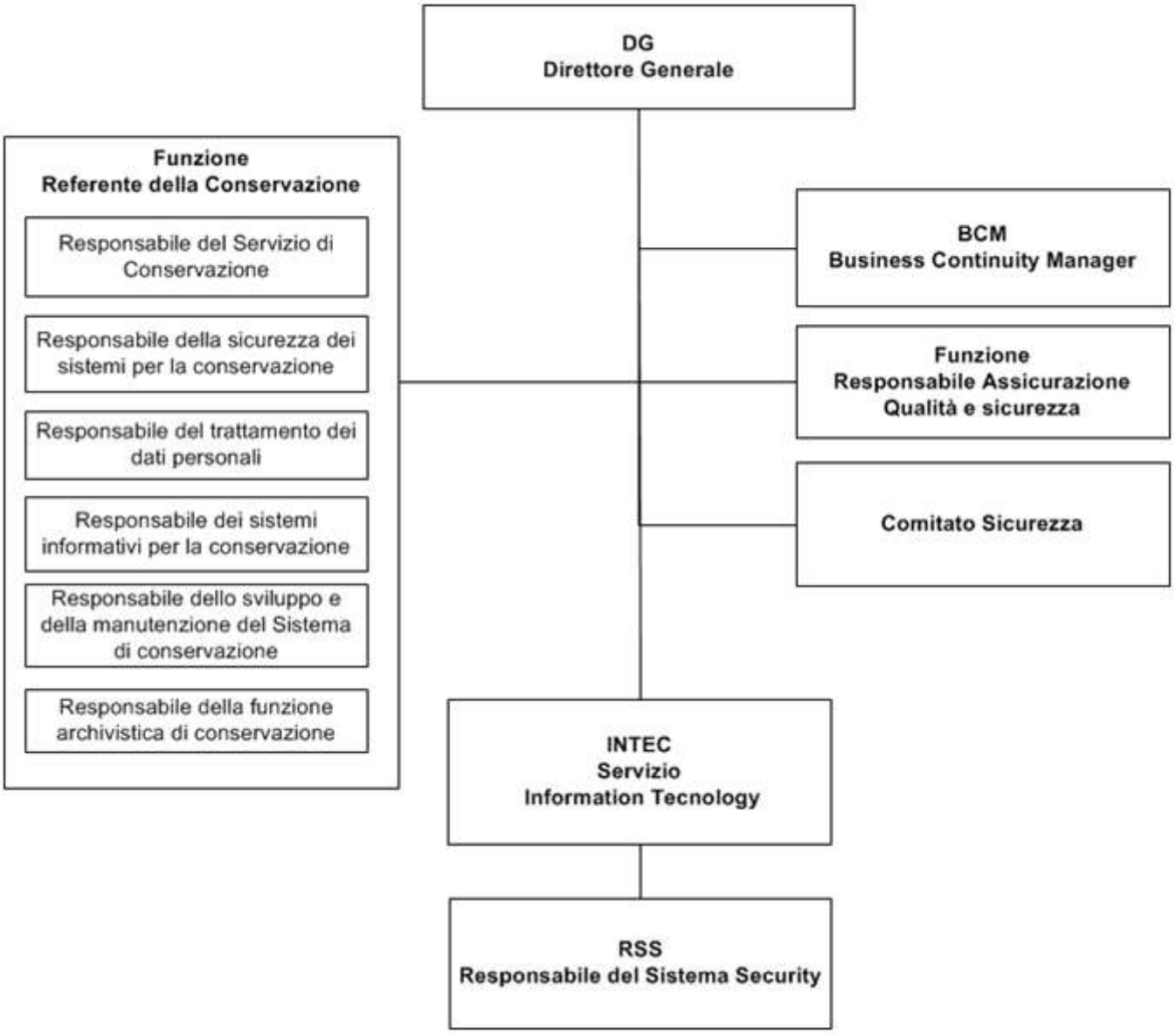
- Tutte le informazioni (dati, documenti, archivi, …) devono essere protetti e conservati;
- Per la riservatezza dei contenuti scambiati, la sicurezza deve essere garantita anche a livello delle reti di comunicazioni dati;
- Deve essere gestita la sicurezza sia di tutti gli apparati inerenti alla struttura aziendale, sia del materiale di consumo considerato sensibile ai fini della sicurezza, sia dei collegamenti, con altre sedi aziendali, aziende collegate, fornitori, clienti, ecc.;
- Tutte le registrazioni considerate riservate devono essere oggetto di monitoraggio costante (manuale o automatico);
- Devono essere predisposte adeguate misure di sicurezza per l'accesso alla sala server;
- Ogni eventuale incidente o evento straordinario che possa pregiudicare la sicurezza deve essere oggetto di analisi e di rapporto scritto;
- Tutti i progetti di nuove applicazioni/servizi andranno valutati in termini di sicurezza informatica (eventualmente inseriti nel Piano di Sicurezza);
- Tutte le modifiche, eventualmente apportate ai processi organizzativi interni, devono essere preventivamente valutate in termini di sicurezza (eventualmente inserite nel Piano di Sicurezza);
- Per tutti i sistemi deve essere individuato un responsabile di riferimento (RS);
- La Politica della Sicurezza è approvata dal DG e comunicata in modo appropriato al personale interessato sia interno che esterno all'azienda;
- La Politica della Sicurezza viene riesaminata periodicamente per accertarne la continuità, idoneità nel corso del Riesame della Direzione.

1.2. Relativamente alle problematiche di sicurezza inerenti la gestione aziendale, sono state stabilite le seguenti responsabilità:

- RAQ: responsabilità di definire, aggiornare ed approvare le procedure di sicurezza di Credemtel Spa;
- RdF: responsabilità di fornire le configurazioni e/o gli aggiornamenti che devono essere implementati nei sistemi di sicurezza (firewall, routing, switch, postazioni di back office…) agli uffici preposti ad implementarle (SIL, SEISLO, CEDACRI ecc.) per assicurare il mantenimento dei livelli di sicurezza anche nei confronti di funzioni e/o entità esterne all'azienda.
- RS: responsabilità di gestione dei singoli sistemi presenti in azienda;
- Funzioni di CREDEM (SEI e SIL): responsabilità della gestione operativa dell'infrastruttura di sicurezza in outsourcing, sia relativamente agli applicativi software sia relativamente ai sistemi di calcolo su cui i medesimi sono installati.

2. Organizzazione per la sicurezza (Security Organization)

2.1. Credemtel Spa ha definito e costituito una organizzazione preposta a sovrintendere e controllare i processi e le attività legate alla sicurezza dell'infrastruttura interna:



- **Il Comitato Sicurezza è composto da**:
    a. DG;
    b. RAQ;
    c. RSS,
    d. CS INTEC;
    e. CS COMME;
    f. CS AMMCO;
    g. Responsabile della sicurezza dei sistemi per la conservazione;
    h. Altri partecipanti ad invito su indicazione di DG o di altri membri.

Le riunioni sono convocate dal DG o dal RAQ che invita tutti i componenti del Comitato e eventuali altri partecipanti ad invito.
Le modalità di convocazione, di svolgimento e di registrazione di dette riunioni, sono indicate nella procedura **PRO14 Riesame della Direzione**.

- **Responsabilità**: nella documentazione di sistema (procedure, istruzioni tecniche, ecc. …) sono definite le responsabilità assegnate ad ogni singola funzione aziendale.
- **Installazione struttura di trattamento dei dati approvata e autorizzata**: la procedura **PRO01 Settore Legale e normativo** riporta la metodologia utilizzata dall'azienda per la gestione e la protezione dei Dati Personali e Sensibili relativi al personale interno ed alle persone e/o Organizzazioni che con l'azienda si relazionano. Tale procedura identifica le figure e le competenze relative al trattamento dei dati in conformità alla normativa vigente e in particolare al D. Lgs. n° 196 del 30/06/2003 e al Regolamento UE 2016/679.
- **Consulenze e Informazioni dall'esterno**: l'azienda ricorre a risorse esterne (ufficio SIL di CREDEM) per l'aggiornamento delle informazioni relative alla Sicurezza, attraverso adeguate fonti di informazione. (es. abbonamenti riviste specializzate e di settore, Internet, ecc.), normative e aggiornamenti.
- **Cooperazione tra organizzazioni**: il Comitato Sicurezza definisce, anche dal punto di vista contrattuale le condizioni di collaborazione tra l'azienda ed altre organizzazioni. In particolare definisce le modalità di utilizzo e di eventuale diffusione di informazioni e/o altre risorse aziendali. Il RAQ ha il compito di sovrintendere regolarmente le eventuali occasioni di collaborazione:
    a. Informando il personale di competenza delle disposizioni impartite dal Comitato Sicurezza;
    b. Effettuando i dovuti controlli periodici;
    c. Verificando periodicamente lo stato di integrità delle risorse aziendali.
- **Riesame dell'attuazione della Politica per la Sicurezza**: l'attuazione e il funzionamento del SGSI viene verificato da personale indipendente dall'attività oggetto di esame nel corso degli audit periodici del Sistema, come descritto in procedura **PRO11 Audit Interno**.

2.2. Credemtel Spa ha definito e costituito una funzione preposta a sovrintendere e controllare i processi e le attività legate alla sicurezza dall'accesso di terze parti.

- **Identificazione dei rischi dall'accesso di terza parte:** in base a quanto definito con la procedura **PRO21 Valutazione del Rischio** sono stati individuati i rischi di accesso alle Informazioni da parte di terzi. Le modalità con cui l'azienda tiene sotto controllo il rischio di accesso non autorizzato alle Informazioni aziendali da parte di terzi, sono riportate nelle seguenti procedure:
    a. **PRO19 Gestione sicurezza fisica**;
    b. **PRO20 Gestione sicurezza logica**.
- **Requisiti di sicurezza nei contratti con fornitori:** le funzioni preposte definiscono, applicano e presidiano la conformità delle forniture e dei servizi in outsourcing ai requisiti di sicurezza specificati, secondo le modalità previste dalla procedura **PRO09 Approvvigionamento**

3. Classificazione e Controllo delle risorse (Asset Classification and Control)

3.1. Credemtel Spa deve classificare, controllare e proteggere appropriatamente gli asset aziendali più importanti.

- **Assegnazione Asset Aziendali**: le risorse aziendali vengono assegnate a seconda delle necessità al personale/ufficio, quest'ultime devono conservarle secondo quanto stabilito dalle direttive aziendali (vedasi **Disciplinare per l'uso dei dispositivi informatici e dei sistemi di comunicazione elettronica e disposizioni di carattere generale in materia di risorse informatiche** allegato alla **PRO20 Gestione della sicurezza logica**).
- **Responsabili**: come indicato nella procedura **PRO08 Manutenzione**, gli addetti alle varie funzioni aziendali, sono responsabili delle risorse (asset) loro assegnate.
- **Inventario degli asset**: per definire i controlli più appropriati e gestire i rischi degli asset, l'azienda, tramite gli addetti incaricati, ha emesso inventari per gli asset fisici e logici più importanti. Essi sono:
  a. Infrastruttura locale:
     - Uffici immobile Credemtel
     - CED dell'immobile Credemtel
  b. Hardware e Data Center:
     - PC personali
     - Server presso l'immobile di Credemtel
     - Supporti rimovibili e riscrivibili
  c. Software base, email, internet:
     - SW base
     - Email
     - Internet
  d. Software applicativi
  e. Base dati
  f. File system
  g. Servizi rete interna:
     - Rete fisica
     - Rete logica
  h. Servizi in outsourcing:
     - Sistema informativo
     - Servizi di interconnessione esterni

3.2. Classificazione delle informazioni.

- **Le informazioni nell'ambito del Processo di Conservazione sono classificate su una scala a tre valori (elaborate in base alla classificazione prevista dal Testo Unico sulla Privacy D. Lgs.vo 196/2003):**

  a. Non riservate: informazioni non contenenti dati personali
  b. Riservate: informazioni contenenti dati personali esclusi quelli sensibili e giudiziari
  c. Sensibili: informazioni contenenti dati personali sensibili e/o giudiziari

  Per ulteriori dettagli riguardo all'identificazione ed alla gestione delle Informazioni, si rimanda alla procedura **PRO21 Valutazione del rischio**.

4. Sicurezza del personale (Personnel Security)

4.1 Sicurezza nella definizione e ricerca dei collaboratori.

Gli obiettivi sono: ridurre il rischio di errori umani, furto, frode o uso improprio delle strutture aziendali; accertarsi che il personale addetto sia stato informato sui rischi relativi alla sicurezza delle informazioni.

- **Responsabilità funzionali per la sicurezza**: per rendere efficace il SGSI sono chiaramente definiti, documentati e comunicati i ruoli, responsabilità ed autorità. L'Organigramma aziendale e la descrizione delle funzioni e dei ruoli sono pubblicate sulla intranet aziendale come previsto dalla procedura **PRO00 Procedura di correlazione posizione-responsabili**.
- **Selezione del personale**: la selezione e assunzione del personale è gestita in outsourcing da GES, di volta in volta, sulla base delle esigenze aziendali e normative, vengono definite e concordate con GES le procedure per la selezione del personale.
- **Dichiarazione di riservatezza**: i dipendenti e collaboratori, e comunque tutte le persone che, anche per un periodo limitato sono incaricati di trattare informazioni riservate e/o importanti per conto di Credemtel Spa devono sottoscrivere un impegno alla riservatezza, che sarà conservato nell'archivio del personale.

4.2 Formazione e informazione degli utenti.

- **Formazione e informazione per la sicurezza delle Informazioni**: per il personale interno, ed eventualmente di terze parti sono previsti corsi di formazione e di addestramento. Tali corsi hanno il fine di garantire che il personale che usa le strutture dell'Information Technology (IT) sia consapevole delle problematiche inerenti alla sicurezza delle Informazioni e abbia l'addestramento tecnico necessario per attuare quanto indicato nella Politica per la Sicurezza durante il normale svolgimento del proprio lavoro. Per le modalità con cui vengono individuate, erogate e registrate le attività di formazione ed addestramento si rimanda alla procedura **PRO10 Gestione della formazione**.

4.3 Risposta agli incidenti ed ai malfunzionamenti.

- **Notifica degli incidenti sulla sicurezza:** a fronte della Valutazione del rischio informatico, Credemtel Spa ha predisposto all'interno delle procedure **PRO19 Gestione sicurezza fisica** e **PRO20 Gestione sicurezza logica** le istruzioni da seguire per la gestione degli incidenti di sicurezza; tali procedure riportano le modalità per gestire il rischio e gli interventi da attuare in caso di emergenza.
- **Notifica delle criticità di sistema**: nell'ambito della periodica rivalutazione del rischio, l'analisi di tutti gli incidenti e delle NC riscontrate, mette il Comitato Sicurezza in condizione di individuare le "vulnerabilità" del sistema e fornisce quindi il punto di partenza per la definizione dei Piani di Miglioramento da proporre alla Direzione per la loro attuazione.
- **Notifica di malfunzionamenti del software**: chiunque noti un malfunzionamento del software è tenuto a registrare una NC sul Sistema di pertinenza, il suo RdF provvederà alla conseguente classificazione del malfunzionamento stesso ed al suo inoltro all'ufficio tecnico competente per la risoluzione come previsto dalla procedura **PRO05 Gestione delle Non Conformità e azioni correttive**.
- **Analisi degli incidenti**: l'insieme delle registrazioni degli incidenti accaduti, raccolto come indicato nelle già citate procedure PRO19 e PRO20**,** permette di monitorare e quantificare il tipo, il volume e i costi degli incidenti e dei malfunzionamenti.
- **Procedimenti disciplinari**: sono considerati come un'azione correttiva anche i procedimenti disciplinari avviati nei confronti del personale che abbia violato le procedure o le "Policy aziendali".

5. Sicurezza materiale e ambientale (Physical and Environmental Security)

5.1. Sicurezza fisica degli ambienti e del loro contenuto.

Obiettivi: impedire l'accesso non autorizzato, il danneggiamento e l'interferenza all'interno del flusso delle informazioni con conseguente interruzione delle attività.

A. ZONE DI SICUREZZA

- **Perimetro di sicurezza**: nell'allegato 2 **Planimetria della sede di Credemtel** della procedura **PRO19 Gestione sicurezza fisica**, sono indicate le aree di lavoro.
- Controllo dell'ingresso alla struttura: nella procedura **PRO19 Gestione sicurezza fisica**, sono indicate le modalità di accoglienza e registrazione dei visitatori in ingresso.
- **Sicurezza di uffici, stanze e servizi**: gli uffici ove vengono svolte attività sensibili, le responsabilità del personale addetto all'apertura e chiusura degli uffici sono fissate nella procedura **PRO19 Gestione sicurezza fisica**.
- **Zona sicura di lavoro**: gli uffici sono zona sicura di lavoro.
  Le aree in cui possono essere custodite informazioni riservate/confidenziali o asset di importanza strategica sono, quando non presidiate, in locali normalmente chiusi a chiave o riposti in armadi chiusi.
  L'area della sala server è chiusa con porta dotata di apertura a badge gestito direttamente dall'ufficio DPSSIF di CREDEM; l'accesso a tale area è normalmente effettuato in presenza di personale interno autorizzato dall'ufficio DPSSIF di CREDEM, come anche identificato nel Documento Programmatico per la Sicurezza (DPS), e comunque con la metodologia identificata nella procedura **PRO19 Gestione sicurezza fisica**.
- **Isolamento di aree di distribuzione e consegna**: la consegna e l'accettazione di merci è regolamentata dalla procedura **PRO19 Gestione sicurezza fisica**. Viene effettuata all'interno dello stabile, nello spazio antistante la porta d'ingresso, in presenza di personale autorizzato al controllo della documentazione di accompagnamento. Questa zona si trova in uno spazio dove non viene trattata alcuna Informazione aziendale.

B. SICUREZZA DELLE ATTREZZATURE

- **Posizionamento e protezione delle attrezzature:** le attrezzature di lavoro sono a disposizione di personale opportunamente addestrato nell'uso delle stesse. Ogni ufficio viene dotato delle risorse tecnologiche necessarie allo svolgimento dell'attività. I PC sono protetti da accesso logico e regolarmente controllati dal punto di vista dell'integrità e funzionalità. La manutenzione viene effettuata regolarmente dal personale in outsourcing (hardware CEDACRI – software CREDEM). I server di produzione sono di proprietà, gestiti e localizzati presso l'outsourcer (CEDACRI) secondo le prassi e regole del fornitore, il quale è certificato ISO 27001. Opportune registrazioni dei controlli effettuati dall' outsourcer sono rese disponibili a richiesta.
- **Alimentazione elettrica**: l'azienda è dotata di un gruppo di continuità per i server di sviluppo ed apparati di rete, che garantisce le dovute condizioni di messa in sicurezza dei dati e delle apparecchiature in caso di caduta dei tensione dell'impianto elettrico. L'operatività è garantita per almeno 1 ora a pieno carico; nel caso del protrarsi della mancanza di tensione per un tempo superiore, l'operatività viene ridotta al fine di mantenere l'operatività con il cliente.
- **Sicurezza della rete**: i cablaggi sono descritti nella procedura **PRO19 Gestione sicurezza fisica**. Nella sala server i cablaggi sono inseriti in canaline come da norma. I cablaggi raggiungono le postazioni passando sia in canaline poste nei muri, sia in canaline esterne; o posizionate sotto i pavimenti galleggianti e si collegano a torrette o prese a muro. I cablaggi inutilizzati sono controllati e affidati in outsourcing a CREDEM.
- **Manutenzione delle attrezzature**: le attrezzature sono utilizzate quotidianamente, quindi c'è un controllo continuo sulle stesse. In ogni caso le attrezzature sono periodicamente controllate dall'Amministratore di Sistema.
- **Sicurezza delle attrezzature fuori sede**: le risorse strumentali che sono o possono essere al di fuori della struttura aziendale sono:

a. Dispositivi portatili;
b. hardware in housing presso gli outsourcer.

Il loro utilizzo è regolamentato dalla procedura **PRO08 Manutenzione**.
Queste apparecchiature sono opportunamente conservate, monitorate e custodite a cura degli affidatari.
In caso di necessità, CS INTEC conferisce un'autorizzazione specifica per movimentare e/o collocare in housing ulteriori attrezzature.

- **Conservazione sicura e riutilizzo delle attrezzature e dei supporti**: i PC che non sono sotto la diretta responsabilità dei dipendenti per quanto riguarda l'uso secondo le indicazioni della procedura **PRO08 Manutenzione** e nel **Disciplinare per l'uso dei dispositivi informatici e dei sistemi di comunicazione elettronica e disposizioni di carattere generale in materia di risorse informatiche** allegato alla procedura **PRO20 Gestione sicurezza logica**, sono opportunamente conservati, per consentirne un riutilizzo sicuro. Le attrezzature inutilizzate e/o obsolete, sono conservate in armadi chiusi a chiave o in magazzino. Il riutilizzo dei supporti è regolamentato dalla istruzione operativa **IST-08-03 Cessazione supporti removibili** della procedura **PRO08 Manutenzione**.

C. CONTROLLI GENERALI

- **Politica di Clear Desk e Screen Saver:** Credemtel Spa ha definito una politica di ordine e pulizia dell'ambiente di lavoro con l'archiviazione in armadi chiusi a chiave dei documenti ritenuti importanti per l'azienda come: contratti, corrispondenza ecc.; I PC sono protetti con uno screen saver con richiesta della password alla riattivazione, per impedire l'accesso non autorizzato ai dati ed alle Informazioni.
- **Prelievo di risorse aziendali:** le risorse aziendali siano esse informatiche, strumentali, strutturali e cartacee, in nessun modo possono essere trasportate all'esterno della struttura, in mancanza di autorizzazione da parte del proprio RdF.
- **Verifica applicazione e rispetto Politica per la Sicurezza**: I RdF hanno il dovere di verificare l'applicazione e rispetto della Politica per la Sicurezza e di segnalare tramite NC sul sistema SECURITY le anomalie o carenze al fine che il RS del sistema le possa gestire.

6. Gestione dei sistemi e delle reti (Computer and Network Management)

6.1. Responsabilità e procedure operative.

Obiettivi: assicurare il corretto e sicuro funzionamento dei sistemi di elaborazione e delle reti.

- **Procedure operative documentate**: Credemtel Spa ha definito ed emesso procedure relative al Sistema di Gestione Integrato Qualità e Sicurezza delle Informazioni come elencate tramite il modulo **Piano di controllo dei documenti** della **PRO15 Gestione della documentazione**.
- **Variazioni alle apparecchiature, al software e alle applicazioni**: tutte le modifiche alle apparecchiature ed al software sono autorizzate ed affidate in outsourcing a CREDEM. Delle modifiche da effettuare ed eseguire è tenuta traccia a cura dell'outsourcer.
- **Procedure di gestione degli incidenti**: l'azienda gestisce tutti gli incidenti e malfunzionamenti del sistema come indicato nelle procedure **PRO19 Gestione sicurezza fisica** e **PRO20 Gestione sicurezza logica** ove si definiscono le responsabilità ed i comportamenti da adottare in caso si verifichino incidenti di sicurezza.
- **Definizione e delimitazione degli incarichi**: Il Consiglio di Amministrazione, sulla base delle specifiche competenze ad autorità regolamentate dalla procedura **PRO00 Procedura di correlazione posizione-responsabili**, conferisce gli incarichi generali e specifici relativi alla Sicurezza. Le funzioni assegnate rispecchiano i privilegi di accesso alle informazioni definiti nella procedura **PRO20 Gestione sicurezza logica**.
- **Tenuta sotto controllo delle risorse esterne**:
    a. Il servizio di pulizia dei locali è affidato a società esterna, regolamentato da apposite clausole contrattuali.
    b. L'assistenza tecnica delle apparecchiature in manutenzione (fotocopiatrici, telefonia, ecc.), in caso di guasto, è effettuata su chiamata e avviene durante l'orario di apertura dell'ufficio, l'assistenza comprende anche i ricambi e il materiale di consumo. Inoltre il personale esterno che ha accesso agli uffici è sempre accompagnato dal personale interno e non accede ad alcuna informazione senza l'autorizzazione da parte di DIR.
    c. L'assistenza tecnica da parte di fornitori dei software applicativi, dei data base ed eventuali altri (come Firewall, Rete ecc.), è definita con specifici contratti di assistenza. I fornitori possono effettuare manutenzioni in loco con i tempi stabili dal contratto o su richiesta di intervento aperta tramite il portale Agorà (DRF per sicurezza logica, workflow di segnalazione problemi sugli immobili e impianti per sicurezza fisica). Preventivamente il fornitore certifica il tipo di intervento e rilascia, in conseguenza dello stesso, regolare rapporto in base agli incarichi ricevuti in relazione al DPS ai sensi del D. Lgs. 196/2003.

6.2. Pianificazione e accettazione del sistema.

Obiettivi: minimizzare il rischio di guasti/disservizi dei sistemi.

- **Capacity Planning (evitare guasti/disservizi per risorse non adeguate)**: Credemtel Spa tiene costantemente sotto controllo la capacità del sistema informatico rispetto a:
    a. necessità degli utenti,
    b. attività svolte,
    c. naturale obsolescenza delle risorse (asset).

  Periodicamente, in occasione del Riesame della Direzione sono valutate le proiezioni future di capacità del sistema informativo.
- **Accettazione dei sistemi:** tutti i sistemi hardware e software acquistati nuovi, sono registrati e assegnati come previsto da procedura **PRO08 Manutenzione**. Il RSS ha la responsabilità di verificare la sicurezza delle nuove applicazioni e pianificarne l'installazione sulle macchine

operative. Gli aggiornamenti relativi ai programmi preinstallati o approvati dall'ufficio SEI (es. MS Office, MS Dev Studio ecc.), non subiscono particolari verifiche.

6.3. Protezione dal software dannoso.

Obiettivi: proteggere l'integrità del software di base e delle informazioni.

- **Controlli contro software dannoso**: tutti i PC sono dotati di antivirus per ogni singola macchina con aggiornamento automatico delle impronte virali, gestito in outsourcing dall'Ufficio SEI della Capogruppo che ha la responsabilità e l'autonomia di definirne le tempistiche e verificarne l'adeguatezza.
    - **Sensibilizzazione del personale al problema del software dannoso:** l'assegnatario di computer e dispositivi mobili è responsabile del loro buon funzionamento ed è quindi tenuto a non modificare l'hardware/software installato e a non scaricare alcun file dannoso attraverso il collegamento internet come definito nel **Disciplinare per l'uso dei dispositivi informatici e dei sistemi di comunicazione elettronica e disposizioni di carattere generale in materia di risorse informatiche** allegato alla procedura **PRO20 Gestione sicurezza logica**. In caso di "infezione" da virus l'assegnatario deve immediatamente comunicare l'incidente come indicato nella già citata procedura PRO20.

6.4. Gestione operativa quotidiana per mantenere integrità e disponibilità (Housekeeping).

Obiettivi: assicurare la disponibilità dei processi di elaborazione dell'informazione e di comunicazione.

- **Backup**: sono effettuati dall'outsourcer del sistema informativo e controllati secondo quanto indicato nella procedura **PRO08 Manutenzione**.

  La procedura agisce ovviamente in sintonia con la procedura **PRO17 Erogazione dei Servizi** e **IST-17-06 Manuale di gestione del Disaster Recovery** e prevede le modalità di ripristino dei dati salvati.
- **Log operativi**: tutte le operazioni svolte sulla rete interna di Credemtel Spa da parte dei PC collegati sono registrate sul log di WINDOWS.
- **Guasti e interruzioni di servizio**: tutti i malfunzionamenti e le interruzioni vengono registrati sul Registro Incidenti IT e gestiti in accordo con l'istruzione **IST-17-03 Gestone incidenti IT** della procedura **PRO17 Erogazione del servizio**.
- **Connessioni ai sistemi da parte dei clienti**: per il monitoraggio delle connessioni applicative da parte dei clienti, sono usati i log dei singoli servizi applicativi mentre il log del firewall è demandato a Sicurezza Logica (ufficio SIL della capogruppo CREDEM).

6.5. Gestione rete.

Obiettivi: garantire la salvaguardia delle informazioni in rete e la protezione delle infrastrutture di rete.

- **Controlli per protezione dati sulla rete**: i PC sono tutti collegati in rete locale (LAN) e i dati aziendali sono di norma mantenuti presso appositi server, qualora l'utente necessiti di caricare dati in locale occorrerà verificare preventivamente che l'hard disk sia cifrato. I computer sono sempre accesi durante l'orario di lavoro, quindi vi è un controllo continuo sulla funzionalità della rete.
  Nell'eventualità vi sia richiesta di acceso alla rete da parte di personale esterno a questi dovrà essere preventivamente attivato un utente di rete, di norma il PC del personale esterno non è autorizzato a connettersi ai domini del gruppo CREDEM ma solo alle singole risorse autorizzate per l'utenza assegnata.
  L'accesso alla rete wi-fi è protetto da certificato di sicurezza di norma concesso solo al personale del gruppo CREDEM.
  Protezione dei dispositivi di rete: i dispositivi di rete sono protetti in appositi armadi chiusi a chiave nella sala server ad accesso controllato o in altri locali chiusi o meno a chiave gestiti in outsourcing dalla capogruppo CREDEM.

6.6. Movimentazione e sicurezza delle unità.

Obiettivi: evitare la perdita, modifica o uso improprio delle informazioni scambiate in rete.

- **Gestione dei supporti removibili**: l'utilizzo di supporti rimovibili è regolamentato dal **Disciplinare per l'uso dei dispositivi informatici e dei sistemi di comunicazione elettronica e disposizioni di carattere generale in materia di risorse informatiche** allegato alla **PRO20 Gestione sicurezza logica**.
- **Dismissione dei supporti**: i supporti rimovibili che contengono dati non più essenziali, vengono distrutti secondo la Procedura **PRO08 Manutenzione Istruzione IST-08-03 Cessazione supporti rimovibili**.
- **Protezione della documentazione di configurazione del sistema**: lo **Schema dell'architettura fisica della rete** allegato alla procedura **PRO19 Gestione sicurezza fisica** contiene uno schema fisico della rete. Le informazioni di configurazione sono gestiti in outsourcing dall'ufficio SEI della Capogruppo e, per la parte di competenza, dall'outsourcer del sistema informativo che gestisce il servizio. Il backup viene gestito dall'outsourcer presso la sua sede, inoltre il backup viene gestito tramite l'applicazione "Tivoli" che non utilizza supporti fisici rimovibili ma partizioni dedicate su disco fisso.

6.7. Scambio di informazioni e software.

Obiettivi: prevenire perdita, modifica, o uso improprio di informazioni nello scambio di informazioni tra organizzazioni.

- **Accordi per lo scambio di informazioni e software tra organizzazioni (clienti, società collegate, altre sedi aziendali, ecc.):** Credemtel Spa distribuisce il software e le soluzioni con le seguenti modalità:
  a. Utilizzo diretto di applicazioni web che non necessitano di installazione;
  b. Installazione diretta presso il cliente da parte di tecnico interno o esterno all'uopo incaricato;
  c. Installazione/aggiornamenti da parte di personale tecnico interno tramite connessione telematica ai PC del cliente da remoto (tramite sw GoToAssist).
- **Misure di protezione per i supporti durante il trasporto:** si effettuano aggiornamenti di software tramite connessione telematica sicura e registrata direttamente sulla postazione del cliente (tramite sw GoToAssist).
- **E-mail:** il server dedicato alla posta è esterno, in quanto servizio in outsourcing.
- **Sicurezza legata ai sistemi elettronici dell'ufficio:** il regolamento **Codice di comportamento interno** e **il Disciplinare per l'uso dei dispositivi informatici e dei dispositivi di comunicazione elettronica e disposizioni di carattere generale in materia di risorse informatiche** allegato alla **PRO20 Gestione sicurezza logica** indicano le regole di sicurezza che il personale deve adottare relativamente alle attrezzature assegnate.
- **Diffusione di informazioni**: non è ammesso diffondere informazioni aziendali di qualsiasi natura. I dati personali dei dipendenti sono conservati solo per scopi retributivi previsti dalla normativa vigente e per i quali si prende a riferimento la normativa nazionale.
- **Protezione delle informazioni da modifiche non autorizzate:** i dati aziendali sono di norma mantenuti presso appositi server. Gli utenti possono accedere e modificare i dati di solo loro competenza. La protezione dei dati è a cura del sistema operativo mediante l'utilizzo delle credenziali assegnate (utente e password).
- **Sicurezza di altre forme di scambio di informazioni (fax, video, voce):** i fax arrivano alle macchine fax e successivamente dirottati al personale interessato.

7. Controllo degli accessi (System Access Control)

7.1. Requisiti di sistema per il controllo degli accessi.
Obiettivi: controllare l'accesso alle informazioni.

- **Politica del controllo degli accessi:** il RSS definisce, in accordo con SIL, la politica degli accessi sulla base delle attività da svolgere. I permessi e i privilegi sono riservati alle varie tipologie di utenti interni. Gli utenti accedono ai files contenuti nel proprio computer o nel server di rete secondo i privilegi legati ai files stessi e quelli relativi al proprio gruppo di utenza. Ogni attività svolta sulla rete interna da parte dei PC collegati sono registrate sul log di Windows. Per il monitoraggio delle connessioni applicative da parte dei clienti, sono usati i log dei singoli servizi applicativi.

7.2. Gestione dell'accesso da parte degli utenti.
Obiettivi: prevenire l'accesso non autorizzato alle informazioni;

- **Registrazione dell'utente**: l'istruzione **IST-10-01 Processo di inserimento personale in azienda** della procedura **PRO10 Gestione della formazione** definisce le modalità di censimento di un nuovo utente.
- **Gestione dei privilegi**: il RSS prescrive le regole di definizione dei privilegi di accesso sui documenti disponibili in rete. Il reparto SEISLO (CREDEM), ingaggiato tramite apposito workflow autorizzativo (DRF), si occupa dell'assegnazione di detti privilegi e i RdF, su richiesta di SIL (CREDEM) hanno in carico la verifica semestrale di congruità e la verifica di utilizzo da parte degli utenti.
- **Gestione della password**: la gestione delle password è prevista nel regolamento **Codice di comportamento interno** e nel **Disciplinare per l'uso dei dispositivi informatici e dei sistemi di comunicazione elettronica e disposizioni di carattere generale in materia di risorse informatiche** allegato alla **PRO20 Gestione sicurezza logica**. In caso di modifiche necessarie ai diritti di accesso il RdF o il RSS provvedono al cambiamento della configurazione dell'utente e ad informare il personale interessato.
- **Revisione dei diritti accesso**: in caso di modifiche necessarie ai diritti di accesso, il RdF o il RSS, provvedono al cambiamento della configurazione dell'utente e ad informare il personale interessato.

7.3. Responsabilità dell'utente.
Obiettivi: prevenire accessi non autorizzati.

- **Uso della password**: l'utente è responsabile della corretta gestione della propria password. Il reparto SEISLO (CREDEM), secondo quanto definito nella **PRO20 Gestione sicurezza logica**, ha l'autorità di resettare detta password se ne è fatta richiesta da parte dell'utente stesso o di altro utente del proprio ufficio tramite un apposito workflow autorizzativo (DRF).
- **Protezioni per apparecchiature non presidiate**: non vi sono di norma apparecchiature non presidiate almeno dal personale presente nell'ufficio. In caso contrario, queste sono conservate nella Sala Server o altri locali aziendali comunque protetti da credenziali di accesso.

7.4. Controllo degli accessi alla rete dall'esterno.
Obiettivi: assicurare la protezione dei servizi in rete.

- **Politica d'uso dei servizi di rete**: il RSS definisce l'uso dei servizi di rete e conferisce la responsabilità della gestione all'utente. Gli utenti accedono ai servizi come indicato nel **Disciplinare per l'uso dei dispositivi informatici e dei sistemi di comunicazione elettronica e disposizioni di carattere generale in materia di risorse informatiche** allegato alla procedura **PRO20 Gestione sicurezza logica**.
- **Autenticazione dell'utente dall'esterno**: i clienti autorizzati accedono previa autenticazione. Le modalità di accesso da computer di clienti remoti sono definite nella procedura **PRO20**

Gestione sicurezza logica Gli utenti autorizzati all'accesso dall'esterno sono i clienti e i fornitori purché formalmente autorizzati via IP o reti interconnesse tramite controllo via firewall. Inoltre possono accedere anche i dipendenti autorizzati al telelavoro o dotati di accesso remoto (sempre autorizzato da GES). Le modalità di accesso sono definite nella procedura **PRO20 Gestione sicurezza logica**.

- **Protezione remota delle porte**: la protezione contro accessi non autorizzati alle singole sottoreti aziendali è garantita da firewall; l'accesso è consentito in funzione dei diritti legati alle proprie credenziali di riconoscimento. La scheda del firewall contiene la configurazione delle protezioni definite.
- **Segregazione di apparecchiature, utenti e informazioni**: attualmente tutti i servizi di rete sono disponibili in funzione all'attività svolta e non ci sono particolari limitazioni.
- **Controlli di connessione dei clienti alla rete**: il RSS, in collaborazione con SIL, ha la responsabilità di controllare le connessioni alla rete sulla base delle richieste di assistenza fatte dai clienti in caso di difficoltà o impossibilità di accedere ai servizi disponibili.
- **Sicurezza apparecchiature e servizi di rete**: le protezioni di ogni asset sono definite nella procedura **PRO19 Gestione sicurezza fisica**.

7.5. Controllo dell'accesso al sistema operativo.
Obiettivi: prevenire l'accesso non autorizzato ai computer (PC personali e server di rete).

- **Identificazione automatica del terminale**: l'accesso al terminale e la relativa identificazione avvengono con le modalità definite per l'utente di rete nel **Disciplinare per l'uso dei dispositivi informatici e dei sistemi di comunicazione elettronica e disposizioni di carattere generale in materia di risorse informatiche** allegato alla procedura **PRO20 Gestione sicurezza logica**.
- **Procedure di logon del terminale**: il logon al sistema avviene con le modalità definite per l'utente di rete nel **Disciplinare per l'uso dei dispositivi informatici e dei sistemi di comunicazione elettronica e disposizioni di carattere generale in materia di risorse informatiche** allegato alla procedura **PRO20 Gestione sicurezza logica**.
- **Identificazione e autenticazione dell'utente**: le modalità univoche di identificazione e autenticazione dell'utente ai servizi dei rete sono indicate nel **Disciplinare per l'uso dei dispositivi informatici e dei sistemi di comunicazione elettronica e disposizioni di carattere generale in materia di risorse informatiche** allegato alla procedura **PRO20 Gestione sicurezza logica**.

- **Sistema di gestione delle password**: le password dell'utente sono gestite direttamente da lui stesso. Il RdF o il RSS possono disabilitare l'accesso dell'utente attraverso la sospensione o la revoca dell'account, mediante richiesta tramite la procedura PERMUTE all'ufficio SEISLO. È prevista la disabilitazione automatica in caso di non utilizzo delle credenziali per 2 mesi o revoca automatica per cessazione del rapporto di lavoro.
- **Accesso alle sottoreti**: l'accesso delle singole apparecchiature alle diverse sottoreti o parte di esse, viene gestito dai firewall.
- **Tempo massimo di connessione**: non ci sono limiti temporali alle connessioni di rete.

7.6. Controllo dell'accesso alle applicazioni.
Obiettivi: prevenire l'accesso non autorizzato alle informazioni.

- **Restrizione degli accessi**: le restrizioni sono determinate sulla base delle tipologie di utenza alla rete, concordate con l'ufficio SIL della capogruppo che gestisce la sicurezza logica come indicato nella procedura **PRO20 Gestione sicurezza logica**.
- **Isolamento delle apparecchiature critiche**: le apparecchiature critiche (server) vengono segregate in apposita sala server ad accesso riservato o presso l'outsourcer del sistema informativo. Attualmente tutte le apparecchiature hanno accesso alla rete. L'accesso delle singole apparecchiature alle diverse sottoreti o parte di esse, viene gestito dai firewall.

7.7. Monitoraggio dell'accesso ai sistemi.

Obiettivi: rilevazione accessi.

- **Conservazione dei log di accesso ai sistemi applicativi offerti ai clienti**: ci sono vari sistemi di log specifici alle singole Aree; questi log sono a disposizione del personale autorizzato. E' compito del firewall tenere il log di tutto il traffico che intercorre tra le Aree. Questo log è a disposizione dell'Outsourcer e dell'ufficio SIL.
- **Sincronizzazione degli orologi**: i server di dominio sono sincronizzato dall'outsourcer del sistema informativo e le macchine si sincronizzano al loro volta sui server di dominio.

7.8. Computer portatili e telelavoro.

Obiettivi: garantire la sicurezza delle informazioni quando sono utilizzate da eventuali postazioni mobili in rete.

- **Computer portatili**: queste apparecchiature sono utilizzate dall'utente a cui sono state assegnate.
- **Telelavoro**: In caso di necessità, per periodi predefiniti, sono rilasciate autorizzazioni per il telelavoro ad incaricati identificati; a questi sono assegnate le istruzioni in forma scritta e riservata, da parte dell'ufficio GES di CREDEM che provvede a richiedere a SEISLO le autorizzazioni per l'accesso da remoto sul firewall. Le modalità di accesso, sono definite nel **Disciplinare per l'uso dei dispositivi informatici e dei sistemi di comunicazione elettronica e disposizioni di carattere generale in materia di risorse informatiche** allegato alla **PRO20 Gestione sicurezza logica**.

8. Sviluppo e manutenzione dei sistemi (System Development and Maintenance)

8.1. Requisiti di sicurezza dei sistemi.

Obiettivi: garantire che le regole di sicurezza siano realmente attuate nei sistemi informatici in esercizio.

- **Analisi dei requisiti e specifiche di sicurezza**: i sistemi hardware e le relative parti sono coperti da contratti di manutenzione che garantiscono ripristini adeguati alle politiche definite. Gli uffici SIL e SIF di CREDEM hanno la responsabilità di monitorare la sicurezza logica e fisica dei sistemi e possono effettuare modifiche agli stessi, previa autorizzazione da parte del RSS. I dipendenti, in caso di eventuali malfunzionamenti di sicurezza, sono tenuti ad aprire NC sul sistema SECURITY. Eventuali ulteriori specifiche di sicurezza saranno determinate in occasione del Riesame della Direzione.

8.2. Sicurezza dei sistemi applicativi.

- **Validazione dei dati d'ingresso**: i programmi utilizzati in Credemtel Spa ed i prodotti collegati, utilizzano software sviluppato da primarie aziende che vantano lunga esperienza nel settore di competenza. Per i SW sviluppati internamente la validazione segue quanto previsto nella procedura **PRO06 Gestione della progettazione**.
- **Controllo sui processi interni per l'integrità dei dati**: nei servizi per i clienti i dati introdotti ed elaborati vengono validati mediante l'uso di software specifici per garantirne l'integrità. I programmi utilizzati in ambito aziendale, sono costantemente in fase di aggiornamento ed implementazione da parte degli uffici che hanno in gestione i relativi sistemi.

8.3. Controlli crittografici

- **Politica d'uso dei controlli crittografici**: Credemtel Spa utilizza sistemi crittografici per i collegamenti web (HTTPS), il trasferimento dati (FTPS) e la connessione di PC da remoto o tra la rete aziendale e talune specifiche reti dei clienti (Linea cifrata tramite apposito sw controllato dal firewall).

8.4. Sicurezza dei files di sistema.

Obiettivi: assicurare che l'utilizzo di software applicativi di terze parti, e le relative attività di supporto siano eseguite secondo le regole definite nei contratti fornitura.

- **Controlli sul software applicativo**: il software applicativo utilizzato è realizzato da fornitori di primaria importanza e dagli stessi è sottoposto a collaudo prima della distribuzione; la distribuzione di aggiornamenti e/o nuove release, avviene con tutta la documentazione necessaria a supporto di una corretta attività nei successivi aggiornamenti ai propri clienti; con i fornitori dei software primari, sono stipulati contratti di manutenzione.

8.5. Sicurezza nei processi di sviluppo e supporto

- **Interdizione delle modifiche al software**: le modifiche al sistema operativo avvengono esclusivamente a cura di SEI (CREDEM) l'ufficio ha anche il compito di identificare la presenza di programmi non licenziati o da non installare tramite la verifica diretta sulle singole macchine. Le modifiche ai programmi sviluppati vengono effettuate internamente o dai fornitori, a seguito di NC segnalate, dell'implementazione di nuove funzionalità, o cambiamenti di legge.
- **Controllo delle modifiche al software**: tutte le modifiche sono testate a cura dell'ufficio che le ha sviluppate o del fornitore. Di ogni modifica ne viene data comunicazione diretta o indiretta.
- **Affidabilità del codice**: tutto il software utilizzato proviene da fornitori riconosciuti come affidabili.

9. Gestione della continuità del servizio (Business Continuity Management)

Gli obiettivi di questa sezione sono di contrastare le interruzioni delle attività di servizio e dei processi di servizio critici, causati da malfunzionamenti o da eventuali avvenimenti straordinari. Infatti: "Lo scopo del Business Continuity Management è garantire la continuità dei processi dell'Organizzazione in funzione del loro valore e della qualità dei prodotti/servizi erogati tramite il supporto dell'infrastruttura di IT, prevenendo e minimizzando l'impatto di incidenti intenzionali o accidentali e dei conseguenti possibili danni.
Per una corretta gestione del governo delle informazioni i sistemi devono garantire la continuità dei servizi**.**
In caso di eventuali avvenimenti straordinari, devono essere rispettate le seguenti regole:

- le procedure applicative, il software di sistema e gli archivi ad uso dei clienti devono essere ripristinati prioritariamente;
- il piano di continuità prevedere il ripristino delle funzioni definite critiche nella Business Impact Analisys (BIA) e non solo i servizi informatici centrali;
- per assicurare la continuità dei servizi devono essere valutate le strategie di ripristino più opportune.

Aspetti di gestione della Business Continuity:

- **Piano di Continuità (Business Continuity) e analisi degli impatti**: in caso verificarsi di un evento di crisi configurabile nello scenario di massima gravità, viene convocato il Comitato di Crisi che, valutato il danno, attiverà il Piano di Continuità come definito nell'istruzione operativa **IST-17-08 Piano di continuità operativa** della procedura **PRO17 Erogazione dei servizi**. In occasione del Riesame della Direzione, si valutano gli impatti dei malfunzionamenti e si verificano le eventuali azioni correttive intraprese nell'ambito del ripristino della continuità del business. Credemtel Spa, conformemente con quanto previsto dalla normativa AgID, ha stipulato un'assicurazione per la responsabilità civile verso terzi nell'ambito delle attività professionali di gestione della conservazione documentale.
- **Redazione ed implementazione di Piani di Continuità**: in occasione del Riesame della Direzione viene verificato il piano di continuità aziendale, la cui implementazione attuale è contenuta nell'istruzione **IST-17-08 Piano di Continuità Operativa** della procedura **PRO17 Erogazione dei servizi**.
- **Struttura di pianificazione Piano di Continuità**: il BCM verifica che le misure in atto siano sempre adeguate e nel contempo ricava eventuali suggerimenti per l'adeguamento del Piano di Continuità.
- **Test, mantenimento e modifiche del Piano di Continuità**: il BCM coordina l'effettuazione annuale dei test di funzionamento dei processi critici in sede di recovery per assicurarsi che le condizioni di base della Business Continuity siano integre (assessment dei danni subiti e provvedimenti immediati). Inoltre, sulla base delle NC rilevate nel periodo, determina se vi siano delle nuove condizioni che possano portare a danneggiamenti importanti per il business aziendale.

10. Conformità (Compliance)

10.1. Conformità a requisiti legali.

Obiettivi: garantire il rispetto delle leggi civili, penali, obblighi statutari, regolamentari o contrattuali e di qualsiasi requisito di sicurezza.

- Identificazione di requisiti legali applicabili: la normativa è presidiata dalla funzione AGL che si avvale della collaborazione continuativa dell'ufficio legale (LEG) di CREDEM e altri studi legali che provvedono anche all'individuazione delle normative applicabili. In particolare, per quanto riguarda la sicurezza dei dati e delle Informazioni, la normativa italiana prevede l'applicazione delle fonti indicate nell'istruzione operativa **IST-17-01 Manuale di Conservazione** della procedura **PRO17 Erogazione dei servizi**.
- Diritti di proprietà intellettuale: per i prodotti software acquisiti si fa riferimento alla procedura **PRO08 Manutenzione** per quanto riguarda la gestione delle licenze software, che copre anche l'aspetto dei controlli periodici.
- Salvaguardia di Verbali e altre informazioni organizzative: la documentazione organizzativa aziendale (statuto, visura camerale, verbali del Consiglio di Amministrazione) è conservata presso l'ufficio SEG di CREDEM.
- Privacy e protezione dei dati personali e sensibili: sono state definite le modalità di gestione dei dati personali e sensibili. Credemtel Spa in qualità di titolare del trattamento definisce le regole di sicurezza per tali dati. Credemtel Spa ha nominato anche un Responsabile del trattamento che informa gli incaricati del trattamento ed effettua i controlli periodici su questi ultimi.
- Uso appropriato e autorizzato dei servizi di IT: l'utilizzo delle risorse aziendali è gestito attraverso politiche aziendali e regolamentato nel **Disciplinare per l'uso di dispositivi informatici e dei sistemi di comunicazione elettronica e disposizioni di carattere generale in materia di risorse informatiche** allegato alla **PRO20 Gestione sicurezza logica**. Per ogni abuso, laddove non costituisca reato, si applicano le norme disciplinari previste dal contratto di lavoro.
- Regolamentazione dei controlli crittografici: l'azienda utilizza servizi crittografici.
- Evidenza oggettiva: laddove la conservazione di documenti in formato elettronico abbia valore legale, l'azienda fornisce annualmente o su richiesta al cliente un attestato di conservazione dei documenti medesimi.

10.2. Risultati delle Valutazioni del Sistema.

- Controlli sull'efficacia del sistema: Credemtel Spa considera gli audit interni un esame sistematico necessario a verificare se quanto previsto dal SGSI è conforme alla Politica per la Sicurezza e se quanto predisposto e pianificato trova effettiva applicazione. Il RAQ pianifica e programma con cadenza annuale tutti gli audit interni.
  Nella definizione del campo di indagine e delle frequenze delle verifiche, dovranno essere considerati anche i risultati di precedenti audit, i reclami dei clienti, le azioni correttive apportate.
  Le valutazioni interne sono condotte dal personale opportunamente formato.
  I risultati della verifica devono essere verbalizzati dall'Auditor Interno. Al RSS spetta la responsabilità della risoluzione delle NC rilevate e la definizione di adeguate azioni correttive e preventive per la risoluzione delle carenze individuate.
  Per la gestione delle verifiche interne è stata emessa la procedura **PRO11 Audit Interno**.
- Conservazione della documentazione: tutta la documentazione utile per l'audit interno quale:
  a. check list
  b. verbali
  c. registrazioni di NC
  d. registrazioni di azioni correttive e preventive

  è opportunamente conservata dall'azienda e ne ha accesso tutto il personale aziendale autorizzato.

10.3. Riesame della Politica per la Sicurezza e conformità tecnica assicurare la conformità dei sistemi con i criteri e gli standard di sicurezza nazionali ed internazionali.

- **Conformità con la Politica per la Sicurezza**: annualmente il RAQ esegue le valutazioni interne di verifica della compatibilità alla Politica per la Sicurezza e della conformità di quest'ultima ai Requisiti della norma ISO/IEC 27001:2014 e a quanto prevista da DPCM 3 dicembre 2013 e, quindi, inerenti quanto definito nell'ambito del Codice dell'Amministrazione Digitale (D.Lgs. 7 marzo 2005, n. 82 e successive modificazioni).
- **Controlli di Conformità tecnica:** il CS INTEC dispone che SEI (CREDEM) verifichi con cadenza massima annuale che software installato sia freeware o coperto da copyright. Il servizio INTEC verifica che l'hardware installato corrisponda a quanto esistente nella documentazione. Le infrastrutture vengono controllate (impianti antifurto, ecc.) dagli outsourcer che le hanno in manutenzione inoltre il CS INTEC e il RSS verificheranno la loro corrispondenza a quanto riportato rispettivamente nella procedura **PRO08 Manutenzione** e nella procedura **PRO19 Gestione sicurezza fisica**. Il RAQ verifica che le procedure siano in linea con quanto stabilito dal Comitato Sicurezza. Infine, le registrazioni relative alla gestione degli incidenti e NC completano il quadro della situazione.
- **Valutazione del rischio informatico:** sulla base dei dati raccolti il Comitato Sicurezza rivaluta criticamente i seguenti elementi:
    a. minacce presenti;
    b. probabilità di accadimento delle minacce e loro gravità;
    c. contromisure adottate;
    d. accettabilità del rischio residuo;
    e. opportunità di rafforzare o introdurre nuove contromisure.
- **Miglioramento continuo**: al termine del Riesame della Direzione, DIR valuta ed approva le opportune azioni correttive e/o di miglioramento.