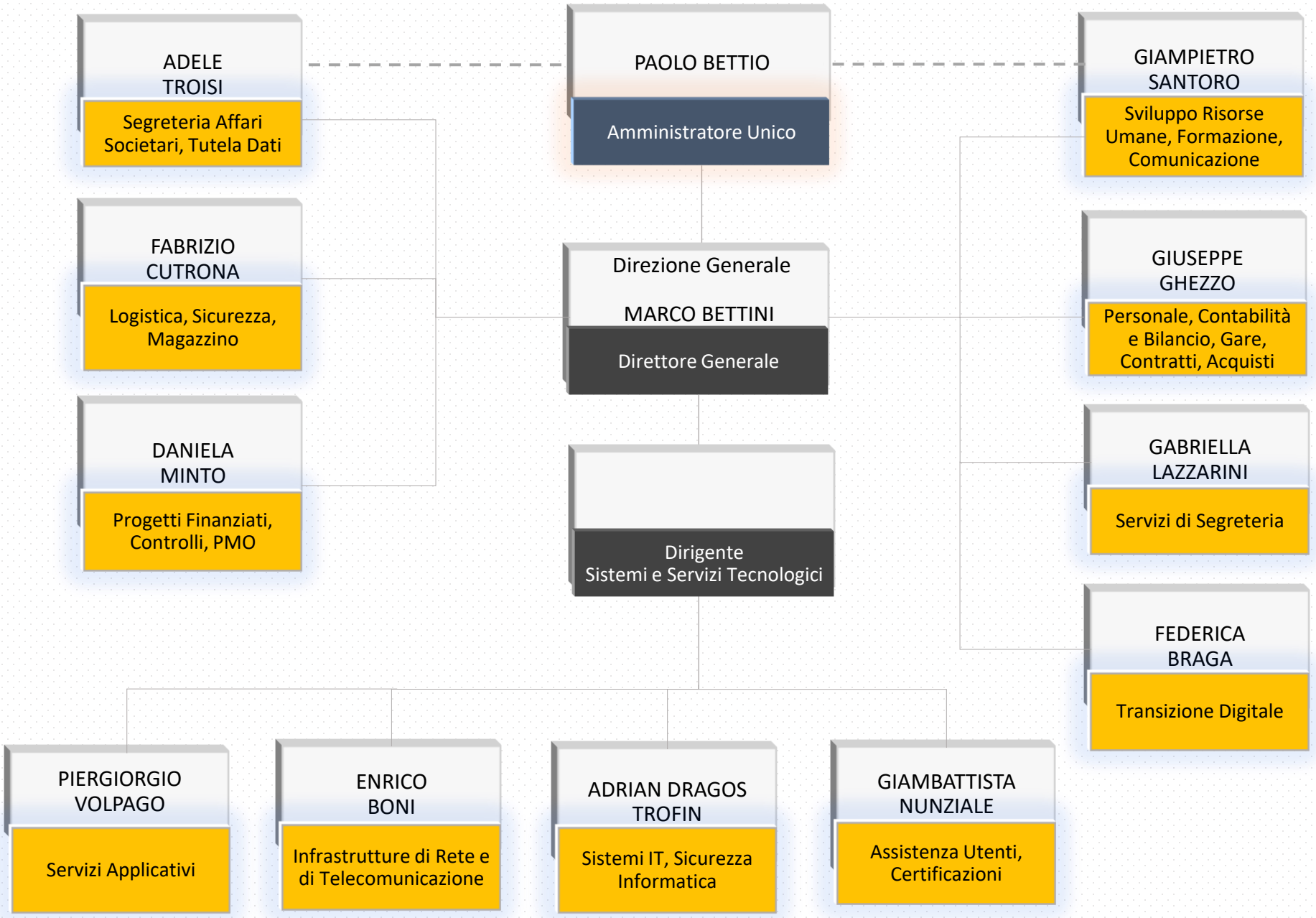
Allegato 1 -

Macrostruttura e Uffici

Macrostruttura Organizzativa

Gennaio 2026



Allegato 2

Provvedimenti di nomina

DISPOSIZIONE ORGANIZZATIVA

Al Direttore Generale sono conferiti i poteri gestionali ai sensi dell'art. 24 dello Statuto aziendale.

Il **Direttore Generale** sovrintende e provvede alla gestione e all'amministrazione della società e a quant'altro nell'interesse della società, salvo quanto non espressamente previsto nelle procure conferite.

Il Direttore Generale sottopone il resoconto dell'attività svolta, delle iniziative intraprese e dei risultati raggiunti, per iscritto, semestralmente all'Organo Amministrativo e se del caso al Collegio Sindacale e al Comitato di Coordinamento e Controllo e comunque provvede a rendicontare in ogni momento, a specifica richiesta.

Il Direttore Generale è coadiuvato nella gestione ordinaria dal Condirettore Generale, a cui è altresì affidata la responsabilità della Direzione Operazioni.

In data 23 novembre 2020 l'Assemblea ordinaria degli azionisti di VENIS S.p.A., per effetto delle dimissioni del Direttore Generale a far data dal 1° dicembre 2020, ha conferito al Condirettore Generale deleghe e relativi poteri del Direttore Generale.

L'Unità **Segreteria Affari Societari riporta funzionalmente direttamente all'Organo Amministrativo**, per le attività di competenza.

Segreteria Affari Societari, Tutela Dati
affidata a Adele Troisi, con il compito di:

- assicurare l'espletamento di tutti gli adempimenti societari;
- coadiuvare le attività degli organi statutari, compreso il Comitato di Coordinamento e Controllo ex. Art. 29 dello statuto sociale, convocandone le riunioni, predisponendo ed istruendo gli argomenti di discussione, curando la verbalizzazione delle sedute e provvedendo agli adempimenti conseguenti con facoltà di richiedere, ove necessaria, la collaborazione delle altre funzioni aziendali;
- curare l'archiviazione della documentazione societaria e della conservazione dei libri sociali;
- coordinare le azioni per il rispetto della normativa in tema di Trasparenza Amministrativa, di Prevenzione della Corruzione e garantisce il rispetto del Modello Organizzativo ai sensi del D. Lgs. 231/2001 curando i rapporti con l'Organismo di Vigilanza;
- assicurare l'efficienza del sistema aziendale in tema di tutela delle informazioni, dei dati personali e dei dati aziendali;
- collaborare con tutte le funzioni aziendali ed in particolare con il Responsabile Risorse Umane, Formazione e Comunicazione per la elaborazione e redazione dei regolamenti interni;
- coadiuvare l'Organo Amministrativo e la Direzione Generale, per le rispettive competenze, nella redazione delle comunicazioni ai soci, agli organi sociali e alle pubbliche amministrazioni.

Al **Condirettore Generale Marco Bettini** riportano direttamente le seguenti **Unità**:

Sviluppo Risorse Umane, Formazione, Comunicazione
affidata a Giampietro Santoro, con il compito di:

- definire i processi aziendali e lo sviluppo e valorizzazione delle risorse umane, prevenendo ed evidenziando situazioni di criticità e proponendo lo sviluppo di nuove competenze e/o soluzioni organizzative;
- condurre tutte le attività relative alla gestione del personale dipendente e delle risorse umane, incluse quelle relative alla redazione e aggiornamento di regolamenti e disposizioni, nonché della informazione e assistenza riguardo le disposizioni contrattuali ed eventuali novazioni;
- coadiuvare il Direttore Generale nelle relazioni con le Rappresentanze Sindacali;
- coordinare la redazione ed organizzare l'implementazione del Piano di Formazione aziendale, identificando le esigenze tecnico-specialistiche in coordinamento con le strutture aziendali;
- coadiuvare la Direzione Operazioni per la definizione ed eventuale organizzazione delle attività di formazione da erogare ai Clienti su sistemi e servizi gestiti dalla Società;
- occuparsi della gestione e promozione dell'immagine aziendale nei confronti dei media e delle istituzioni, presidiando i siti web e account social della società, e supportando l'Organo Amministrativo e la Direzione nelle relazioni con l'esterno e con i mezzi di informazione, anche in coordinamento con le strutture comunali di competenza;
- definire contenuti e programmi per l'organizzazione di eventi e attività di relazione esterna aziendale e coadiuvare la Segreteria di Direzione per l'organizzazione.

L'Unità Sviluppo Risorse Umane, Formazione, Comunicazione riporta funzionalmente anche all'Organo Amministrativo.

Acquisti, Contratti, Amministrazione e Bilancio
affidata a Giuseppe Ghezzo, con il compito di:

- gestire le procedure per l'affidamento di forniture di beni e servizi, secondo la normativa vigente;
- gestire le procedure di gare ad evidenza pubblica, coordinando la predisposizione dei bandi e degli atti di gara, sovrintendendo al lavoro delle commissioni aggiudicatrici, adempiendo agli obblighi di natura pubblicistica, e provvedendo alla predisposizione dei contratti di appalto, anche avvalendosi di *service infragruppo* comunale o altre stazioni appaltanti nell'ambito dei Soci aziendali;
- predisporre i contratti di acquisto e vendita;
- curare la contabilità generale e supportare il Direttore Generale nella redazione del bilancio e delle situazioni infrannuali;
- presidiare la gestione finanziaria della società e i rapporti con le banche;
- ottemperare agli adempimenti fiscali;
- ottemperare agli adempimenti previdenziali e retributivi del personale;
- gestire il sistema di controllo di gestione curando le fasi di rendicontazione amministrativa delle attività al Cliente, nonché prevedendo ed evidenziando situazioni di rischio e/o inefficienza nella gestione delle commesse.

Segreteria di Direzione
affidata a Gabriella Lazzarini, con il compito di:

- coordinare e gestire il pool di segreteria aziendale a supporto degli organi sociali e della Direzione, inclusi gli spazi riunione comuni.
- è Responsabile della gestione documentale, ai sensi del DPCM 3 dicembre 2014 e gestisce e coordina il protocollo e tutta la gestione documentale dell'azienda, incluse le regole su modelli e flussi sia interni che esterni.
- coordinare l'organizzazione di seminari, conferenze, eventi aziendali e della partecipazione dell'Organo Amministrativo e della Direzione ad attività seminariali,

convegnistiche, di studio e scambio pratiche con altri enti nazionali, locali e internazionali, ed in generale nelle attività di relazione esterne.

Alla sig.ra Lazzarini è anche affidato l'incarico di Responsabile della gestione documentale, ai sensi del DPCM 3 dicembre 2014.

Sviluppo Offerta

affidata a Federica Braga, con il compito di:

- predisporre e curare ogni offerta e proposta di nuove attività di sviluppo per i Clienti;
- coordinare e sovraintendere le attività relative al progetto SAD Metropolitano (POR FESR Asse 2 – Agenda Digitale) e al nuovo sistema di Contabilità.

Progetti Finanziati, Controlli, PMO

affidata a Daniela Minto, con il compito di:

- coordinare i rapporti con i committenti istituzionali, le attività gestionali e lo stato avanzamento lavori per eventuali programmi speciali (es. Progetti europei, PON Metro, Progetti co-finanziati);
- identificare e gestire opportunità di finanziamento per progetti innovativi;
- definire e gestire la metodologia aziendale per project management delle commesse;
- definire processi e standard aziendali in materia di gestione di commesse/progetti e le procedure per favorire il controllo della produttività delle attività di delivery.
- monitorare le tempistiche delle commesse e l'utilizzo delle risorse assegnate, valutando la produttività e le performance delle commesse, evidenziando situazioni di rischio e/o inefficienza nella gestione delle commesse ai fini della loro prevenzione/correzione;
- collaborare con l'Unità Personale, Contabilità e Bilancio, Gare, Contratti, Acquisti sul sistema di controllo di gestione, supportando le fasi di rendicontazione amministrativa delle attività al Cliente;
- elaborare la reportistica per la consuntivazione delle attività della società, e in particolare della relazione annuale di attività per il Comune di Venezia;
- coadiuvare la Direzione Generale nelle attività di analisi funzionale e gestione dell'outsourcing per i progetti complessi.

Logistica, Sicurezza, Magazzino

affidata a Fabrizio Cutrona, con le seguenti responsabilità:

- presidiare e gestire gli interventi per i servizi di sede e più in generale tutti i servizi necessari al funzionamento aziendale, prevenendo, pianificando e gestendo tutti gli interventi necessari all'efficiente funzionamento delle strutture e degli impianti nelle sedi aziendali;
- presidiare e gestire tutte le attività per il rispetto delle normative in tema di sicurezza del lavoro ai sensi del D.Lgs 81/2008;
- presidiare e coordinare ogni attività legata alla gestione del magazzino aziendale;
- presidiare coordinare e garantire i diritti di accesso a strutture e apparati funzionali alla continuità operativa dei servizi gestiti dall'azienda

Certificazioni, Sistema Informativo Aziendale

affidata a Giambattista Nunziale, con le seguenti responsabilità:

- presidiare, indirizzare, coordinare e gestire il Sistema Informativo Aziendale e la sua evoluzione, anche in coordinamento con le altre Unità aziendali;
- definire l'evoluzione del Sistema Informativo Aziendale per una più efficace gestione della pianificazione e del monitoraggio delle performances, relazionandosi con l'Unità Progetti Finanziati, Controlli, PMO;
- presidiare, promuovere e gestire le attività relative all'acquisizione e al mantenimento delle certificazioni necessarie alla ottimale operatività aziendale, anche coordinando quanto dovuto per le ispezioni annuali e revisionando e aggiornando processi e modelli, in un'ottica di semplificazione e funzionalità.

Al Condirettore Generale è affidata anche la **Direzione Operazioni**, con il compito di:

- assicurare la corretta e puntuale gestione di tutte le commesse assegnate alla società;
- curare le relazioni con i Clienti e analizzarne esigenze e fabbisogni;
- definire le linee di sviluppo e innovazione per la pianificazione industriale e i piani operativi dell'azienda;
- coordinare e sovraintendere le attività delle linee di competenza e, in particolare, lo sviluppo delle applicazioni, l'esercizio di sistemi e reti, la gestione dei servizi, l'assistenza tecnica e applicativa, e la loro gestione operativa;
- coordinare le attività svolte dai Responsabili delle Unità Operative e assicurare il corretto svolgimento delle attività di dispiegamento dei servizi;
- gestire il rapporto con il Comune di Venezia per le attività di conduzione, manutenzione e sviluppo del Sistema Informativo Comunale, sottoscrivendo preventivi, offerte e, più in generale, ogni documento funzionale alla gestione e sviluppo del sistema;
- autorizzare l'acquisto di beni mobili, servizi, lavori e macchinari in genere, ad esclusione di contratti di consulenza, nell'ambito del budget operativo approvato dal Direttore Generale per le aree di competenza e nel rispetto della normativa vigente, dei regolamenti e delle procedure aziendali, e nei limiti delle procure conferitigli;
- gestire il rapporto con fornitori terzi per l'approvvigionamento di beni, servizi, lavori e macchinari in genere, nell'ambito del budget operativo approvato per le aree di competenza e nel rispetto dei regolamenti e delle procedure aziendali;
- sovraintendere all'andamento delle unità a suo diretto riporto, elaborando le direttive, promuovendo, coordinando e gestendo l'organizzazione, il personale ed il funzionamento delle Unità Operative, provvedendo a tutto quanto si renderà necessario ed opportuno per assicurare il regolare svolgimento dell'attività, incluso il supporto al coordinamento dei team di progetto delle Unità Operative, in funzione degli obiettivi e in coerenza con i piani aziendali approvati;
- elaborare e proporre all'Unità Sviluppo Risorse Umane, Formazione e Comunicazione i piani di aggiornamento professionale e di training on the job, sentiti i Responsabili delle Unità Operative a riporto, al fine di garantire una costante crescita delle competenze delle risorse assegnate;
- sovrintendere alla gestione del personale della propria Direzione, nell'ambito dell'applicazione del contratto collettivo e degli accordi e regolamenti aziendali;
- garantire i livelli di servizio attesi dalla produzione, in coerenza con i piani e gli indirizzi dell'Azienda e dei contratti stipulati, anche tenendo conto delle raccomandazioni e segnalazioni dell'Unità Progetti Finanziati, Controlli, PMO.

Rispondono alla Direzione Operazioni le seguenti **Unità Operative**:

Infrastrutture di Rete e di Telecomunicazione

affidata a Enrico Boni, con le seguenti responsabilità:

- gestire la produzione di tutte le commesse di competenza, garantendone standard e tempistiche di rilascio, definendo i gruppi di progetto per ciascuna commessa e il relativo personale impiegato, con il supporto del Direttore Operazioni;
- indirizzare e guidare lo sviluppo tecnologico dei sistemi e servizi di telecomunicazione e trasmissione dati dell'azienda;
- identificare e valutare le tecnologie più adeguate alla erogazione dei servizi dell'azienda;
- proporre gli standard aziendali tecnologici per i sistemi di rete e telecomunicazioni;
- progettare e/o coordinare la progettazione (quando esterna) delle infrastrutture ed i sistemi di rete locale, metropolitana e geografica ed i servizi di telecomunicazione, anche identificando scenari e proposte di miglioramento;
- predisporre progetti di fattibilità ed esecutivi per il dominio di competenza;

- predisporre i capitolati tecnici per gli approvvigionamenti relativi al dominio di competenza;
- produrre la documentazione tecnica relativa al dominio di competenza;
- contribuire, per la parte relativa al dominio di competenza, all'analisi delle esigenze finalizzata alla predisposizione delle offerte tecniche per nuove attività/proposte/progetti;
- garantire la realizzazione, collaudo, gestione e manutenzione delle infrastrutture e dei sistemi di rete locale, metropolitana e geografica;
- coordinare le attività, anche amministrative, relative alla Telefonia Fissa e Mobile, curare la progettazione e la conduzione dei sistemi complessi di telefonia IP e di videoconferenza;
- gestire il servizio di assistenza e manutenzione di sistemi e centralini telefonici;
- collaborare con la Direzione Operazioni nella definizione di progetti esecutivi e per il rispetto dei requisiti tecnologici per il proprio dominio di competenza;
- coadiuvare la Direzione Operazioni nell'individuazione delle soluzioni da adottare e degli approvvigionamenti esterni che dovessero rendersi necessari;
- supervisionare le attività e l'allocazione dei tempi di lavoro di tutte le risorse umane assegnate e degli eventuali fornitori esterni;
- garantire i livelli di servizio attesi in coerenza con i piani dell'Azienda e dei contratti stipulati;
- collaborare alla redazione dei budget di spesa per il piano annuale per la parte relativa al dominio di competenza.

ICT Factory, Innovazione, Sviluppo Progetti

affidata a Paolo Cotti Cometti, con le seguenti responsabilità:

- gestire la produzione di tutte le commesse di competenza, garantendone standard e tempistiche di rilascio, definendo i gruppi di progetto per ciascuna commessa e il relativo impiego di personale, con il supporto del Direttore Operazioni;
- indirizzare e guidare gli standard per lo sviluppo software dell'azienda;
- proporre gli standard aziendali tecnologici per le architetture e gli sviluppi software;
- realizzare, coordinare eventuali fornitori esterni, collaudare, mettere in esercizio e manutenere soluzioni software per i Clienti e per l'Azienda (Cliente interno);
- riorganizzare e gestire il supporto specialistico (ticketing) di secondo livello necessario alla conduzione delle applicazioni gestionali e dei servizi in esercizio presso il Comune di Venezia e gli altri Clienti;
- predisporre progetti di fattibilità ed esecutivi;
- predisporre i capitolati tecnici per gli approvvigionamenti relativi al dominio di competenza;
- produrre la documentazione tecnica relativa al dominio di competenza;
- contribuire, per la parte relativa al dominio di competenza, all'analisi delle esigenze e predisporre offerte tecniche per nuove attività/proposte/progetti;
- collaborare con la Direzione Operazioni nella definizione dei progetti esecutivi e per il rispetto dei requisiti tecnologici per il proprio dominio di competenza;
- proporre soluzioni innovative e di eccellenza per adeguare e migliorare i servizi esistenti;
- sviluppare, presidiare e gestire progetti strategici che richiedono la collaborazione di tutte le Unità Operative (es. Piattaforma CzRM DIME, Smart Control Room, …);
- coadiuvare la Direzione Operazioni nell'individuazione delle soluzioni da adottare e degli approvvigionamenti esterni che dovessero rendersi necessari;
- supervisionare le attività e l'allocazione dei tempi di lavoro di tutte le risorse umane assegnate e degli eventuali fornitori esterni;
- garantire i livelli di servizio attesi in coerenza con i piani dell'Azienda e dei contratti stipulati;

- collaborare alla redazione dei budget di spesa per il piano annuale per la parte relativa al dominio di competenza.

Sistemi IT, Sicurezza Informatica, Assistenza Utenti
affidata ad Antonio Pezuol, con le seguenti responsabilità:

- gestire la produzione di tutte le commesse di competenza, garantendone standard e tempistiche di rilascio, definendo i gruppi di progetto per ciascuna commessa e il relativo impiego di personale, con il supporto del Direttore Operazioni;
- supervisionare le attività e l'allocazione puntuale dei tempi di lavoro di tutte le risorse umane assegnate e degli eventuali fornitori esterni;
- definire e garantire l'applicazione delle politiche di sicurezza informatica;
- fornire supporto in ambito privacy;
- è responsabile della sicurezza dei sistemi e dei dati e garantisce la supervisione tecnica delle infrastrutture tecnologiche centrali (Data Centre), anche supervisionando eventuali soggetti esterni/fornitori di servizi;
- indirizzare e guidare lo sviluppo tecnologico dei sistemi centrali e periferici;
- identificare e valutare le tecnologie più adeguate per i sistemi centrali e periferici;
- definire gli standard aziendali tecnologici per i sistemi centrali e periferici;
- progettare l'infrastruttura tecnologica di Sistemi Informativi centrali e periferici, anche identificando scenari e proposte di miglioramento;
- realizzare e manutenere nel tempo l'infrastruttura tecnologica di Sistemi Informativi centrali e periferici, attraverso la conduzione tecnico-sistemistica dei sistemi in carico e delle basi dati, nel rispetto degli standard;
- supervisionare il funzionamento e l'evoluzione dei sistemi di messaging, collaboration e posta elettronica, Identity Management e condivisioni di rete, sistemi DNS e di gestione dei dati e dei relativi backup;
- garantire i servizi di sicurezza a protezione delle infrastrutture ICT per tutto il patrimonio di sistemi e servizi ospitati presso il Data Centre;
- definire e pianificare i fabbisogni di approvvigionamento hardware, per una corretta ed efficiente conduzione dei servizi di informatica distribuita e assistenza tecnica;
- gestire il servizio di assistenza tecnica dei dispositivi HW e SW per i Clienti, anche attraverso le attività di installazione di dispositivi hardware (HW) e componenti software (SW) e il presidio delle installazioni distribuite (sale riunioni, consiglio, sale stampa);
- gestire l'assistenza alle postazioni di lavoro ed il fleet management;
- garantire l'assistenza utente per i sistemi di messaging, collaboration e posta elettronica, Identity Management e condivisioni di rete;
- gestire la logistica delle sale dati del Data Centre, monitorando i servizi critici ed i parametri ambientali ed energetici;
- predisporre progetti di fattibilità ed esecutivi per la parte relativa al dominio di competenza;
- predisporre i capitolati tecnici per gli approvvigionamenti relativi al dominio di competenza;
- produrre la documentazione tecnica relativa al dominio di competenza;
- provvedere all'analisi delle esigenze e predisporre offerte tecniche per nuove attività/proposte/progetti relativi al dominio di competenza;
- collaborare con la Direzione Operazioni nella definizione dei progetti esecutivi e il rispetto dei requisiti tecnologici per il proprio dominio di competenza;
- coadiuvare la Direzione Operazioni nell'individuazione delle soluzioni da adottare e degli approvvigionamenti esterni che dovessero rendersi necessari;
- supervisionare le attività e l'allocazione dei tempi di lavoro di tutte le risorse umane assegnate e degli eventuali fornitori esterni;
- garantire i livelli di servizio attesi in coerenza con i piani dell'Azienda e dei contratti stipulati;

- collaborare alla redazione dei budget di spesa per il piano annuale per la parte relativa al dominio di competenza.

Per il dettaglio delle funzioni svolte dalle diverse Unità si rimanda al documento “Microstruttura funzionale”.

Allegato 3

Guida alla formazione del documento accessibile

Guida pratica per la creazione di un documento accessibile

Il presente documento è tratto, con alcuni adeguamenti al caso di specie, dalla "Guida pratica per la creazione di un documento accessibile", redatta dall'Agenzia per l'Italia Digitale (AgID) il 18 luglio 2016 e aggiornato nel marzo 2017.

Introduzione

Per accessibilità si intende "*la capacità dei sistemi informatici ivi inclusi i siti web e le applicazioni mobili, nelle forme e nei limiti consentiti dalle conoscenze tecnologiche, di erogare servizi e fornire informazioni fruibili, senza discriminazioni, anche da parte di coloro che a causa di disabilità necessitano di tecnologie assistive o configurazioni particolari*" (art. 2, comma 1 lett. a), Legge 4/2004, come modificata dal D.lgs n. 106/2018).

La guida vuole essere di ausilio nella creazione di documenti accessibili pubblicabili *online* sul sito *web* della società. Tali documenti devono risultare accessibili a tutti, secondo la normativa vigente, comprese le persone che usano le tecnologie assistive (ad esempio i lettori vocali di schermo).

Il formato digitale più idoneo a soddisfare l'esigenza di disporre di documenti accessibili *online*, è il **PDF accessibile (PDF/A)**.

È preferibile generare *ab origine* un PDF accessibile (mediante conversione) in quanto **non sono rispondenti ai criteri di accessibilità i PDF derivanti da scansioni di documenti analogici che generano "documenti-immagine" non leggibili dai lettori vocali.**

Si descrivono, nel seguito, i principi base per creare un documento originario accessibile, impostati, a titolo di esempio, sulla versione Word 2010. In generale, essendo tali principi di tipo logico-funzionale, oltre che tecnico-operativo, sono emulabili e realizzabili con alcuni aggiustamenti pratici anche sulla versione Word 2016, segnalati caso per caso. Analogamente, alcuni principi sono applicabili su altri editor di testo di tipo proprietario o Open, nonché su fogli di calcolo e programmi di presentazioni.

I principi base sono raggruppati per i seguenti aspetti principali.

Struttura dei contenuti

Prima di creare un documento, è opportuno riflettere sulla sua struttura e contenuto. Per fare questo è opportuno trattare il documento come un libro: esso avrà un titolo e più capitoli, all'interno di ogni capitolo più paragrafi. Se il documento è articolato e complesso è opportuno creare un sommario in base alla struttura che si sceglie di dare. Sarà buona norma utilizzare un

linguaggio semplice e frasi brevi, per agevolare la comprensibilità e la lettura, così come evitare l'uso di tabelle e grafici complessi.

In ultimo, si consiglia, in fase di salvataggio dei documenti, di **utilizzare denominazioni sintetiche e semanticamente significative in relazione ai contenuti**.

Proprietà del documento

A fini documentali e per facilitare successive revisioni del documento, occorre inserire le seguenti proprietà. Alcune, oltre a rappresentare metadati obbligatori, risulteranno utili in futuro anche per l'inserimento del documento nel sistema di gestione documentale ai sensi delle Regole tecniche sul documento informatico[1]:

a) l'identificativo univoco (il titolo "significativo" del documento);

b) il riferimento temporale (la data);

c) l'oggetto;

d) il soggetto che ha formato il documento (l'autore del documento);

e) l'eventuale destinatario (Destinazione);

f) lingua.

L'amministratore di sistema verificherà nell'impostazione del pc di tutto il personale la presenza di tutte le proprietà suddette (lettere a-f) ed eventualmente provvedere ad aggiungerle.

Per visualizzare, modificare o inserire le proprietà del documento occorre seguire i seguenti passi:

1. fare clic sulla scheda "File";
2. fare clic su "Informazioni" per visualizzare e inserire le proprietà del documento: in alto a destra, cliccando sul menù a tendina "Proprietà", si potrà accedere a "Mostra riquadro documenti", che consente di inserire Autore, Titolo, Oggetto, Parole chiave, ecc.;
3. tornare indietro su "File" e fare clic su "verifica documento";
4. fare clic su "controlla documento";
5. fare clic su "controlla" e verificare le informazioni risultanti;
6. fare di nuovo clic su "File" per tornare al documento. Nella versione Word 2016 le suddette operazioni appaiono più immediate.

[1] http://www.gazzettaufficiale.it/eli/id/2015/01/12/15A00107/sg
http://www.agid.gov.it/sites/default/files/leggi_decreti_direttive/dpcm_13_11_2014_regole_tecniche_documento_informatico.pdf

Per quanto concerne la proprietà "**Autore**" del documento è da rilevare che per i documenti posti alla firma di altri, l'autore del documento va sempre indicato con il nominativo del soggetto firmatario, mentre l'estensore del documento (chi lo scrive e lo sottopone alla firma) va indicato per esteso (Cognome e Nome) nel campo "**Redattore**".

Stili e formattazione

Usare sul documento gli stili e le funzionalità di lista per formattare i contenuti in capitoli, paragrafi e punti elenco, al fine di dare una struttura. In questo modo sarà più facile convertire successivamente il documento di origine in formato PDF accessibile.

In particolare, i seguenti comandi sono visibili e sono selezionabili nella barra multifunzione della scheda "Home":

1. utilizzare i titoli: utilizzare gli stili (di intestazione) per creare una struttura logica del documento. Per esempio, non occorre aumentare le dimensioni del testo per creare l'aspetto di intestazioni o dare loro risalto, ma inserire uno stile adeguato allo scopo dell'elemento (per esempio "Titolo1", "Titolo2", "Titolo3", ecc.).
2. utilizzare le liste: utilizzare gli stili (di elenco) per le liste. Se gli elementi seguono una sequenza specifica, utilizzare un elenco numerato. Non utilizzare segni di punteggiatura o altri marcatori per creare l'impressione di una lista. È possibile selezionare la tipologia di elenchi (elenchi puntati, elenchi numerati, a più livelli).

Entrambe le indicazioni sono fondamentali. Se il documento è sottoposto ad un sistema di lettura, infatti, ad esempio per un soggetto non vedente, il dispositivo riconosce titoli ed elenchi formati attraverso i comandi mentre non riconosce come tali quelli creati con modalità che si limitano a emulare la struttura. Inoltre, se non si utilizzano intestazioni ed elenchi immediatamente riconoscibili, è necessario rispettare il principio delle "alternative testuali".

Si suggerisce, inoltre, di non creare allineamenti mediante la barra spaziatrice, ma utilizzando la tabulazione. Evitare, quando possibile, l'utilizzo di paragrafi vuoti, ad esempio per aumentare la distanza tra due paragrafi, utilizzando invece la spaziatura del paragrafo.

Evitare il testo giustificato in quanto potrebbe pregiudicare la lettura a schermo e l'immediato riconoscimento della posizione dei capoversi.

Posizionare, infine, gli oggetti nel documento (foto, forme, grafici, ecc.) con una disposizione "in linea" con il testo, in modo da facilitare la lettura tramite un lettore di schermo.

Inserire didascalie o alternative testuali per immagini, forme ecc.

Per le tabelle, nel caso in cui si cambi pagina, va inserita nuovamente l'intestazione.

Sommario automatico

Avendo inserito correttamente i titoli e i paragrafi, il sommario rispecchierà l'ordine dei titoli inseriti e consentirà inoltre di spostarsi automaticamente, cliccando tra le varie parti del testo. Per ottenere il sommario occorre cliccare nella scheda multifunzione su "Riferimenti", poi su "Sommario" e sul tipo di sommario preferito.

Collegamenti ipertestuali

1. Per inserire un collegamento ipertestuale selezionare il testo interessato, cliccare sul tasto destro del mouse e scegliere "Collegamento Ipertestuale". Per i collegamenti ipertestuali utilizzare testi significativi. All'interno della schermata è possibile inserire il collegamento ipertestuale ed inserire l'indirizzo (in basso). Inoltre, cliccando sulla voce "Descrizione", posizionata sulla destra, è possibile inserire la descrizione al collegamento ipertestuale, quando necessario (per esempio inserendo informazioni sulla destinazione di collegamenti ipertestuali esterni: "Vai al sito web del Comune di …"); è opportuno non inserire testi poco significativi ai link, come per esempio "clicca qui"; infine premendo il tasto OK il testo selezionato risulterà automaticamente sottolineato;
2. **non sottolineare parti del testo, in quanto ciò potrebbe generare confusione circa la presenza di collegamenti ipertestuali**.

Colori

Se il colore è l'unica caratteristica visiva che distingue un elemento grafico dall'altro, fare in modo che nella visualizzazione in scala di grigi il contrasto tra i vari elementi sia adeguato. In alternativa meglio utilizzare altri accorgimenti (per esempio puntinato o tratteggiato per la grafica)

1. Utilizzare un buon contrasto di colore: il contrasto tra il colore del testo e lo sfondo deve essere almeno pari al rapporto 4,5:1 (rapporto indicato dalle Linee guida per l'accessibilità dei contenuti web, WCAG 2.0). Per effettuare la verifica è possibile scaricare e utilizzare uno strumento sul contrasto colore, come ad esempio Contrast checker. Si consiglia di evitare di inserire il testo utilizzando colori con poco contrasto rispetto allo sfondo (per esempio, evitare il testo giallo/arancione su sfondo bianco);
2. non utilizzare il colore o la forma come unico modo per identificare qualcosa nel documento ed utilizzare descrizioni quando necessario.

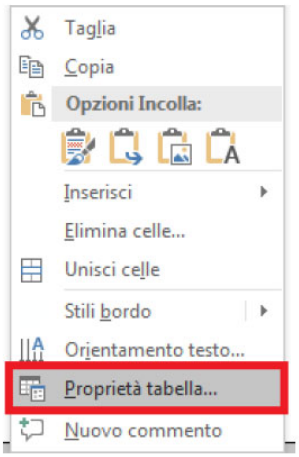
Tabelle e loro struttura

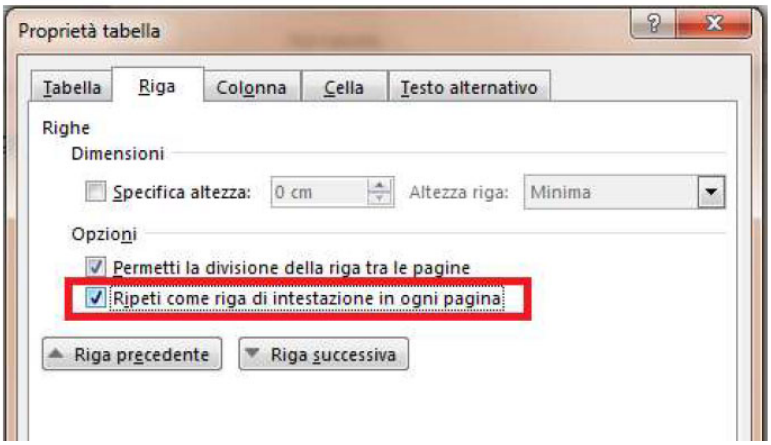
Se nel documento è necessario inserire tabelle di riepilogo, devono essere utilizzati i seguenti accorgimenti:

1. scegliere una struttura semplice della tabella e non una struttura a doppia entrata o a tabelle annidate, per facilitare la lettura da parte delle tecnologie assistive, in particolare

dei lettori di schermo. Se necessario, e se possibile, suddividere le tabelle a doppia entrata in più tabelle semplici, una dopo l'altra;

2. inserire le intestazioni di colonna alla tabella selezionando la riga: cliccare poi con il tasto destro sulla riga selezionata e scegliere la voce "Proprietà Tabella". All'interno della finestra "Proprietà Tabella" selezionare la scheda "Riga" e cliccare sulla casella di controllo "Ripeti come riga di intestazione in ogni pagina" (ciò è particolarmente utile se una tabella va su più pagine);





3. inserire un testo alternativo e una descrizione della tabella, facendo clic nella tabella: cliccare con il tasto destro sulla tabella e scegliere la voce "Proprietà Tabella". All'interno della finestra "Proprietà Tabella", selezionare la scheda "Testo Alternativo" e inserire il titolo e una descrizione della tabella;
4. evitare celle vuote (eventualmente inserire la dicitura "dato non disponibile").

Immagini

1. Aggiungere testi alternativi alle immagini. Per inserire un testo alternativo all'immagine e una descrizione cliccare con il tasto destro sull'immagine interessata e poi cliccare su "Formato

immagine". All'interno della finestra "Formato immagine" (che si apre in alto a destra) selezionare "Testo alternativo" ed inserire titolo e descrizione. La descrizione, intercettabile dal lettore di schermo, sarà visualizzata come testo alternativo dell'immagine dopo la trasformazione in PDF, posizionandovi sopra il cursore;

2. Inserire, anche per quanto riguarda eventuali grafici presenti nel documento, un testo alternativo e una descrizione.

In entrambi i casi è opportuno inserire didascalia e fonte con descrizione di contenuto di immagini e grafici. In Word 2016 il testo alternativo si raggiunge cliccando sulla terza icona quadrata con delle frecce.

Caratteri

Usare "font" di caratteri "senza grazie" (cioè che non hanno i tratti terminali chiamati appunto "grazie") come per esempio "Arial" o "Verdana". I "font" "senza grazie" sono più facilmente leggibili sullo schermo di un computer. Si consiglia di utilizzare una dimensione minima 12 ed una interlinea compresa tra 1,2 e 1,5.

Audio/Video

Per rendere accessibile una registrazione audio è necessario fornire una trascrizione di tutte le parole pronunciate nella registrazione. Un video, per essere considerato accessibile a tutte le categorie di utenti, deve essere accompagnato da alternative testuali equivalenti. Sottotitoli o trascrizioni testuali sono utili sia alle persone con disabilità uditive sia agli utenti che non dispongono del *player* adatto alla riproduzione.

Si consiglia di caricare i propri video su una piattaforma *online* che permette di visualizzare i sottotitoli, come YouTube, servizio che inoltre ha il vantaggio di creare automaticamente i sottotitoli per ogni video caricato. L'accuratezza finale dei testi potrebbe non essere alta, ma questi possono essere corretti e migliorati direttamente online (si veda la guida su come aggiungere sottotitoli su YouTube). In alternativa è anche possibile caricare un proprio file di sottotitoli.

Anche in PowerPoint occorre prestare attenzione alle informazioni veicolate attraverso suoni, colori e link.

In particolare:

- limitare l'utilizzo di animazioni e transizioni: oltre a creare difficoltà agli utenti con disabilità visiva, possono anche creare problemi in fase di esportazione in PDF
- utilizzare sempre un Layout (scelto tra quelli disponibili) in modo da strutturare correttamente il contenuto
- evitare l'utilizzo di tabelle per la formattazione del testo

- se si inseriscono collegamenti esterni, inserire tra parentesi l'URL in formato esteso (per la versione a stampa)
- inserire sempre il testo alternativo per tutte le immagini, anche per quelle utilizzate come Pulsanti di azione
- se si inseriscono elementi audio/video, assicurarsi che tale contenuto sia disponibile in formati alternativi (trascrizione/sottotitoli)

Come controllo finale, utilizzare lo strumento di Verifica Accessibilità fornito direttamente da Office.

Una volta creato il documento in questo modo, salvarlo direttamente da PowerPoint come PDF in modo da preservarne l'accessibilità

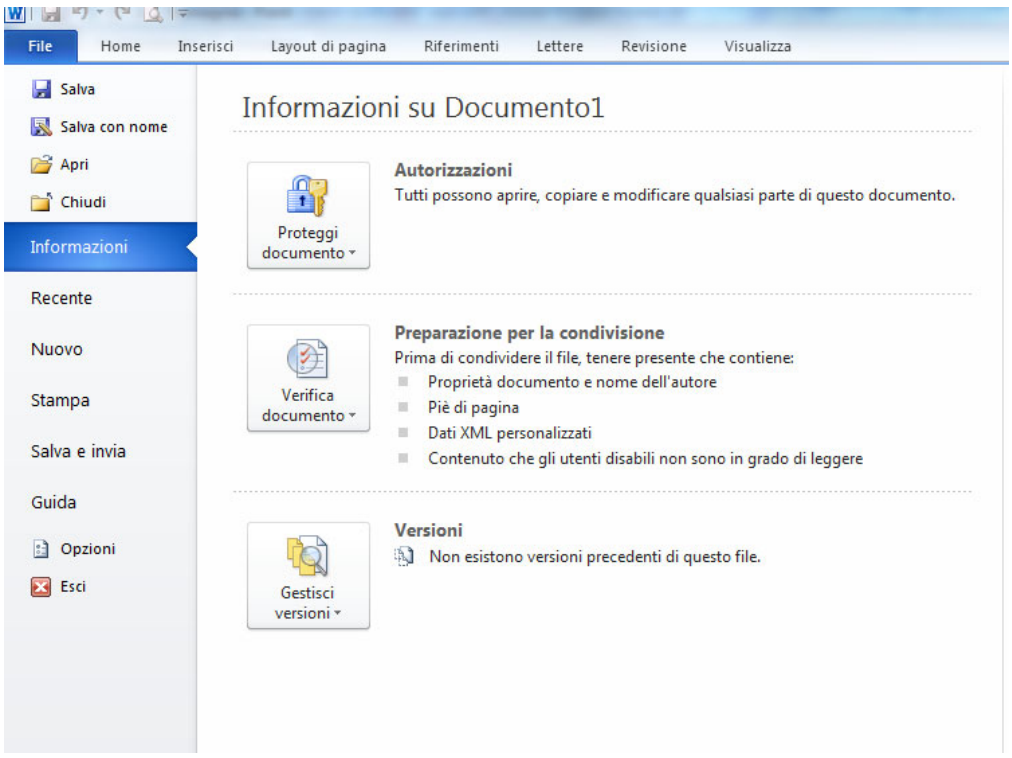
Verifica di accessibilità del documento originario

Dalla versione word 2010 in poi è possibile utilizzare la funzionalità di word per la verifica di accessibilità del documento.

Pertanto, dopo aver redatto il documento originario, si suggerisce di effettuare una verifica di accessibilità utilizzando gli strumenti dell'editor di testo.

Per effettuare la verifica è necessario che il file sia salvato in **formato ".docx"**.

Per effettuare la verifica cliccare sulla scheda "File", poi su "Verifica documento" e su "Verifica Accessibilità", comparirà sulla destra il box con il risultato della verifica di accessibilità.

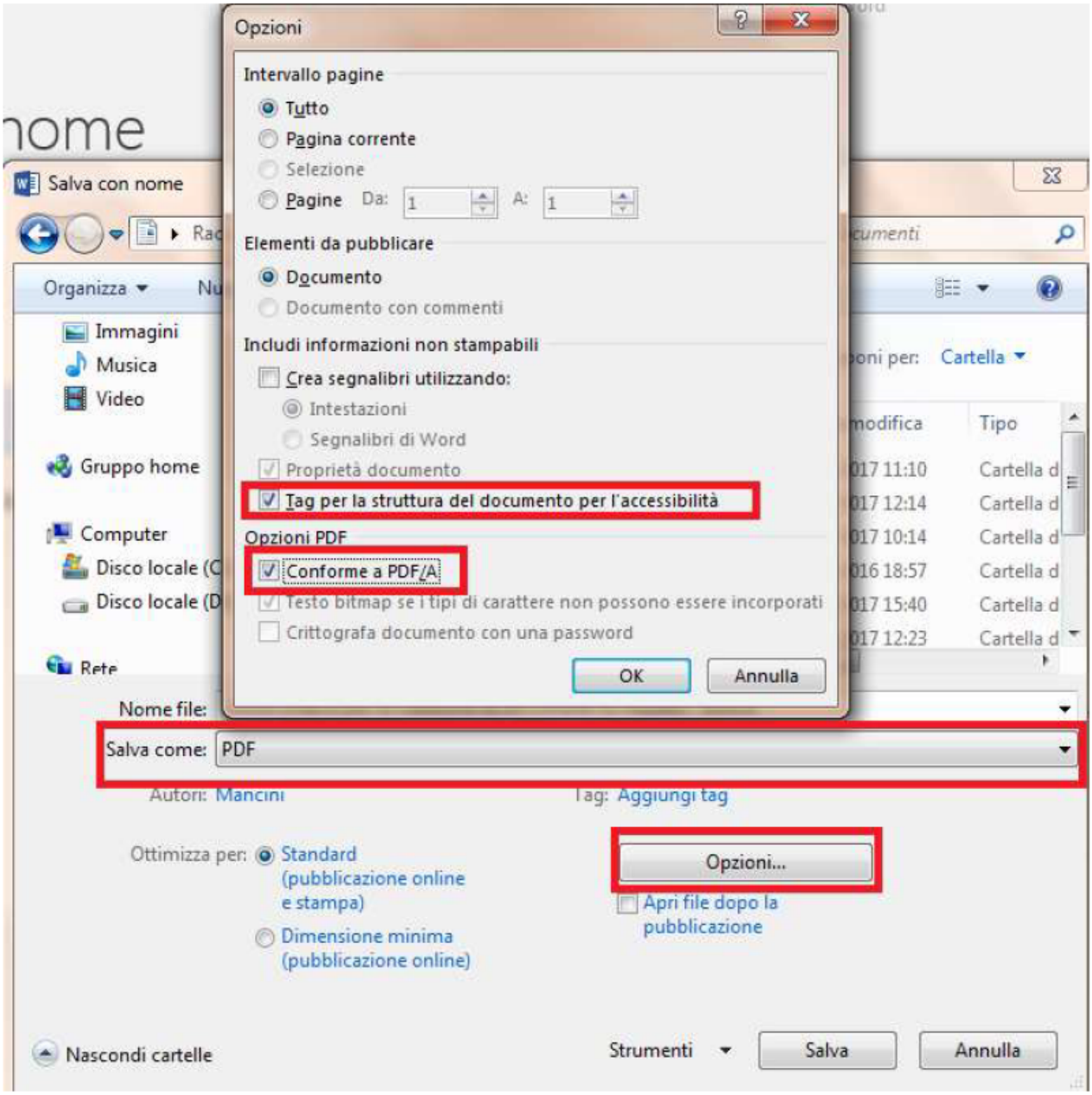


Rimuovere le eventuali anomalie segnalate. Per Word 2016 si effettua la verifica andando nella sezione “Revisione” e attivando “Verifica di accessibilità”. Altre informazioni sono disponibili sulla pagina verifica di accessibilità per Word.

Conversione del documento originario in PDF

Per effettuare la conversione **da Word 2010 in PDF**, si eseguono i seguenti passi:

1. cliccare su “File”;
2. cliccare sulla voce “Salva con nome”;
3. selezionare il formato “PDF” nel menu a tendina;
4. cliccare sul bottone “Opzioni”;
5. selezionare “Crea segnalibri, utilizzando: intestazioni” e “Tag per la struttura del documento per l’accessibilità”;
6. selezionare “Conforme a PDF/A
7. cliccare sul pulsante “OK”;
8. cliccare su “Salva”.



In Word 2016 dopo il punto 2, si procede cliccando su “Altre opzioni”, si sceglie di salvare in PDF e successivamente su “Opzioni”, che apre una finestra in cui si ha la possibilità di richiedere la conformità a PDF/A; infine, riprendere dal punto 7 per salvare. Si fa presente che il PDF/A è il formato da preferire per la conservazione a lungo termine del documento, caratterizzato dall’assenza di collegamenti esterni, codici eseguibili, contenuti crittografati. Utilizzando Word 2016 su MAC, dopo “Salva con nome” occorre scegliere se il salvataggio in PDF è effettuato per la distribuzione elettronica in modalità online accessibile o per la stampa.

Per altre versioni di office o altri sistemi operativi consultare la guida ufficiale Microsoft Office[2].

Verifica di accessibilità del PDF

La conversione da un documento di testo "accessibile" a PDF da sola non sempre garantisce che il documento PDF risultante sia accessibile. Dopo avere effettuato la conversione del documento originario in PDF è possibile effettuare un controllo sull'accessibilità di quest'ultimo, utilizzando **una delle ultime versioni di Adobe Acrobat Professional**, al fine di verificare, in particolare, che la conversione abbia mantenuto i "tag", l'ordine di esposizione, i testi alternativi alle immagini, i "tag" semantici delle tabelle, ecc.

Se possibile, si consiglia anche di effettuare una lettura del documento PDF con un lettore di schermo, come ad esempio Jaws, VoiceOver, NVDA, per verificare se sussistono delle inesattezze o se appaiono parole poco comprensibili alla lettura vocale: sommario, titoli, acronimi, numeri, collegamenti ipertestuali, ordine delle parole nel testo, articoli, preposizioni, parole in lingua straniera, punteggiatura, ecc..

In relazione alle diverse indicazioni da seguire per i vari documenti, utilizzabili come documenti originari accessibili, citati in premessa, si vedano, a titolo di esempio, le indicazioni per Word, Pages, Open Office e Adobe.

[2] https://support.office.com/it-it/article/Creare-file-PDF-accessibili-064625e0-56ea-4e16-ad71-3aa33bb4b7ed

Allegato 4

TITOLARIO

Titolario

I Liv.	Classe	Sottoclasse			Descr. Titolazione
I					Direzione
I	1				Direzione
II					Servizi Generali
II	1				Servizi Generali
II	2				Amministrazione
II	3				Risorse Umane
II	4				Acquisti, Gare e Contratti, Magazzino
II	5				Sistema Qualità, Relazioni Esterne, Formazione
III					Sistemi e Servizi tecnologici, Sicurezza Informatica
III	1				Sistemi e Servizi tecnologici, Sicurezza Informatica
III	2				Sistemi e Servizi Telecomunicazioni
III	3				Sistemi e Servizi IT
III	4				Informatica Distribuita, Contact Center
III	5				Banda Larga, altri progetti
IV					Sistemi e Servizi Applicativi
IV	1				Sistemi e Servizi Applicativi
IV	2				Personale
IV	3				Tributi
IV	4				Casa
IV	5				Anagrafe, Servizi Elettorali
IV	6				Polizia Municipale
IV	7				Comunicazione Globale
IV	8				Casinò
IV	9				Contabilità
IV	10				Dematerializzazione
IV	11				Laboratorio di Sviluppo

I Liv.	Classe	Sottoclasse			Descr. Titolazione
IV	12				Enti Territoriali
V					Progetto Pon Metro
V	1				Pon Metro
VI					Progetto React EU
VI	1				PON METRO 2014-2020 REACT-EU: PIANO OPERATIVO CITTÀ DI VENEZIA

Allegato 5

Modello di registro di emergenza

VENIS S.p.A.
MODELLO DI REGISTRO DI PROTOCOLLO DI EMERGENZA

A. Schema di provvedimento di autorizzazione allo svolgimento delle operazioni di registrazione di protocollo sul registro di emergenza.

N°	data	Tipo (in uscita, in entrata, interno)	Mittente/ destinatario	Oggetto	Classificazione	N. allegati	Mezzo di trasmissione	note
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								

B. Schema di provvedimento di autorizzazione allo svolgimento delle operazioni di registrazione di protocollo sul registro di emergenza.

Ai sensi dell'art. 63 del DPR 28 dicembre 2000 n. 445, preso atto che, per le cause sotto riportate:

- Data interruzione: *[campo da compilare]*
- Ora interruzione: *[campo da compilare]*
- Causa della interruzione: *[campo da compilare]*

non è possibile utilizzare la normale procedura informatica, si autorizza lo svolgimento delle operazioni di registrazione di protocollo sul Registro di emergenza.

Il Responsabile della gestione documentale

[firma autografa del responsabile]

C. Schema di provvedimento di revoca allo svolgimento delle operazioni di registrazione di protocollo sul registro di emergenza.

Ai sensi dell'art. 63 del DPR 28 dicembre 2000 n. 445,

considerato che, per le cause sotto riportate:

- Data interruzione: *[campo da compilare]*

- Ora interruzione: *[campo da compilare]*
- Causa della interruzione: *[campo da compilare]*

non è stato possibile utilizzare la normale procedura informatica e, dunque, è stato autorizzato lo svolgimento delle operazioni di registrazione di protocollo sul Registro di emergenza;

preso atto che dalla data sotto riportata:

- Data ripristino: *[campo da compilare]*
- Ora ripristino: *[campo da compilare]*

è stato ripristinato il normale funzionamento della procedura informatica, si revoca l'autorizzazione allo svolgimento delle operazioni di registrazione di protocollo sul Registro di emergenza e si dispone il tempestivo inserimento delle informazioni relative ai documenti protocollati in emergenza nel sistema informatico, con automatica attribuzione della numerazione di protocollo ordinaria, mantenendo la correlazione con la numerazione utilizzata in emergenza.

Il Responsabile della gestione documentale

[firma autografa del responsabile]

Allegato 6

Piano di sicurezza informatica

Politiche specifiche per la sicurezza delle informazioni

Compilato:	A.Trofin (Responsabile Sistemi IT, Sicurezza Inf.)	15/05/2025
Rivisto:	G. Nunziale (Responsabile Assistenza Utenti, Certificazioni)	15/05/2025
Autorizzato:	M. Bettini (Condirettore Generale e Direttore Operation)	16/05/2025

Versione: 2
Variante: 0

Classificazione: Documento pubblico

Compendio:	Indicazioni operative
Riferimenti:	ISO/IEC 27001 - ed. 2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements ISO/IEC 27017 - ed. 2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services ISO/IEC 27018 - ed. 2019 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors ISO/IEC 20000-1 ed. 2018 Information technology — Service management Service management system requirements
Altri documenti correlati:	• *Manuale del sistema di gestione per la sicurezza delle informazioni "Manuale SSIV" (VSI-AS-MS-01)* • *Politiche per la Sicurezza delle Informazioni (VSI-SI-PSI-01)* • *Politica di sicurezza per i servizi Cloud (VSI-SI.PSI-02)*
Moduli associati:	
Principali modifiche rispetto alla versione precedente:	Adeguamento all'edizione 2022 della norma 27001

INDICE

1.Titolo....7
1.1. Premessa al documento....7
1.2. Scopo del documento....7
1.3. Campo di applicazione del documento....8
1.4. Abbreviazioni....8
1.5. Gestione del documento....8
2.Principi generali....9
2.1. Principi e obiettivi per la sicurezza delle informazioni....10
3.Organizzazione per la Sicurezza delle Informazioni....12
3.1. Ruoli e Responsabilità per la Sicurezza delle Informazioni....12
3.2. Separazione dei compiti....13
3.3. Contatti con le Autorità e con Gruppi Specialistici....14
3.4. Sicurezza delle informazioni nella gestione dei progetti....15
3.5. Dispositivi portatili....15
4.Sicurezza delle risorse umane....17
4.1. Aspetti di sicurezza nelle fasi di selezione e inserimento....17
4.2. Termini e condizione di impiego....18
4.3. Modifica e cessazione....20
5.Gestione degli Asset....22
5.1. Tracciamento degli asset ICT....22
5.2. Catalogo degli asset....23
5.3. Classificazione degli asset....23
5.4. Trasporto dei supporti fisici....24
5.5. Dismissione e distruzione degli asset ict....24
6.Classificazione delle informazioni....25
6.1. Premessa....25
6.2. Ownership dell'informazione....26
6.3. Classificazione ed etichettatura....26
6.4. Ciclo di vita dell'informazione....30
6.5. Misure di sicurezza....31
6.6. Supporti digitali – sistemi informatici....34
6.7. Supporti digitali – dotazioni informatiche aziendali....36
7.Controllo accessi....40
7.1. Requisiti generali per il controllo degli accessi....40
7.2. Gestione degli accessi utenti....42
7.2.1. Attribuzione delle credenziali e dei relativi permessi....42

7.2.2. Riesame dei diritti di accesso 43
7.2.3. Off boarding o Modifica di mansione 43
7.3. Responsabilità degli utenti 43
7.4. Controllo degli accessi a livello di rete 43
7.5. Controllo degli accessi sistemistici 44
7.6. Password 45

8.Crittografia 47

8.1. Premessa 47
8.2. Modello di crittografia 48
8.3. Politica per la crittografia 49
8.3.1. Obbligatorietà crittografica 49
8.3.2. Gestione chiavi crittografiche 49
8.3.3. Protezione chiavi crittografiche 49
8.3.4. Gestione del ciclo di vita delle chiavi 50
8.3.5. Certification Authority 50
8.3.6. Protezione fisica 50
8.4. Misure di trasmissione 50
8.5. Misure di memorizzazione 51

9.Sicurezza fisica ambientale 52

9.1. Gestione della sicurezza delle sedi, delle aree e dei locali 52
9.1.1. Criteri di gestione degli accesi al CED 54
9.1.2. Procedura di gestione degli accessi al CED 55
9.1.3. Ingresso visitatori sprovvistidi badge abilitato 55
9.2. Gestione della sicurezza degli asset e delle apparecchiature 56
9.3. Sensori 58
9.4. Ventilazione e condizionamento 59
9.5. Energia Elettrica 60
9.6. Rilevazione e soppressione incendi 61
9.7. Smaltimento e riutilizzo delle apparecchiature 61
9.8. Controlli di sicurezza sulle apparecchiature in ingresso e in uscita 62
9.9. Clear desk policy 63
9.10. Clear screen policy 63

10.Sicurezza delle attività operative 66

10.1. Procedure operative e responsabilità correlate 66
10.2. Gestione dei cambiamenti 66
10.3. Gestione della Capacità 66
10.4. Separazione degli ambienti di sviluppo, test e produzione 67
10.5. Protezione dai malware 68
10.6. Backup 68
10.7. Monitoring e log management 70
10.8. Controllo dei software operativi 71

10.9. Gestione delle vulnerabilità tecniche 72
10.10. Considerazioni sugli audit ai sistemi informativi 72

11. Sicurezza delle comunicazioni 73

11.1. Obiettivi di Sicurezza delle Reti 73
11.2. Segregazione delle Reti 74
11.3. Trasferimento delle Informazioni 74

12. Acquisizione, sviluppo e manutenzione dei sistemi informativi 77

12.1. Premessa 77
12.2. Requisiti di Sicurezza per i Sistemi Informatici e Sicurezza nelle Applicazioni 77
12.2.1. Analisi e specifica dei requisiti per la sicurezza delle informazioni 77
12.2.2. Sicurezza dei Servizi Applicativi su Reti Pubbliche 79
12.2.3. Protezione delle transazioni dei servizi applicativi 80
12.3. Sicurezza nei processi di sviluppo e supporto 81
12.3.1. Politica per lo sviluppo sicuro 81
12.3.2. Procedure per il controllo dei cambiamenti di sistema 81
12.3.3. Riesame tecnico delle applicazioni in seguito a cambiamenti nelle piattaforme operative 83
12.3.4. Limitazioni ai cambiamenti dei pacchetti software 83
12.3.5. Principi per l'ingegnerizzazione sicura dei sistemi 83
12.3.6. Ambiente di sviluppo sicuro 84
12.3.7. Sviluppo affidato all'esterno 86
12.3.8. Test di sicurezza dei sistemi 87
12.3.9. Test di accettazione dei sistemi 87
12.4. Dati di test 88
12.4.1. Protezione dei dati di test 88

13. Relazione con i fornitori 89

14. Gestione degli incidenti di sicurezza delle informazioni 91

14.1. Premessa 91
14.2. Gestione degli incidenti relativi alla sicurezza delle informazioni e dei miglioramenti 91
14.2.1. Responsabilità e procedure 91

15. Aspetti relativi alla sicurezza delle informazioni nella gestione della continuità operativa 93

15.1. Premessa 93
15.2. Continuità della sicurezza delle informazioni 93
15.2.1. Attuazione della continuità della sicurezza delle informazioni 94
15.3. Ridondanze 95
15.4. Verifica, riesame e valutazione della continuità della sicurezza delle Informazioni 95

16. Conformità 96

16.1. Premessa 96
16.2. Conformità ai requisiti cogenti e contrattuali 96
16.2.1. Identificazione della legislazione applicabile e dei requisiti contrattuali 96

16.2.2. Diritti di proprietà intellettuale 96
16.2.3. Protezione delle registrazioni 98
16.2.4. Privacy e protezione dei dati personali 99
16.2.5. Regolamentazione sui controlli crittografici 100
16.3. Riesami della sicurezza delle informazioni 100
16.3.1. Riesame indipendente della sicurezza delle informazioni 100
16.3.2. Conformità alle politiche e alle norme per la sicurezza 101
16.3.3. Verifica tecnica della conformità 102

1. Titolo

Per VENIS l'informazione rappresenta un patrimonio la cui attenta gestione è strategica per la tutela e lo sviluppo del business aziendale. Al tal riguardo, VENIS si è dotata di una policy di Sicurezza delle Informazioni (Rif. VSI-SSI-PSI-01-2025), enunciante i principi che si prefigge di osservare e far rispettare. In accordo a tale politica e in considerazione delle disposizioni normative vigenti applicabili, VENIS ha pertanto definito regole di sicurezza delle informazioni con l'obiettivo di fornire indicazioni in merito ai requisiti minimi di sicurezza ed alle necessarie misure di attuazione.

1.1. Premessa al documento

Il Sistema di Gestione per la Sicurezza delle Infomazioni di VENIS (SSIV), in conformità a quanto indicato dagli standard internazionali di riferimento si struttura secondo un approccio Risk Based che prevede l'individuazione, la valutazione e la gestione dei possibili rischi che possano compromettere la sicurezza delle informazioni trattate nell'ambito della gestione dei servizi e delle soluzioni ICT infrastrutturali.

Nella realizzazione del presente documento si è fatto riferimento alle norme:

- ISO/IEC 27000:2018
- ISO/IEC 27001:2022
- ISO/IEC 27002:2022
- ISO/IEC 27017:2015
- ISO/IEC 27018:2019

1.2. Scopo del documento

L'obiettivo del presente documento è quello di illustrare i principi, gli obiettivi e gli standard che VENIS adotta al fine di proteggere opportunamente le informazioni trattate, mediante l'istituzione, l'attuazione, il monitoraggio, il riesame ed il miglioramento progressivo del SSIV. Più in dettaglio il documento definisce:

- i principi e gli obiettivi che VENIS si impegna a rispettare e a perseguire, al fine di proteggere opportunamente le informazioni trattate dai Servizi ICT erogati in perimetro SSIV;
- gli standard adottati in conformità a quanto indicato dalle norme internazionali ISO/IEC 27000:2018, ISO/IEC 27001:2022, ISO/IEC 27002:2022, ISO/IEC 27005:2018, ISO/IEC 27017:2015, ISO/IEC 27018:2019.

1.3. Campo di applicazione del documento

Il presente documento è applicabile al personale dipendente interno di VENIS e in particolare a quelle funzioni aziendali dove vengono trattati dati e informazioni che possono ritenersi critiche sulla base dei criteri di seguito definiti, nonché al personale esterno di terze parti (quali ad esempio fornitori, outsourcer, clienti, consulenti, etc.).

La norma va applicata in maniera integrale in tutte le unità dell'Azienda per evitare una disomogeneità di protezione che si traduce in un elevato rischio di fuoriuscita o di modifica non autorizzata di informazioni.

1.4. Abbreviazioni

SSIV	Sistema di Gestione per la Sicurezza delle Informazioni di VENIS SQV
DG	Direzione Generale
RSI	Responsabile della Sicurezza delle Informazioni
RSG	Referente per i Sistemi di Gestione
SASI	Servizio Assicurazione Sicurezza delle Informazioni

1.5. Gestione del documento

E' responsabilità del RSI provvedere alla gestione, alla revisione perlomeno annuale e all'eventuale aggiornamento del presente documento.

2. Principi generali

VENIS identifica e persegue i tre requisiti fondamentali della sicurezza delle informazioni, ovvero:

- ***la riservatezza,*** orientata ad assicurare che l'informazione sia disponibile solo agli utenti autorizzati;
- ***l'integrità***, volta a salvaguardare la completezza, l'accuratezza e la conformità dell'informazione durante l'acquisizione, la conservazione, l'elaborazione e la presentazione;
- ***la disponibilità***, finalizzata ad assicurare che gli utenti autorizzati abbiano accesso alle informazioni ed agli elementi architetturali associati, quando se ne evidenzi l'effettivo bisogno attraverso opportune richieste.

La mancanza di adeguati livelli di sicurezza connessi a tali requisiti può esporre i dati e le informazioni, trattate nell'ambito dei Servizi/Soluzioni ICT infrastrutturali in ambito, a rischi di sicurezza che possano avere impatti negativi sull'attività aziendale, quali ad esempio: danni di immagine aziendale, mancata soddisfazione da parte del cliente, sanzioni legate alla violazione delle normative vigenti e danni di natura economica e finanziaria.

Per garantire il corretto livello di sicurezza per il patrimonio informativo gestito mediante i Servizi/Soluzioni informatiche erogate ai clienti, nell'ambito del perimetro definito dal "Manuale del Sistema di Gestione per la Sicurezza delle Informazioni di VENIS – SSIV *(VSI-CER-MS-02_Manuale SSIV)*", VENIS predispone e gestisce le adeguate misure di protezione.

In particolare, per quanto riguarda gli aspetti di sicurezza, tale obiettivo può essere perseguito solo attraverso la definizione, l'attuazione, il monitoraggio, il riesame ed il miglioramento continuo di un Sistema di Gestione per la Sicurezza delle Informazioni.

Tale sistema rappresenta un approccio strutturato sulla base del ciclo di Deming (Plan, Do, Check, Act), che partendo dagli obiettivi identificati nell'ambito della Sicurezza delle informazioni da VENIS, tenendo in considerazione ulteriori elementi di input (appetito al rischio aziendale, caratteristiche delle operations aziendali, ecc.),

adotta le suddette misure di protezione, ne verifica periodicamente la validità e la congruenza e identifica eventuali aree di miglioramento.

2.1. Principi e obiettivi per la sicurezza delle informazioni

VENIS afferma i seguenti obiettivi e principi a cui è ispirato il SSIV adottato:

- VENIS riconosce nel patrimonio informativo, gestito nell'ambito dei Servizi/Soluzioni ICT infrastrutturali erogati, un asset fondamentale al fine del corretto perseguimento degli obiettivi di business aziendali e pertanto si impegna ad adottare gli elementi di sicurezza necessari a garantirne un opportuno livello di protezione;
- coerentemente a tale impegno, VENIS ritiene che, per alcuni ambiti specifici, la corretta protezione di tale patrimonio debba basarsi sull'adozione di un Sistema di Gestione per la Sicurezza delle Informazioni, che possa garantire un approccio strutturato, completo e continuativo alle tematiche di sicurezza e che costituisca lo strumento che, partendo dagli obiettivi aziendali di sicurezza e dalle risorse che è necessario proteggere, permetta di individuare e valutare i rischi di sicurezza e di contrapporre loro gli opportuni presidi;
- la corretta definizione di tale Sistema di Gestione per la Sicurezza delle Informazioni è strutturata secondo un approccio Risk Based, descritto nella documentazione correlata alla **metodologia di risk management**;
- VENIS riconosce che l'istituzione, l'attuazione, il monitoraggio, il riesame, il mantenimento e il miglioramento riguarda tutti i soggetti interni ed esterni che accedono alle informazioni che vanno protette, ognuno secondo quanto di sua competenza. Al fine di definire opportuni presidi di sicurezza, VENIS ha comunque assegnato alcune delle responsabilità correlate a specifiche funzioni e soggetti aziendali nell'ambito del perimetro del proprio SSIV;
- VENIS si impegna, nei suoi soggetti apicali competenti, a fornire le necessarie risorse affinché il SSIV adottato possa correttamente ed efficacemente garantire la protezione delle informazioni appartenenti all'ambito definito.

I principi qui introdotti sono definiti dal Comitato di Sicurezza del SSIV che assicura di procedere periodicamente alla loro revisione ed al loro aggiornamento, in modo da garantire che essi riflettano eventuali evoluzioni del contesto aziendale di riferimento in materia di sicurezza dell'informazione.Si evidenzia, infine, che essi sono ulteriormente declinati negli obiettivi di sicurezza, che derivano da obblighi cogenti, da normative o da decisioni autonome dell'azienda legate anche ad esigenze di mercato e di opportunità commerciale. VENIS ha quindi identificato gli obiettivi, di alto livello, per la sicurezza delle informazioni a supporto e tutela della propria missione, affinché questa sia efficacemente espletata:

- **garantire la continuità delle Soluzioni ICT infrastrutturali e servizi Cloud erogati** per salvaguardare il patrimonio aziendale (informativo, sociale, finanziario e d'immagine) e quello degli enti a cui eroga tali Servizi;
- **salvaguardare la disponibilità, la riservatezza e l'integrità delle informazioni trattate** nell'ambito dei Servizi/Soluzioni ICT infrastrutturali erogate anche secondo i più recenti modelli di servizio Cloud (modalità IaaS, SaaS e PaaS) al fine di proteggere le informazioni dei propri clienti, degli utenti e di conseguenza il proprio patrimonio aziendale nei suoi aspetti finanziari, fisici, di proprietà intellettuale e di reputazione;
- **limitare gli incidenti di sicurezza ICT** che possono avere impatto sulla sicurezza delle informazioni gestite mediante i Servizi/Soluzioni ICT infrastrutturali , identificandoli tempestivamente, gestendoli in modo da limitare il più possibile gli impatti alla comunità e provvedendo ad analizzare tali eventi al fine di ridurne la probabilità di accadimento futuro;
- **ottemperare a tutte le leggi e disposizioni regolamentari che disciplinano l'attività di VENIS**, con particolare riguardo alla propria qualificazione come CSP accreditato da AGID per l'erogazione di Servizi ICT anche in Cloud verso la Pubblica Amministrazione.

A seguito dell'identificazione degli obiettivi per la sicurezza sono identificati gli standard e le politiche per la sicurezza delle informazioni.

3. Organizzazione per la Sicurezza delle Informazioni

L'obiettivo del SSIV, relativamente a tale area, è quello di garantire che tutte le responsabilità, relative alla sicurezza delle informazioni, dei soggetti che prendono parte al SSIV siano opportunamente indirizzate, ivi inclusi i soggetti esterni che realizzano attività di supporto a VENIS.

3.1. Ruoli e Responsabilità per la Sicurezza delle Informazioni

VENIS identifica e indirizza, le responsabilità in merito alla gestione della protezione delle informazioni, nell'ambito del SSIV. Il Presente documento rappresenta una delle ulteriori principali fonti di definizione delle responsabilità nell'ambito del SSIV. Le responsabilità relative alla sicurezza delle Informazioni sono inoltre definite da:

- Codice Etico di Condotta e Sistema Disciplinare;
- Modello Organizzativo 231
- Assegnazione e regole d'uso dei dispositivi mobili aziendali e delle utenze;
- Regolamento Amministratori di Sistema;
- Disciplinare interno contenente le norme di comportamento per l'accesso e l'utilizzo dei sistemi e delle risorse informatiche, della navigazione internet, della gestione della posta elettronica, nonché della gestione dei documenti analogici di VENIS;
- Manuale del Sistema di Gestione per la Sicurezza delle Informazioni;

In particolare, per quanto concerne gli aspetti organizzativi della sicurezza delle informazioni si evidenziano le seguenti regole applicate nell'ambito del perimetro identificato del SSIV:

- L'attribuzione delle responsabilità deve riguardare sia aspetti operativi che aspetti di indirizzo del SSIV (es. definizione degli obiettivi, l'analisi degli aspetti di sicurezza per i vari progetti, la definizione e l'attuazione

di una metodologia di analisi dei rischi, il monitoraggio dei livelli di sicurezza garantiti);

- Tutti gli asset e i processi coinvolti nel perimetro del SSIV devono essere identificati e assegnati formalmente alla funzione responsabile;
- Tutto il personale coinvolto nel SSIV è responsabilizzato nell'efficace realizzazione del SSIV al fine di garantire l'applicazione delle politiche e il raggiungimento degli obiettivi di sicurezza;
- Particolare rilevanza deve essere attribuita alle responsabilità di review periodica e di verifica interna del SSIV.

Il Manuale SSIV e la documentazione del SSIV, anche quando ereditata dalle altre iso possedute dall0azienda, rappresentano gli strumenti che governano l'organizzazione per la sicurezza delle informazioni.

L'obiettivo in oggetto si istanzia nel completare, integrare e mantenere aggiornato tale corpus normativo.

3.2. Separazione dei compiti

L'assegnazione delle responsabilità deve rispettare il principio di separazione dei compiti per ridurre le possibilità di uso improprio, modifica non autorizzata o non intenzionale degli asset del perimetro del SSIV.

VENIS individua, nel perimetro del SSIV, i ruoli in potenziale conflitto tra loro e istituisce controlli e approvazioni finalizzati al mitigare i rischi (es. uso improprio, modifica non autorizzata o non intenzionale).

Nell'ambito del SSIV si possono individuare i seguenti ambiti in cui si potrebbe individuare un rischio in ambito SoD:

- Gestione degli approvvigionamenti – A tale riguardo si faccia riferimento alla Procedura "Gli approvvigionamenti in VENIS" in cui sono formalizzati tutti i controlli, conformi a quanto richiesto dal Codice delgli Appalti, finalizzati al mitigare il rischio di frodi mediante la

separazione dei ruoli all'interno del processo di acquisto;

- Gestione delle utenze (es. account, profili, …) – A tal riguardo si faccia riferimento al Cap. 4 "Controllo degli accessi" del presente documento;
- Change, test, deploy Management – A tal riguardo si faccia riferimento al Cap. 8 "Acquisizione, sviluppo e manutenzione dei sistemi" del presente documento.
- Separazione degli ambienti di sviluppo, test e produzione - A tal riguardo si faccia riferimento al Cap. 10.4.

3.3. Contatti con le Autorità e con Gruppi Specialistici

L'obiettivo del SSIV è quello di assicurare un pronto supporto in ambito ICT alle richieste che pervengono a VENIS dalle Autorità e un adeguato aggiornamento delle competenze delle risorse coinvolte nella sicurezza delle informazioni rispetto alle tematiche trattate

nell'ambito delle associazioni e dai gruppi specialistici in tema di sicurezza delle informazioni.

VENIS assicura il supporto alle Autorità con particolare riguardo agli aspetti relativi ai sistemi informatici che possono emergere, ad esempio, nel corso di verifiche del Garante Privacy o di indagini della competente Autorità Giudiziaria.

Nel caso di contatti con l'Autorità del Garante per la Privacy, questi vengono istituiti, mantenuti e gestiti da Data Protection Officer, supportato dal RSI.

Il RSI ha il compito di garantire il necessario supporto alla Autorità Giudiziaria e alle Autorità preposte alla sicurezza dello Stato e del territorio.

Al fine di garantire il mantenimento e il continuo aggiornamento delle conoscenze e delle competenze il personale, partecipa a convegni e a gruppi specialistici dedicati alla sicurezza delle informazioni e alla ICT Security (es. AIEA / ISACA, CLUSIT, …) mantenendo un registro di tali iniziative formative.

3.4. Sicurezza delle informazioni nella gestione dei progetti

L'obiettivo del SSIV, relativamente a tale ambito, è assicurare che gli aspetti di sicurezza delle informazioni siano considerati in tutti i progetti e che, qualora necessario, siano definiti gli opportuni requisiti di sicurezza.

VENIS ha istituito un processo di gestione dei progetti che prevede il coinvolgimento del RSI per analizzare eventuali esigenze di sicurezza delle informazioni per la Progettazione Applicativa, Sistemistica e di Rete, i requisiti per la sicurezza e la protezione dei dati.

VENIS richiede che il RSI sia coinvolto sempre all'inizio di un progetto. Tale coinvolgimento assicura che siano considerati obiettivi di sicurezza delle informazioni tra quelli di progetto e, ove ritenuto opportuno sarà condotta una opportuna dedicata attività di risk assessment.

3.5. Dispositivi portatili

L'obiettivo del SSIV, relativamente a tale ambito, è assicurare che siano adottate politiche e presidi per la gestione dei rischi introdotti dall'uso di dispositivi portatili e che quindi – per quanto tecnicamente possibile – che le informazioni gestite dai dispositivi mobili aziendali siano adeguatamente protette riducendo la possibilità data leakage.

VENIS ha definito e istituito un insieme di presidi per la gestione e la sicurezza dei dispositivi portatili oggetto dei servizi erogati.

Opportune regole di comportamento che formalizzano le responsabilità degli utenti a cui sono assegnati dispositivi mobili, sono formalizzate nel "*Disciplinare interno contenente le norme di comportamento per l'accesso e l'utilizzo dei sistemi e delle risorse informatiche, della navigazione internet, della gestione della posta elettronica, nonché della gestione dei documenti analogici di VENIS.*

COMPUTER PORTATILI

La gestione dei computer portatili prevede l'applicazione di strumenti di cifratura dei dischi per prevenire i rischi di perdita/furto del dispositivo e delle informazioni in questo contenute. La soluzione adottata permette la gestione automatica del dispositivo legato al dominio mediante opportune politiche. Le porte di accesso sono inibite al collegamento di dispositivi di archiviazione esterna.

SMARTPHONE

In merito alla gestione degli smartphone VENIS adotta l'approccio BYOD. Ai dipendenti di VENIS viene dunque data la possibilità di usare l'utenza aziendale con uno Smartphone che, non essendo direttamente gestibile dall'azienda, può essere considerato ai fini della sicurezza delle informazioni come un dispositivo personale *(vedi regolamento "Assegnazione e regole d'uso dei dispositivi mobili aziendali").*

4. Sicurezza delle risorse umane

L'obiettivo del SSIV, relativamente a tale area, è quello di assicurare che le risorse umane, coinvolte nei differenti aspetti della sicurezza delle informazioni nell'ambito di applicazione, siano in grado di garantire un opportuno livello di protezione delle informazioni.VENIS adotta tutte le fasi di selezione, di ingresso, di impiego della risorsa oltre che la fase di chiusura del rapporto lavorativo assicurando che:

- il personale e i collaboratori comprendano le proprie responsabilità e siano adatti a ricoprire i ruoli per i quali sono presi in considerazione;
- il personale e i collaboratori siano a conoscenza delle loro responsabilità per la sicurezza delle informazioni e vi adempiano;
- gli interessi dell'organizzazione come parte del processo di variazione o di cessazione del rapporto di lavoro siano tutelati.

4.1. Aspetti di sicurezza nelle fasi di selezione e inserimento

L'obiettivo del SSIV, relativamente a tale ambito, è garantire che il profilo del personale candidato all'inserimento nel perimetro di applicazione sia allineato con i requisiti di professionalità, conoscenza, consapevolezza in tema di sicurezza delle informazioni ed etica che tale sistema persegue.

In VENIS il processo di selezione prevede, nel rispetto delle leggi e dei regolamenti applicabili:

- un'analisi critica delle referenze, delle qualifiche accademiche e professionali dichiarate, oltre che del Curriculum Vitae;
- una valutazione complessiva dell'adeguatezza degli aspetti professionali e personali (affidabilità, competenze, etica, esperienze passate) raccolti in sede di colloqui.

A fronte del Provvedimento Garante per la Privacy "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici

relativamente alle attribuzioni delle funzioni di amministratore di sistema", si specifica che VENIS garantisce, all'interno dei

processi di attribuzione dei ruoli e delle responsabilità, che:

l'attribuzione delle funzioni di amministratore di sistema da parte del Titolare o del Responsabile del trattamento avviene previa 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;

- la designazione quale amministratore di sistema deve essere individuale e recare l'elencazione analitica degli ambiti di responsabilità e di operatività consentiti in base al profilo di autorizzazione assegnato. Gli elementi ai quali si fa riferimento nel presente paragrafo sono tenuti in considerazione anche nell'ambito della ricerca e selezione di fornitori esterni.

In riferimento alle modalità di inserimento si faccia riferimento alla procedura di "on- boarding".

4.2. Termini e condizione di impiego

L'obiettivo del SSIV, relativamente a tale ambito, è garantire che il personale interessato dal Sistema di Gestione, sia informato e formato per adempiere i propri compiti con particolare riferimento alla sicurezza delle informazioni.

Nell'ambito della documentazione e dei contratti prodotti in fase di assunzione sono indirizzati alcuni aspetti afferenti la gestione della sicurezza delle informazioni; in particolare:

- l'informativa al trattamento dei dati personali ai sensi del D.Lgs 196/2003 (Codice in materia di protezione dei dati personali);
- sottoscrizione, laddove necessario, di patti di riservatezza ("Non disclosure agreement");
- il "Modello di organizzazione, gestione e controllo ex D. Lgs. 8 Giugno

2001 N. 231" che articola in particolare il "sistema sanzionatorio" per il personale, i "Principi generali di comportamento" (che contengono indicazioni sulla riservatezza e l'integrità delle informazioni e dei dati aziendali)

- il "Codice di comportamento" che contiene espliciti riferimenti alla protezione delle informazioni aziendali;
- le presenti "Politiche specifiche per la Sicurezza delle Informazioni" che dettano le linee guida per la definizione delle regole di sicurezza delle informazioni adottate in VENIS;
- il "Disciplinare comportamentale per la sicurezza delle informazioni – VSI-AT- POS- 02" che contiene regole di comportamento per l'utilizzo sicuro degli asset ICT e delle informazioni da parte degli utenti.

In relazione alle sanzioni previste in caso di comportamento difforme rispetto a quanto richiesto dalla società nei documenti afferenti la sicurezza (istruzioni di lavoro, policy, procedure, etc.), si farà riferimento al Sistema disciplinare ed ai meccanismi sanzionatori di cui al Modello di Organizzazione, Gestione e Controllo ex D.lgs 231/2001. In caso di contestazione disciplinare con sospensione cautelativa si provvede al blocco di tutte le utenze. Tale blocco viene poi confermato in caso di provvedimento di licenziamento oppure revocato.

Gli accordi contrattuali specificano, laddove necessario, i ruoli e le responsabilità di alto livello anche in tema di sicurezza delle informazioni comprendendo l'accettazione delle politiche di sicurezza aziendali.

Nello specifico VENIS si pone l'obiettivo di formare adeguatamente, secondo le rispettive esigenze, il personale coinvolto nel SSIV in merito alle tematiche di sicurezza delle informazioni.

In particolare VENIS comunica al personale che opera nel SSIV tutte le normative aziendali che costituiscono il corpo documentale di riferimento per tale sistema di gestione.

A livello aziendale il processo di formazione aziendale assicura che le risorse in ambito siano opportunamente formate su tematiche di sicurezza delle informazioni (i contenuti sono responsabilità di RSI), ivi inclusa la creazione di una cultura aziendale orientata alla corretta considerazione degli aspetti di sicurezza nell'operatività dei diversi ruoli.

Il personale è informato circa il corretto utilizzo degli asset aziendali assegnati (Rif. "Disciplinare interno contenente le norme di comportamento per l'accesso e l'utilizzo dei sistemi e delle risorse informatiche, della navigazione internet, della gestione della posta elettronica, nonché della gestione dei documenti analogici di VENIS).

A completamento di ciò, per assicurare la corretta gestione del personale delle Terze Parti (fornitori), VENIS ha definito delle regole per indirizzare la gestione dei fornitori ICT (*Gestione delle relazioni con i fornitori ICT*) in cui si prevedono gli esempi delle integrazioni contrattuali per enfatizzare gli aspetti relativi alla sicurezza delle informazioni delle attività e delle responsabilità del personale esterno.

4.3. Modifica e cessazione

L'obiettivo del SSIV, relativamente a tale ambito, è garantire che la gestione dell'attribuzione di asset e privilegi al personale sia allineata con le effettive necessità aziendali.

In caso di cessazione o modifica di posizione organizzativa del personale dipendente o collaboratori, si procede alla cessazione/cambiamento degli accessi logici e fisici della

risorsa, alla verifica che siano rispettati i termini e le modalità di restituzione o di sostituzione (in linea con l'eventuale cambio di impiego) degli asset aziendali assegnati.

In particolare, alla conclusione del rapporto di lavoro:

- sono disabilitate/rimosse tutte le credenziali di autenticazione utilizzate dal dipendente e/o collaboratore per l'accesso alle reti, ai sistemi ed alle applicazioni aziendali;
- sono disabilitate/rimosse anche le credenziali utilizzate dalla persona per l'accesso fisico ai locali ed alle aree ad accesso ristretto dell'Azienda (ad esempio abilitazioni badge).

Il dipendente / collaboratore deve restituire tutte le risorse aziendali avute in dotazione secondo le procedure operative di riferimento.

5. Gestione degli Asset

L'obiettivo del SSIV, è quello di garantire che gli asset, e in particolare quelli ICT, siano identificati e le informazioni trattate dai Sistemi ICT siano opportunamente classificate secondo metriche che ne evidenzino la criticità in termini di sicurezza, al fine di facilitare la corretta implementazione di misure di protezione adeguate.

5.1. Tracciamento degli asset ICT

Affinché sia garantito un corretto livello di protezione delle informazioni, tutti gli asset ICT correlati all'ambito del SSIV devono essere opportunamente tracciati, nel rispetto delle regole di seguito elencate.

- Ciascun asset identificato deve essere assegnato ad un referente o ad un riferimento aziendale identificabile. Gli asset tracciati devono essere quelli ritenuti rilevanti ai sensi del SSIV e possono includere tra le varie tipologie: software (applicazioni, DB, ecc.), hardware (server, PC, elementi di rete, ecc.), asset fisici (documenti, ecc.), infrastrutture (dispositivi di comunicazione, ecc.), ecc.
- Il tracciamento degli asset deve riguardare le diverse fasi della vita dell'asset stesso (ivi compresa la sua dismissione).
- Ove applicabile (es. PdL) è necessario che siano predisposti documenti che definiscano puntualmente l'utilizzo accettabile dei suddetti asset.
- Per gli asset ICT di proprietà di VENIS dati in utilizzo a terze parti, che collaborano con VENIS stessa, è necessario identificare un riferimento aziendale che sarà responsabile del ciclo di vita dell'asset e che assicurerà la condivisione con il personale delle terze parti delle politiche interne di utilizzo sicuro dell'asset. Il referente interno deve tener tempestivamente tracciato l'assegnatario esterno dell'asset e assicurarne la restituzione al termine del periodo di collaborazione.

5.2. Catalogo degli asset

Gli asset ICT devono essere opportunamente censiti all'interno del relativo catalogo. L'ownership di tale attività è assegnata al Responsabile della Funzione che governa la gestione del relativo Asset.In fase di IT Change Management, gli asset ICT devono essere catalogati nella fase di Gestione della domanda.Il censimento di un asset ICT consegnato ad un dipendente neoassunto deve essere eseguito durante la fase di onboarding, come definito nella procedura Istruzioni operative per la consegna di PdL ad un nuovo ingresso.

Ogni owner della tipologia di asset ICT ha il compito di effettuare una volta l'anno una verifica sulla correttezza e completezza del catalogo e delle relative assegnazioni.

5.3. Classificazione degli asset

Gli asset ICT tracciati devono essere opportunamente classificati in termini di criticità della sicurezza delle informazioni in essi contenuti, al fine di garantire la corretta applicazione di misure di protezione. Tale classificazione deve essere realizzata nel rispetto delle seguenti indicazioni.

- La classificazione deve tenere conto del valore della risorsa, della sua criticità ai fini aziendali, degli aspetti di riservatezza, integrità e disponibilità, degli eventuali aspetti legali.
- La classificazione deve essere effettuata sulla base delle valutazioni dei referenti (o almeno di quelli principali se ne esistono di molteplici) dei sistemi o secondo diverse logiche aziendali definite (nell'ambito del processo di gestione dei rischi ICT).
- La classificazione deve essere periodicamente aggiornata (nell'ambito del processo di gestione dei rischi ICT).

5.4. Trasporto dei supporti fisici

Per i servizi di trasporto di beni aziendali all'esterno dell'organizzazione, nell'ambito dei contratti sono definite opportune clausole di sicurezza. Le procedure di riferimento definiscono clausole contrattuali, relative alla sicurezza delle informazioni, per i servizi di trasporto.

A tale riguardo si sottolinea che i dispositivi portatili (laptop) sono dotati di cifratura del disco (Bitlocker).

Tale soluzione è gestita in automatico dal laptop mediante attestazoone dello stesso al dominio aziendale: le policy prevedono l'attivazione della configurazione del Bitlocker in automatico al collegamento con il domain controller.

E' attiva la funzionalità TPM (Trusted Platform Module) che, tramite un chip di crittografia insito nel BIOS/HW della PdL, lega il dispositivo, la chiave di cifratura generata e utilizzata e il PIN in modo che non sia possibile decifrare il disco esportandolo su altro sistema.

5.5. Dismissione e distruzione degli asset ict

VENIS, per l'ambito della dismissione e distruzione degli asset ICT centrali, ha adottato una procedura che definisce ruoli, responsabilità e attività operative al fine di presidiare opportunamente tali fasi.

6. Classificazione delle informazioni

6.1. Premessa

Per VENIS l'informazione rappresenta un patrimonio la cui attenta gestione è strategica per la tutela e lo sviluppo del business aziendale. Le informazioni, qualsiasi sia il supporto su cui risiedano, devono dunque essere tutelate e gestite attuando le misure di sicurezza opportune in relazione all'importanza che rivestono per VENIS e individuate attraverso uno specifico processo di classificazione.

In particolare, gli obiettivi di sicurezza riguardano il presidio dei aspetti di riservatezza, integrità, disponibilità, verificabilità e accountability delle informazioni gestite.

Ciò premesso, il processo di classificazione delle informazioni, si focalizza principalmente sul presidio degli aspetti di riservatezza adottando una classificazione principalmente derivante dall'analisi di quest'ultima.

Il presente capitolo ha lo scopo di:

- Definire il trattamento delle informazioni e di stabilire, per ogni livello di classificazione, le modalità di comunicazione, conservazione e distruzione al fine di consentire l'accesso, la modifica e l'uso delle informazioni solo alle persone autorizzate;
- Determinare in modo inequivocabile la proprietà delle informazioni cosicché sia possibile esercitare su di esse tutti i diritti riconosciuti dall'ordinamento giuridico.

In accordo con la Politica di Sicurezza delle informazion di VENIS e in considerazione delle disposizioni normative vigenti applicabili, VENIS ha pertanto definito regole di sicurezza delle informazioni con l'obiettivo di fornire indicazioni in merito ai requisiti minimi di sicurezza e alle necessarie misure di attuazione. Il controllo della corretta applicazione di questa norma è compito del RSI.

6.2. Ownership dell'informazione

I Proprietari (Owner) delle informazioni sono identificati nei Responsabili delle Unità Organizzative in cui l'informazione e/o la relativa forma documentata è gestita.

Il Proprietario delle informazioni è responsabile per la gestione delle informazioni durante tutto il ciclo di vita. Egli può identificare uno o più delegati a cui attribuire, in tale ambito e anche con modelli di delega e controllo gerarchici, le relative responsabilità operative mantenendone comunque la responsabilità finale (accoutability).

6.3. Classificazione ed etichettatura

Il valore dell'informazione è definito sulla base di almeno quattro fattori:

- L'importanza che l'informazione ha all'interno dell'Azienda;
- L'importanza che è data all'informazione all'esterno dell'Azienda;
- La natura operativa o strategica dell'informazione;
- Gli effetti negativi che potrebbero derivare all'Azienda e ai dipendenti in caso di accessi non autorizzati, perdita e/o distruzione dell'informazione.

I requisiti di sicurezza del patrimonio informativo sono la riservatezza, disponibilità e integrità. La maggior parte delle informazioni non richiedono una classificazione in quanto sono informazioni per le quali la normale prassi operativa è una forma sufficiente di controllo.

La seguente classificazione, basata principalmente sull'analisi del profilo relativo alla riservatezza dei dati trattati, che regolamenterà tutte le fasi successive del ciclo di vita, va applicata per quelle informazioni che, per il loro valore, richiedono appropriati controlli.

Seguendo questo principio si possono individuare i seguenti livelli di classificazione:

- Pubblica

- Uso Interno
- Confidenziale
- Esclusivo.

Si riporta nella tabella seguente la definizione dei quattro livelli sopra elencati e, per ognuno di essi, degli esempi di tipologie di informazione il cui grado di riservatezza afferisce:

Livello di classificazione	Definizione	Esempi di tipologie di Informazione
Pubblica	• Informazioni ricevute dall'esterno che non presentano precedenti classificazioni in merito alla riservatezza e che non sono vincolate da accordi di riservatezza • Informazioni che dal punto di vista aziendale possono circolare liberamente all'interno e all'esterno dell'Azienda. • Per quanto riguarda le informazioni pubbliche generate all'interno dell'Azienda, pur non avendo caratteristiche di riservatezza, sono comunque necessarie revisione e approvazione di contenuto e forma da parte delle strutture aziendali preposte	• Bilancio pubblicato • Campagne pubblicitarie trasmesse • Comunicati ufficiali • Informazioni destinate ai siti Internet Altre informazioni e documenti non precedentemente menzionati che possono essere diffuse al pubblico o a vasti bacini d'utenza (es: Annunci di lavoro, brochure, • ...)
Uso interno	• Informazioni che dal punto di vista aziendale o per l'esistenza di diritti di proprietà appartenenti a VENIS possono circolare, in forma completa, soltanto all'interno dell'Azienda. • La perdita di riservatezza di queste informazioni può avere un impatto diretto non grave, ma le informazioni potrebbero essere utilizzate in modalità potenzialmente dannose.	• Elenchi telefonici interni • Verbali riunioni • Organigrammi, Linee guida, Direttive, Documenti funzioni • Norme e procedure (es. Procedure operative, Istruzioni di lavoro, ...) • Informazioni destinate

		alla Intranet aziendale • Database / Archivi dati
Confidenziale	• Informazioni critiche per le attività dell'organizzazione, la cui diffusione non autorizzata, la perdita, la manomissione o l'uso indebito potrebbero ostacolare il realizzarsi di determinate azioni strategiche impattando sul business ed arrecare danni gravi a VENIS, ai suoi dipendenti e/o a terzi. • Queste informazioni, data la loro delicatezza, sono soggette a misure restrittive. • La loro diffusione è basata sul principio di necessità ("*need to know*") e inoltre sono messe a disposizione delle sole persone autorizzate dal Proprietario, anche mediante un sistema di delega, a • conoscerle per lo svolgimento del loro lavoro.	• Comunicazioni interne relative all'andamento aziendale, i dati di contabilità analitica e di bilancio • Password shipment • Informazioni relative agli incidenti di sicurezza • Informazioni relative al vulnerability management

Esclusivo	Informazioni strategicamente rilevanti e definite tali dal Vertice Aziendale, la cui diffusione, sia interna che esterna a VENIS, possa causare gravi danni in area tecnica, commerciale, gestionale e finanziaria. • La loro diffusione è basata sul principio di necessità ("*need to know*") e inoltre sono • destinate ad un numero limitato di soggetti, definito dal Proprietario delle informazioni.	• Documenti strategici e informazioni riguardanti operazioni societarie acquisizioni, cessioni, scorpori, etc.) • Riorganizzazioni aziendali e strategie future (piani poliennali)

Per meglio supportare il Proprietario (Owner) dell'informazione nella definizione della classificazione delle informazioni, ferma restando la responsabilità nell'approvare il livello di classificazione del documento, si stabilisce che:

- Per i documenti prodotti all'interno di VENIS (in formato cartaceo o elettronico – comprese le e-mail) la classificazione delle informazioni è responsabilità di colui che redige/elabora il documento stesso (autore).
- Per i documenti provenienti dall'esterno della Società la classificazione delle informazioni è responsabilità dell'utente destinatario del documento stesso.
- L'etichettatura, in alcuni casi può non risultare tecnicamente possibile (es. Documenti esterni originali non etichettati, documenti originali redatti antecedentemente all'introduzione della presente norma , ...). In tali casi occorre valutare di volta in volta se necessario e come rendere comunque esplicita la classificazione delle informazioni trattate.
- Nei messaggi di posta elettronica contenenti informazioni o documenti classificati deve essere specificato nell'oggetto la tipologia di classificazione.

- Solo per il livello "Strettamente Confidenziale" sulla parte in basso a destra va posto il numero di pagina costituito da una o più cifre separate da una barra, di cui la prima indica il numero del foglio e la seconda il totale dei fogli componenti il documento (ad es., la pag. 3 di un documento di 6 fogli viene indicato 3/6).

Si noti che in caso di dati personali, il trattamento è consentito ai soli incaricati o ai responsabili del trattamento e deve rispettare le disposizioni della normativa Privacy tempo per tempo applicabile.

In caso di documenti cartacei, il Proprietario delle informazioni, o un suo delegato, si occupa di identificare o di far realizzare una "Master Copy" dell'informazione, da utilizzarsi come riferimento per generare le copie che devono essere distribuite ai destinatari e agli utilizzatori. La "Master Copy" ha anche la funzione di garantire la disponibilità dell'informazione e di sopperire a eventuali richieste di destinatari e utilizzatori autorizzati.

Dopo aver classificato l'informazione è necessario seguire alcune regole relative alla gestione e alla protezione della stessa.

Le informazioni devono essere ricevute e utilizzate appropriatamente solo dalle persone (destinatari) che ne necessitano per ragioni di lavoro, o per poter svolgere specifiche attività aziendali. Tali informazioni inoltre (copia conforme o per conoscenza) dovranno essere ricevute solo dalle persone che per la responsabilità o la posizione aziendale che occupano ne devono essere informati.

Sono di seguito descritte le modalità operative per la comunicazione via mail, via posta ordinaria o consegna diretta, per la conservazione e distruzione delle informazioni.

6.4. Ciclo di vita dell'informazione

Tutte le informazioni, una volta impresse su un qualsiasi tipo di supporto, sono tipicamente caratterizzate da un ciclo di vita. Quest'ultimo, nell'ambito

della Classificazione delle Informazioni, può essere strutturato nelle seguenti fasi principali:

- Etichettatura (labeling) – una volta classificata, l'informazione è etichettata per rendere esplicito il livello di classificazione attribuito; le modalità di etichettatura variano in base alla tipologia di supporto su cui l'informazione è trattata
- Accesso e consultazione – l'informazione può essere disponibile per consultazione o è possibile consentirne l'accesso in scrittura
- Trasmissione – l'informazione può essere trasmessa attraverso un mezzo elettronico (es. fax, e-mail) o fisico (es. posta tradizionale)
- Archiviazione e duplicazione – l'informazione, laddove in formato digitale può essere memorizzata, ad esempio a seguito della sua creazione, su un database o su una share di rete, oppure, se in formato cartaceo, custodita in un archivio (es. armadio, cassettiera)

Dismissione – al termine del proprio ciclo di vita l'informazione deve essere dismessa. Questo si traduce, in termini operativi, nella dismissione del supporto che contiene il dato (ad esempio, documento cartaceo, chiavetta USB, ecc.) con le modalità più opportune, coerentemente con la tipologia di supporto. Un processo di dismissione sicura garantisce pertanto che le informazioni al termine del loro ciclo di vita non vengano divulgate a persone non autorizzate.

Le fasi del ciclo di vita dell'informazione permettono quindi di determinare, congiuntamente alle tipologie di supporti attraverso i quali è trattata l'informazione, l'ambito di applicazione su cui verranno applicate le specifiche misure di protezione, come riportato nei paragrafi seguenti.

6.5. Misure di sicurezza

Al fine di assicurare un adeguato livello di protezione delle informazioni, sono definite specifiche misure di protezione da adottare dipendentemente dal supporto su cui risiede.

Le misure di protezione di seguito identificate rappresentano una baseline minimale di sicurezza che può essere integrata a fronte delle risultanze del processo di analisi dei rischi di sicurezza delle informazioni.

	Basso [Pubblico]	Medio [Uso Interno]	Alto [Confidenziale]	Molto Alto [Esclusivo]
ETICHETTATURA (LABELING)	▪ Facoltativa - notazione "PUBBLICO " o "AD USO PUBBLICO" su etichetta applicata al supporto o indicata su prima pagina documento cartaceo	▪ Facoltativa - notazione "INTERNO" o "AD USO INTERNO" su etichetta applicata al supporto o indicata su prima pagina documento cartaceo	▪ Obbligatoria - notazione "CONFIDENZIALE" o "AD USO CONFIDENZIALE" su etichetta applicata al supporto o indicata su tutte le pagine del documento cartaceo	▪ Obbligatoria - notazione "ESCLUSIVO" o "AD USO ESCLUSIVO" su etichetta applicata al supporto o indicata su tutte le pagine del documento cartaceo
ACCESSO E CONSULTAZIONE	▪ Nessun requisito di sicurezza specifico	▪ Consentito al personale interno e al personale esterno autorizzato dal relativo referente interno (es. Responsabile del Contratto)	▪ Consentito solo a personale interno autorizzato dal responsabile di Funzione e, ove strettamente necessario, a personale esterno autorizzato dal relativo referente interno (es. Responsabile del Contratto), previa stipula di NDA	▪ Consentito solo a personale inserito all'interno della apposita lista di distribuzione definita dall'owner dell'informazione

TRASMISSIONE	▪ Nessun requisito di sicurezza specifico	▪ Fax / mezzo postale – invio consentito verso personale interno o verso personale esterno autorizzato dal relativo referente interno (es. Responsabile del Contratto)	▪ Fax / mezzo postale – invio consentito solo a personale interno autorizzato dal responsabile di Funzione e, ove strettamente necessario, a personale esterno autorizzato dal relativo referente interno (es. Responsabile del Contratto), previa stipula di NDA ▪ Fax / mezzo postale – l'invio deve avvenire con annotazione del destinatario e del livello di classificazione. L'originale cartaceo inviato via fax, il fax ricevuto non deve essere lasciato nel dispositivo di stampa/fax ▪ Mezzo postale - invio ▪ posta raccomandata	▪ Fax - l'invio non può avvenire ▪ Mezzo postale – invio consentito solo a personale inserito all'interno della apposita lista di distribuzione definita dall'owner dell'informazione e solo in busta sigillata per mezzo di posta raccomandata con ricevuta ▪
ARCHIVIAZIONE E DUPLICAZIONE	▪ Nessun requisito di sicurezza specifico	▪ Archiviazione in armadio o cassettiera ▪ Copia / stampa – consentita a tutto il personale interno e solo	▪ Copia / stampa – consentita solo al personale interno autorizzato dal responsabile di Funzione e, ove strettamente necessario, a personale esterno autorizzato dal	▪ Copia/stampa autorizzata e registrata, a cura dall'owner dell'informazione, su un apposito registro ▪ La stampa/ fotocopia non deve essere lasciata nel

		al personale esterno autorizzato dal relativo referente ▪ interno (es.	relativo referente interno (es. Responsabile del Contratto), previa stipula di NDA ▪ La stampa/ fotocopia non deve essere lasciata nel	dispositivo di riproduzione ▪ Archiviazione in cassaforte o armadi di sicurezza chiusi a
DISMISSIONE	▪ Nessun requisito di sicurezza specifico	▪ Consigliate procedure di dismissione/ cancellazione sicura	▪ Procedure di dismissione/cancellazione sicura (es. distruzione tramite dispositivo trita-documenti)	▪ Procedure di dismissione/ cancellazione sicura tracciate (es. distruzione tramite dispositivo trita- ▪ documenti)

6.6. Supporti digitali – sistemi informatici

La tabella seguente illustra le misure di protezione da adottare sui Sistemi Informatici sulla base del ciclo di vita e del livello di classificazione.

	Basso [Pubblico]	Medio [Uso Interno]	Alto [Confidenziale]	Molto Alto [Esclusivo]
ETICHETTATURA (LABELING)	▪ Nessuna misura di sicurezza richiesta	▪ Identificazione in fase di definizione dei requisiti della classificazione delle informazioni trattate	▪ Identificazione in fase di definizione dei requisiti della classificazione delle informazioni trattate ▪ Identificazione della presenza al	▪ Identificazione in fase di definizione dei requisiti della classificazione delle informazioni trattate ▪ Identificazione della presenza al suo interno di dati esclusivi

			suo interno di dati confidenziali	
ACCESSO E CONSULTAZIONE	▪ Nessuna misura di sicurezza richiesta	▪ Gestione controllo accessi centralizzata (autenticazione) Privilegi d'accesso assegnati a tutti gli utenti sulla base del need-to-know (approvazione responsabile di Funzione)	▪ Gestione controllo accessi centralizzata (autenticazione) Privilegi d'accesso assegnati a tutti gli utenti sulla base del need-to-know (approvazione responsabile di Funzione)	▪ Gestione controllo accessi centralizzata (autenticazione e autorizzazione) con strong authentication ▪ Privilegi d'accesso assegnati solo sulla base del need-to- know (sia per utenti interni che esterni approvazione responsabile Sicurezza delle informazioni
TRASMISSIONE	▪ Nessun requisito di sicurezza specifico	▪ Crittografia a livello di canale di trasmissione (consigliata)	▪ Crittografia a livello di canale di trasmissione (es. HTTPS, SFTP)	▪ Crittografia a livello di canale di trasmissione e a livello di dato/applicativo

ARCHIVIAZIONE E DUPLICAZIONE	▪ Nessuna misura di sicurezza richiesta	▪ Nessuna misura di protezione richiesta	▪ Crittografia a livello di dato/ database o di disco ▪ Consigliata cifratura backup ▪ Non consentita la presenza in chiaro di informazioni confidenziali ▪ all'interno dei log	▪ Crittografia a livello di dato/database ▪ Cifratura backup ▪ Non consentita la presenza in chiaro di informazioni esclusive all'interno dei log
DISMISSIONE	▪ Nessuna misura di sicurezza ▪ richiesta	▪ Consigliate procedure di dismission e ▪ sicura	▪ Procedure di dismissione sicura	▪ Procedure di dismissione sicura

6.7. Supporti digitali – dotazioni informatiche aziendali

La tabella seguente illustra le misure di protezione da adottare sulle informazioni trattate tramite Dotazioni Informatiche Aziendali, in base al loro ciclo di vita e al relativo livello di classificazione.

	Basso [Pubblico]	Medio[Uso Interno]	Alto [Confidenziale]	Molto Alto [Esclusivo]

ETICHETTATURA (LABELING)	▪ Facoltativa notazione "PUBBLICO" o "AD USO PUBBLICO" su metadato file o indicata su template documento digitale	▪ Facoltativa - notazione "INTERNO" o "AD USO INTERNO" su metadato file o indicata su template documento digitale	▪ Obbligatoria - notazione "CONFIDENZIALE" o "AD USO CONFIDENZIALE" su metadato file o indicata su template documento digitale	▪ Obbligatoria - notazione "ESCLUSIVO" o "AD USO ESCLUSIVO" su metadato file o indicata su template documento digitale
ACCESSO E CONSULTAZIONEz	▪ Nessun requisito di sicurezza specifico	▪ Consentito verso personale interno o verso personale esterno autorizzato dal relativo referente interno (es. Responsabile del Contratto),	▪ Consentito solo a personale interno autorizzato dal responsabile di Funzione e, ove strettamente necessario, a personale esterno autorizzato dal relativo referente interno (es. Responsabile del Contratto), previa stipula di NDA	▪ Consentito solo a personale inserito all'interno della apposita lista di distribuzione definita dal owner dell'informazione

TRASMISSIONE	▪ Nessun requisito di sicurezza specifico	▪ Posta elettronica o altri strumenti aziendali di comunicazione/condivisione (es. Yammer, Lync, chiavetta USB aziendale), invio consentito verso personale interno o verso personale esterno autorizzato dal relativo referente interno (es. Responsabile del Contratto),	▪ Invio solo a personale interno autorizzato (approvazione responsabile di Funzione) e, ove strettamente necessario, a personale esterno autorizzato dal relativo referente interno (es. Responsabile del Contratto), previa stipula di NDA ▪ Posta elettronica o altri strumenti di ▪ comunicazione.	▪ Invio consentito solo a personale inserito all'interno della apposita lista di distribuzione definita dal owner dell'informazione ▪ Posta elettronica o altri strumenti aziendali di comunicazione/condivisione – cifratura dei contenuti ▪ Posta elettronica - Indicazione "Esclusivo" sull'oggetto della ▪ mail
ARCHIVIAZIONE E DUPLICAZIONE	▪ Nessun requisito di sicurezza specifico	▪ Salvataggio, se non temporaneo, consentito solo su strumenti messi a disposizione dall'azienda e non su dispositivi personali	▪ Salvataggio consentito solo su strumenti messi a disposizione dall'azienda ▪ Archiviazione, ove possibile, su dischi di rete condivisi ad accesso controllato ▪ Effettuare il salvataggio sulle postazioni di lavoro locali o su dispositivi	▪ Salvataggio consentito solo su strumenti messi a disposizione dall'azienda. ▪ Archiviazione consentita solo su Sistemi Informatici centralizzati ad accesso controllato. ▪ Non è consentito il salvataggio sulle

			removibili limitandolo al tempo strettamente necessario ▪ Consigliata cifratura ▪ dei file	postazioni di lavoro locali o su dispositivi removibili ▪ Cifratura dei file
DISMISSIONE	▪ Nessun requisito di sicurezza ▪ specifico	▪ Consigliate procedure di dismissione/canc ▪ ellazione sicura	▪ Procedure di dismissione/canc ella zione sicura	▪ Procedure di dismissione/can cella zione sicura

7. Controllo accessi

L'obiettivo del SSIV, relativamente all'area del controllo degli accessi logici, è quello di proteggere opportunamente le informazioni in ambito prevenendo che si possano verificare:

- utilizzi impropri dei privilegi di accesso alle informazioni ;
- distruzione dei dati;
- esportazioni non autorizzate ed utilizzo di informazioni riservate.

Tale protezione è realizzata attraverso l'adozione, da parte di VENIS, di misure tecniche, organizzative e procedurali relative alle seguenti specifiche tematiche.

7.1. Requisiti generali per il controllo degli accessi

I principi di gestione degli accessi alle risorse e alle informazioni sono realizzati con i seguenti meccanismi:

- Identificazione e autenticazione - ovvero il processo che consente di validare il tentativo di connessione (da parte di un sistema, di un'applicazione o di un altro utente) ai sistemi per instaurare con essi un "colloquio". La modalità di riconoscimento (login) prevede, nella maggior parte dei casi, la digitazione di una user-id o chiave utente e di una parola segreta (password) conosciuta solo dall'utente e dalla risorsa alla quale si vuole accedere;
- controllo degli accessi e autorizzazione - il processo che permette di verificare l'associazione di sufficienti privilegi alla utenza per consentire l'accesso alle informazioni. Alla fase di autenticazione segue infatti una fase di autorizzazione, finalizzata all'abilitazione delle sole funzionalità concesse alla utenza;
- registrazione degli accessi - operazione che consiste nella scrittura su appositi archivi non modificabili, delle operazioni compiute per l'utilizzo di una risorsa (utente, tipo operazione, data/ora, etc.).

A livello generale gli aspetti di controllo degli accessi ai dati ed alle informazioni devono essere conformi alle regole identificate nelle apposite procedure operative.

A tale documento si aggiungono le seguenti linee guida:

- La gestione degli accessi ai dati ed alle informazioni deve essere applicata ai diversi livelli (sistemistico, applicativo, networking) mediante i quali si può accedere agli stessi.
- I meccanismi di controllo degli accessi devono essere conformi alle normative applicabili.
- I controllo degli accessi deve essere basato su un approccio di deny-all (default) e di gestione delle autorizzazioni correlate (eccezione).
- I profili autorizzativi assegnati devono basarsi su schemi standard. Eventuali autorizzazioni aggiuntive devono essere trattate come aggiuntive rispetto a tali profili base.
- I profili autorizzativi concessi agli utenti devono essere periodicamente verificati dai responsabili dele risorse al fine di garantire la continua consistenza dei livelli di protezione delle informazioni e delle effettive necessità lavorative.
- Attraverso un processo controllato, agli utenti sono assegnate delle credenziali di accesso personali.

I criteri per l'accesso logico ai sistemi VENIS tengono conto della normativa Privacy per il quale l'accesso ai sistemi che trattano dati personali prevede l'utilizzo di una chiave personale univoca.

Qualora si ritenga indispensabile l'utilizzo di chiavi di gruppo (a fronte di limitazioni tecniche o su sistemi non ritenuti critici a seguito dell'analisi dei rischi), tale soluzione deve essere autorizzata dal RSI.

7.2. Gestione degli accessi utenti

L'attribuzione, la modifica e la revoca delle credenziali di accesso ai sistemi deve essere effettuata secondo dei processi standardizzati e strutturati.

- L'attribuzione e la modifica delle credenziali e dei profili autorizzativi devono essere tracciati.
- Le credenziali attribuite agli utenti devono essere personali.
- La componente segreta delle credenziali di accesso è composta in conformità alle normative applicabili e secondo criteri che ne garantiscano un opportuno livello di protezione (lunghezza, scadenza, composizione, ecc.).

7.2.1. Attribuzione delle credenziali e dei relativi permessi

A seguito dell'esecuzione del procedimento di onboarding vengono assegnati all'utenza specifici permessi; generalmente la gestione di tali permessi è condotta tramite l'assegnazione della utenza a specifici Gruppi di Active Directory.

In alcuni casi eccezionali i profili di alcuni servizi sono gestiti a livello applicativo; in tal caso la funzione aziendale dedicata inoltra la richiesta ai gruppi applicativi di competenza per completare le opportune configurazioni.

In caso di risorse esterne il processo si svolge in modo analogo ad eccezione che l'utenza standard non è richiesta dalla funzione "Sviluppo Risorse Umane, Formazione e Comunicazione" ma dal Responsabile interno della risorsa esterna.

La corretta configurazione di quanto richiesto è comunicato via email alla risorsa oggetto della richiesta.

Le credenziali relative a risorse esterne devono essere impostate con una durata limitata a 12 mesi.

7.2.2. Riesame dei diritti di accesso

L'attività di monitoraggio delle abilitazioni delle utenze Active Directory, ha l'obiettivo di rimuovere tutte le abilitazioni non più necessarie in modo da garantire la continua consistenza dei livelli di protezione delle informazioni.

7.2.3. Off boarding o Modifica di mansione

Il processo di cessazione delle utenze Active Directory in VENIS è descritto nel documento "VSI-SSI-POS-20 *Gestione e controllo degli accessi logici".*

In caso l'utenza avesse profili gestiti a livello applicativo, la funzione "Sistemi IT,Sicurezza Informatica" inoltra la richiesta ai gruppi applicativi di competenza per cancellare le opportune configurazioni.

La modifica delle mansioni prevede un processo analogo attivato sempre dalla funzione "HR" che richiede la revisione di tutte le profilazioni specifiche.

7.3. Responsabilità degli utenti

Le regole relative alle prassi di sicurezza nell'uso di informazioni segrete di autenticazione,sono definite nella norma aziendale "Disciplinare interno contenente le norme di comportamento per l'accesso e l'utilizzo dei sistemi e delle risorse informatiche, della navigazione internet, della gestione della posta elettronica, nonché della gestione dei documenti analogici di VENIS (VSI-SS-POS-03)" in cui si sottolinea che l'utente deve rispettare rigorosamente le regole di sicurezza relative alle credenziali (user-id e password) dei propri account (privilegiati o no) che sono personali, non condivisibili, confidenziali e non cedibili a terzi.

7.4. Controllo degli accessi a livello di rete

Al fine di garantire che le misure di controllo degli accessi siano efficaci, è necessario che gli utenti rispettino le seguenti regole.

- I meccanismi di controllo degli accessi a livello di rete devono essere previsti sia per gli accessi da rete locale che da accessi remoti.
- Gli accessi da remoto devono essere regolamentati da più livelli di autenticazione e, qualora applicabile, da almeno un livello basato su Strong authentication.
- Gli accessi alla rete aziendale da remoto devono essere effettuati attraverso protocolli sicuri e/o attraverso soluzioni VPN.
- Le credenziali di autenticazione concesse per l'accesso a livello di rete devono essere personali.

Per ulteriori informazioni si faccia riferimento al Par. 11 "Sicurezza delle comuncazioni" del presente documento.

7.5. Controllo degli accessi sistemistici

Relativamente agli accessi sistemistici, la corretta applicazione del SSIV prevede il rispetto delle seguenti regole:

- Gli accessi effettuati a livello sistemistico devono essere regolamentati da meccanismi di autenticazione.
- Le credenziali di autenticazione concesse per l'accesso a livello sistemistico devono essere personali. L'eventuale utilizzo di credenziali standard (e.g. Root, DB Admin) devono essere adottate solo qualora strettamente necessario e mediante modalità che garantiscano la tracciabilità della loro attribuzione.
- I profili sistemistici devono rispettare il principio del "need to know".
- Gli accessi effettuati a livello sistemistico devono essere registrati su appositi archivi non modificabili (es. tramite SIEM).

Per gli accessi a livello sistemistico devono essere previste misure di session time- out che limitino le sessioni sospese a limitate finestre temporali.

- Le utenze amministrative sono basate su Active Directory. Le limitazioni d'uso sono legate esclusivamente alla profilatura dell'utente ed alle policy di dominio, per quanto riguarda l'accesso ai server e soltanto gli utenti amministratori possono accedere a registry, local policy, registro eventi, ecc.

- A livello client nessun utente deve avere privilegi amministrativi; eventuali eccezioni sono tracciate e approvate dal RSI.

VENIS utilizza strumenti (FreeIPA) integrati con Active Directory per gestire l'autenticazione ai server linux. Per l'accesso sistemistico a SANET si utilizza il tool Radius, mentre per Oracle Exadata l'accesso è consentito solamente al Database Administrator.

7.6. Password

Per assicurare l'accesso agli utenti autorizzati e per prevenire accessi non autorizzati a sistemi e servizi dell'organizzazione è necessario l'utilizzo di una password nel rispetto delle seguenti regole.

- La password deve rispettare i requisiti di complessità e temporalità (lunghezza, tipologia, scadenza, recupero, ecc.) stabiliti a livello aziendale e dalla normativa vigente.
- Il personale VENIS è tenuto a seguire le norme comportamentali per un corretto utilizzo e conservazione delle password stabilite a livello aziendale (es.Clear Desk Policy).
- La password iniziale deve essere modificata dopo il primo accesso.

Nello specifico le password policy client adottate prevedono:

- Massima durata 90 giorni;
- Minimo 12 caratteri alfanumerici di cui almeno tre differenti (scelti tra lettere minuscole, maiuscole, numeri e caratteri

speciali);

- History minima di 5 password
- Almeno un numero
- Almeno un carattere speciale
- Almeno un carattere maiuscolo

La passord policy per gli amministratori deve esserre più complessa che per gli utenti normali

Nello specifico le password policy di root vengono generate automaticamente dal sistema in maniera aleatoria, con i seguenti criteri di complessità:

- Massima durata 90 giorni;

Minimo quattordici caratteri alfanumerici di cui almeno tre differenti (scelti tra lettere minuscole, maiuscole e numeri);

8. Crittografia

8.1. Premessa

L'obiettivo del SSIV adottato da VENIS, relativamente a tale area, è quello di garantire adeguati strumenti crittografici per proteggere le informazioni e i Servizi ICT maggiormente critici dal punto di vista della sicurezza, evitando accessi non autorizzati, utilizzo malevolo o compromissioni involontarie delle informazioni stesse. Ulteriore obiettivo risulta inoltre assicurare la continuità dei servizi erogati da VENIS attraverso il recupero delle informazioni criptate.

In particolare, come definito nella Politica di Sicurezza delle Informazioni (VSI-SI-PS-01) gli obiettivi di sicurezza riguardano il presidio degli aspetti di riservatezza, integrità, disponibilità, verificabilità e accountability delle informazioni gestite.

I controlli crittografici permettono di raggiungere obiettivi legati alla sicurezza delle informazioni, in particolare:

- Confidenzialità: criptazione delle informazioni di tipo sensibile e/o critiche, anche in caso di trasmissione o memorizzazione;
- Integrità/Autenticità: strumenti crittografici come la firma digitale o codici di autenticazione dei messaggi utilizzati ai fini di garantire autenticità ed integrità di informazioni sensibili e/o critiche in fase di trasmissione o memorizzazione;
- Non-ripudio: uso di tecniche crittografiche a supporto di evidenze dell'avvenimento o non avvenimento di un evento o di una azione;
- Autenticazione: utilizzo di tecniche crittografiche per autenticare utenti ed altre entità del sistema che richiedono l'accesso o transazioni con utenti, entità e risorse del sistema.

Le metodologie di criptazione sono utilizzate ai fini della prevezione dalle seguenti minacce:

- Intercettazione: lettura e conseguente perdita di riservatezza di una'nformazione durante il processo di trasmissione della stessa a causa di non-criptazione, criptazione con algoritmo inefficiente o chiave fragile;
- Modifica: alterazione di una informazione durante i processi di trasmissione e/o memorizzazione della stessa;
- Impersonificazione: trasmissione di una informazione caratterizzata da falso mittente, il quale, fingendo di essere una terza persona, ne usurpa credenziali ed autorità.
- Ripudio della potestà di un messaggio: trasmissione di una informazione e successiva negazione dell'esecuzione di tale atto da parte dell'autore.

8.2. Modello di crittografia

Il modello di crittografia si basa sulla protezione della riservatezza delle informazioni. In particolare, le misure di protezione crittografica devono essere applicate alle informazioni con Livello di Classificazione "Confidenziale" o "Esclusivo", delineate nel capitolo 6 di tale documento.

La violazione della riservatezza delle informazioni con livelli di classificazione precedentemente dettagliati possono originare effetti gravosi sull'operatività aziendale, sugli asset e sulle risorse di VENIS.

La definizione delle metodologie crittografiche da utilizzare devono essere ponderate in base alla valutazione del rischio IT con le esigenze legate all'operatività, identificate in solidità ed efficacia dell'algoritmo di cifratura. Tali metologie devono essere comunque sempre rispettate come segue:

Livello di classificazione	Pubblica	Uso Interno	Confidenziale	Esclusivo
Trasmissione	Non previsto	Facoltativo	Obbligatorio	Obbligatorio

Memorizzazione	Non previsto	Non previsto	Facoltativo	Obbligatorio
Documenti	Non previsto	Non previsto	Non previsto	Obbligatorio (Confidenziale)

8.3. Politica per la crittografia

Le crittografia, attraverso un sistema di gestione di chiavi crittografiche, consente di rendere una informazione offuscata, in modo da non essere comprensibile/intelligibile a persone non autorizzate alla lettura di tali informazioni, assicurandone comunque sempre l'autenticità.

8.3.1. Obbligatorietà crittografica

Ogni qualvolta si utilizzino informazioni caratterizzate da Livelli di Classificazione "Confidenziale" o "Esclusivo" si rende necessario l'utilizzo di protocolli sicuri di trasmissione ed un sistema di memorizzazione sicuro attraverso l'uso di tecniche crittografiche.

8.3.2. Gestione chiavi crittografiche

Gli strumenti crittografici devono generare e gestire, con modalità formalizzata, le chiavi di crittografia.

8.3.3. Protezione chiavi crittografiche

Le chiavi crittografiche devono essere protette da modifica, perdita e distruzione. Le chiavi private utilizzate per la crittografia a chiave pubblica (o asimmetrica) o per la cifratura simmetrica devono essere contenute nel wallet Oracle di VENIS. La password per l'accesso a tale wallet deve essere mantenuta sull'applicativo SESAME.

8.3.4. Gestione del ciclo di vita delle chiavi

Le chiavi crittografiche devono essere protette da modifica, perdita e distruzione. Le chiavi private utilizzate per la crittografia a chiave pubblica (o asimmetrica) o per la cifratura simmetrica devono essere contenute nel wallet Oracle di VENIS. La password per l'accesso a tale wallet deve essere mantenuta sull'applicativo SESAME.

8.3.5. Certification Authority

I certificati pubblici devono essere emessi da una Certification Autority esterna pubblicamente riconosciuta. Tale certificati devono inoltre possono essere emessi limitatamente alle macchine di Front End ed NGINX.

8.3.6. Protezione fisica

I sistemi e gli apparati utilizzati per generare, memorizzare ed archiviare le chiavi devono essere protetti sia logicamente che fisicamente.

8.4. Misure di trasmissione

Durante la trasmissione di informazioni caratterizzate da Livelli di Classificazione "Confidenziale" o "Esclusivo" deve essere controllato che:

- L'accesso all'informazione critica è permesso esclusivamente agli utenti muniti di chiave per la decodifica;
- La comunicazione dell'informazione dal sistema alla workstation utente deve avvenire in maniera sicura cifrando il canale di scambio (VPN, SSH, SSL/TLS, PPTP);
- Lo scambio effettuato via posta elettronica deve essere cifrato (recupero via HTTPS).

8.5. Misure di memorizzazione

Durante la memorizzazione di informazioni caratterizzate da Livelli di Classificazione "Confidenziale" o "Esclusivo" deve essere controllato che:

- L'accesso all'informazione critica è permesso esclusivamente agli utenti autorizzati all'accesso;
- Non è consentito il salvataggio su strumenti differenti da quelli messi a disposizione da VENIS;
- Ogni strumento utilizzato per la memorizzazione (disco ottico, floppy, USB) deve essere criptato e posto in luogo sicuro;
- Il trasporto di suddetti strumenti di memorizzazione deve avvenire in modo sicuro;

Il recupero dell'informazione crittografata deve essere possibile a seguito dell'avvallo della Direzione di VENIS.

9. Sicurezza fisica ambientale

L'obiettivo del SSIV, relativamente all'area della sicurezza fisica e ambientale, è quello proteggere opportunamente gli ambienti in cui sono custoditi gli apparati ICT necessari per erogare i Servi ICT, i dispositivi stessi oltre che gli impianti di supporto necessari per il loro corretto funzionamento; questo al fine di evitare:

- accessi fisici non autorizzati alle sedi, ai locali tecnici e al centro di elaborazione dati (CED) che ospitano asset ICT appartenenti al perimetro del SSIV;
- danneggiamenti e/o distruzione e/o furto di tali asset ICT contenenti informazioni appartenenti al perimetro del SSIV.

Tale protezione è garantita attraverso l'adozione, da parte di VENIS, di misure tecniche, organizzative e procedurali relative alle tematiche di seguito riportate.

9.1. Gestione della sicurezza delle sedi, delle aree e dei locali

Il RSI, coordinando le funzioni Certificazioni e S.I.A. e Sistemi IT,Sicurezza Informatica ciascuna per le aree di propria competenza, come definito in Disposizione Organizzativa (VOP-OP-FG-02), Microstruttura funzionale (VOP-OP- FG-03), definisce e assicura un insieme minimo di requisiti di sicurezza da applicare alle sedi, alle aree e ai locali che contengono Sistemi ICT siti nei CED.

Gli asset ICT fisici contenenti le informazioni appartenenti al SSIV devono essere tutelati tramite l'adozione di misure di sicurezza per le sedi, le aree ed i locali, in modo da scongiurare il danneggiamento o la sottrazione d'informazioni e beni aziendali. È quindi necessario:

- individuare le sedi, le aree e i locali che ospitano asset contenenti le informazioni in ambito SSIV, identificandone la criticità e predisponendo opportune planimetrie che descrivano in modo sistematico la pianta della sede e i principali dettagli che possono interessare il relativo presidio di sicurezza;
- proteggere l'accesso al sito mediante adeguati presidi di portineria e/o

vigilanza (es. ronde e presidio 24x7), gestione e videosorveglianza dei varchi e, ove opportuno, sensori antintrusione (es. infrarossi, reti allarmate) lungo il perimetro; i sistemi a tutela degli ingressi e dei varchi verso l'esterno devono essere installati e regolarmente sottoposti a verifiche e manutenzione;

- limitare l'esposizione e il numero dei varchi del perimetro delle sedi verso l'esterno e comunque monitorarli costantemente (es. appunto con sistemi di video sorveglianza);
- proteggere in particolare i CED da accessi non autorizzati attraverso varchi videosorvegliati monitorati, allarmi antintrusione (es. sensori volumetrici, sensori magnetici) e sicurezza alle eventuali finestre (es. vetri antisfondamento);
- assicurare un adeguato posizionamento dei sistemi di videoregistrazione in ambiente ad accesso controllato (es. nel CED stesso, in locali opportunamente protetti);
- assicurare una corretta ed efficace politica di cancellazione Immagini che garantisca la conservazione delle immagini per un massimo di 7 gg;
- assicurare l'efficacia di procedure o politiche di accesso alle immagini registrate della videosorveglianza che deve essere permesso mediante l'utilizzo di utenze nominali assegnate a persona opportunamente designate in ambito Privacy;
- assicurare che le aree non presidiate siano fisicamente chiuse e controllate con cadenza regolare. Tali aree non devono essere accessibili senza una regolare verifica o autorizzazione e un formale controllo;
- garantire che tutte le porte antincendio siano allarmate;
- presidiare nello specifico gli accessi ai CED mediante porte con serrature a badge e gestione puntuale (mediante registrazione) dei visitatori e in genere di chi accede ai CED accompagnato da personale dotato di badge abilitato;
- gli accessi ai centri di elaborazione devono prevedere strumenti di autenticazione a due fattori (es. badge e PIN);

- proteggere l'accesso non autorizzato a eventuali locali tecnici che ospitano apparati ICT (es. rack di piano, switch LAN).

9.1.1. Criteri di gestione degli accesi al CED

L'accesso alle aree CED (ivi inclusi i locali TLC o i locali tecnici in esso contenuti) deve avvenire attraverso una porta con elettro-serratura, comandata da lettore di badge controllato dal sistema centrale di controllo accessi.

I locali che non siano identificabili come CED o gli armadi tecnici fuori dal CED in cui siano collocati apparati di rete necessari alla distribuzione dei servizi all'interno della sede (es. switch di piano), devono essere chiusi a chiave e le chiavi devono essere gestite, dalle funzioni responsabili della Segreteria e dalle funzioni responsabili della gestione della logistica degli impianti, in modalità sicure che prevedano perlomeno:

- etichettatura delle chiavi;
- conservazione in bacheche chiuse/presidiate;
- movimentazione delle chiavi tracciate in un apposito registro.

L'accesso all'area CED e agli eventuali differenti locali è consentito a a:

- personale (interno e esterno) speficatamente autorizzato;
- visitatori accompagnati da personale speficatamente autorizzato.

Nel primo caso l'accesso all'area CED e agli eventuali differenti locali è consentito soltanto ai possessori di badge:

- non scaduto, e rilasciato dalla funzione aziendale preposta al suo controllo;
- specificamente abilitato all'apertura dei varchi corrispondenti;
- autorizzato dal RSI

L'accesso ai locali CED da parte dei visitatori (es. collaboratori esterni, fornitori, terze parti, etc.) deve essere limitato e deve sempre prevedere l'accompagnamento da parte del personale autorizzato ad operare nel CED che è responsabile di tracciare nell'apposito registro tali accessi e vigilare costantemente la presenza e le attività del visitatore.

Procedura di gestione degli accesi al CED

9.1.2. Procedura di gestione degli accessi al CED

A fronte di esigenze di attribuzione/modifica delle abilitazioni di accesso ai locali CED relative ad una risorsa, il suo responsabile deve emettere una richiesta tramite il sistema di ticketing aziendale che informi in copia il RSI per l'approvazione della richiesta.

Il richiedente deve indicare le motivazioni della domanda di accesso. In caso di richiesta di accesso per personale esterno la validità dell'autorizzazione deve avere durata limitata nel tempo (con un massimo periodo di 12 mesi).

9.1.3. Ingresso visitatori sprovvistidi badge abilitato

I visitatori sprovvisti di badge abilitato possono accedere ai locali CED se accompagnati da personale dotato di badge abilitato. Quest'ultimo è responsabile di tracciare nel registro cartaceo opportunamente predisposto nei locali interessati, l'accesso del visitatore identificando:

- Data dell'accesso;
- Cognome e nome del visitatore;
- Società di appartenenza del visitatore;
- Orario di ingresso e di uscita;
- Cognome e nome dell'accompagnatore (personale dotato di badge abilitato)
- Firma dell'accompagnatore (personale dotato di badge abilitato).

9.2. Gestione della sicurezza degli asset e delle apparecchiature

Le apparecchiature ICT devono essere protette in modo tale da garantire nel tempo la riservatezza, l'integrità e la disponibilità delle informazioni accedute attraverso esse. Devono quindi essere ubicate in aree sicure e/o fisicamente protette da minacce e pericoli ambientali in modo da prevenire la perdita, il danno o la compromissione del patrimonio informativo.

A tal fine è necessario:

posizionare correttamente le apparecchiature ICT all'interno dei CED o dei locali tecnici gestendo adeguatamente il cablaggio (es. cablaggio strutturato fascettato e, ove opportuno, etichettato), evitando materiale superfluo e curando la pulizia1 e l'ordine di tali locali;

al fine di garantire una corretta pulizia e manutenzione dei locali del CED e degli apparati contenuti, procedere ad una attività di pulizia programmata volta a sanitizzare gli ambienti, mantenere efficiente i sistemi di ventilazione e condizionamento e minimizzare qualsiasi situazione che possa provocare incidenti e di pulizia deve comprendere tutte le aree della sala e fissare una frequenza minimale semestrale;

- al fine di limitare l'accesso ai dispositivi ICT centrali (es. personale impiantistico che deve aver accesso ai CED per operare sulle infrastrutture ma non deve accedere ai sistemi ICT), i rack devono essere possibilmente chiusi a chiave e tali chiavi gestite in cassette ad accesso controllato;
- il cablaggio dati, ove possibile, deve essere separato dal cablaggio elettrico. Il cableggio in genere deve essere preferibilmente gestito mediante canaline per favorire il suo ordine strutturato;
- predisporre le condizioni ambientali ottimali2 per il corretto funzionamento delle apparecchiature ICT (es.: condizionamento e relativi allarmi, sensori di temperatura, sensori di umidità, sensori antiallagamento);

- proteggere le apparecchiature ICT da interruzioni di energia o altre anomalie elettriche, attraverso la predisposizione di opportuni meccanismi3 (ad es. linee di alimentazione multiple, UPS, generatori, batterie tampone, ecc.);
- manutenere le apparecchiature in osservanza alle specifiche tecniche dei fornitori, in modo da garantirne nel tempo integrità e disponibilità;
- tutte le apparecchiature e gli impianti (es. condizionamento, sistemi rilevamento antincendio/fumi, sistemi spegnimento, sensori di allarmi, UPS, generatore di continuità, impianto elettrico) devono prevedere manutenzione e verifiche periodiche documentate.

Di seguito sono identificate ulteriori regole comportamentali rivolte al personale VENIS:

- il personale operante nel CED deve comunicare tempestivamente a RSI e al Proprio Responsabile eventuali incidenti, violazioni alle norme aziendali (es. l'asportazione, la manomissione o il danneggiamento di beni aziendali) e ogni possibile rischio percepito;
- è vietato cedere a terzi le proprie credenziali di accesso (badge e PIN), anche temporaneamente, e nel caso ne venga meno il possesso deve esserne data tempestiva comunicazione alla Sicurezza;
- è vietato accedere alle aree riservate se non in possesso di specifica autorizzazione;
- è vietato, per chi è in possesso della prevista autorizzazione, permettere l'accesso a personale non autorizzato o privo di badge se non tramite le prestabilite procedure di richiesta;
- il personale operante nel CED deve assicurarsi che le porte siano chiuse al momento dell'uscita;
- è vietato lasciare le porte aperte della sala, degli armadi blindati, casseforti e rack, o ostruirle per evitarne la completa chiusura. Il personale operante nel CED deve inoltre assicurarsi di non lasciare le chiavi incustodite o facilmente accessibili;

- è vietato duplicare le chiavi senza esserne autorizzati o consegnarle anche solo temporaneamente al personale non autorizzato;
- è vietato eseguire operazioni che possano arrecare danno, direttamente o indirettamente ai beni aziendali;
- è vietato, al di fuori di quanto regolarmente movimentato con le procedure aziendali di acquisto/manutenzione, introdurre in azienda strumenti, apparecchiature o altri oggetti se non preventivamente autorizzati;
- è vietato utilizzare per scopi diversi dall'attività lavorativa o con modalità diverse da quelle stabilite i beni aziendali in dotazione. E' altresì vietato aggirare, rendere inefficiente, eliminare, alterare, qualsiasi strumento di controllo (antincendio, antifurto, ecc.) senza giustificato motivo e senza specifica autorizzazione;
- è vietato spostare e/o disattivare apparecchiature/strumenti senza l'autorizzazione del personale responsabile;
- è vietato effettuare personalmente interventi di manutenzione sugli apparati (tali azioni devono essere eseguite solo dal personale specializzato preventivamente autorizzato).

9.3. Sensori

I CED devono essere provvisti di adeguati sistemi di rilevamento ambientali per tutti i sistemi di cui sopra. Tali sensori devono essere adeguatamente posizionati e mantenuti nel tempo. In particolare, si deve considerare l'installazione di:

- sensori per il monitoraggio della temperatura ambientale e dell'umidità della sala CED;
- sensori antiallagamento volti a individuare perdite d'acqua derivanti dall'esterno della sala CED (posizionati nei pressi o attorno e all'interno del pavimento rialzato della sala) e individuare perdite d'acqua dai sistemi di raffreddamento / condizionamento (posizionati ad esempio sotto ai condizionatori);

- eventuali sensori specifici per il monitoraggio dei rack contenenti gli apparati di elaborazione.

9.4. Ventilazione e condizionamento

Le condizioni ambientali all'interno dei CED devono essere monitorate e mantenute entro determinati limiti di temperatura e umidità, al fine di garantire un funzionamento ottimale degli apparati. In particolare, durante la progettazione del sistema di ventilazione e condizionamento e in seguito a cambiamenti rilevanti nell'architettura degli apparati, si deve:

- mantenere la temperatura ambientale ottimale (es. tra i 21 e i 24 °C);
- mantenere l'umidità relativa controllata (es. tra il 45% e il 50%);
- garantire la massima efficienza del sistema d'aerazione e nella distribuzione dei flussi d'aria fredda;
- garantire quanto più possibile la ridondanza degli impianti di
- condizionamento, evitando quindi i sistemi centralizzati (a singola unità) in favore di unità di condizionamento distribuite;
- garantire la pulizia dell'impianto al fine di evitare incidenti dovuti ad accumuli di polvere nell'impianto di ventilazione e nei dispositivi ospitati;
- evitare perdite d'aria nel pavimento;
- prevedere degli adeguati sistemi di raffreddamento per tutte le zone del CED particolarmente soggette a surriscaldamento;
- garantire l'efficienza degli impianti di condizionamento e ventilazione predisponendo controlli periodici e le relative procedure di manutenzione;
- monitorare, ove possibile costantemente gli impianti e, in caso di malfunzionamento e avarie, prevedere notifiche di allarme e relative procedure operative per ripristinarne il corretto funzionamento.

9.5. Energia Elettrica

Al fine di garantire l'alta affidabilità della connessione alle linee elettriche, il CED deve avere, ove possibile, due connessioni fisicamente separate a due distinte cabine del fornitore della rete elettrica. Ove ciò non fosse possibile per problemi di natura tecnologica o di fattibilità, la connessione alla cabina elettrica deve avvenire almeno tramite due distinti cavi. Tutti gli apparati contenuti nei CED devono essere collegati ad un gruppo di UPS opportunamente dimensionati in base al tipo di carico, al duplice fine di garantire una continua erogazione di corrente e consentire una protezione verso eventuali sbalzi e picchi.

di corrente. In particolare, durante la progettazione del sistema di UPS e in seguito a cambiamenti rilevanti nell'architettura degli apparati, si deve garantire l'efficienza degli UPS predisponendo dei test periodici di controllo e le relative procedure di manutenzione. I CED devono essere collegati ad un gruppo di continuità, ovverosia un generatore elettrico secondario attivabile in caso di mancanza di energia elettrica per un periodo di tempo prolungato. A seconda della criticità del CED e dei processi / servizi erogati, è possibile valutare la tipologia di generatore e il suo dimensionamento. In particolare, durante la progettazione del generatore secondario e in seguito a cambiamenti rilevanti nell'architettura degli apparti, si deve:

- assicurare che il gruppo di continuità entri in funzione in modo automatico a fronte di un tempo prestabilito di mancanza di energia elettrica. Tale tempo deve essere congruo con l'effettiva autonomia del gruppo UPS che fornisce la continuità al CED;
- definire una procedura di attivazione manuale del generatore nel caso in cui il sistema non entri in funzione autonomamente e addestrare il relativo personale preposto in caso di emergenza;
- predisporre una procedura per la gestione del rabbocco del carburante nel caso in cui la mancanza di energia elettrica superi il tempo di autonomia del generatore;
- garantire l'efficienza del generatore predisponendo dei test periodici di controllo e le relative procedure di manutenzione.

9.6. Rilevazione e soppressione incendi

Nei CED deve essere installato un completo sistema di rilevazione degli incendi che comprenda un sistema di rilevazione del calore e del fumo. Nell'installazione del sistema di rilevazione deve essere tenuto in considerazione quanto segue:

- deve essere installato sia del rilevatore di fumo che del calore;
- l'installazione deve essere certificata e in accordo alla normativa vigente;
- l'installazione deve coprire tutte le aree e le zone del CED;
- l'installazione deve avvenire considerando i sistemi di aerazione e ventilazioni specifici di ogni CED al fine di rilevare un principio di incendio o surriscaldamento.

Nei CED deve essere presente un impianto di soppressione degli incendi. Tale impianto deve considerare l'adozione di:

- porte taglia fuoco e pareti realizzate in materiale ignifugo;
- sistema di spegnimento automatizzato;
- utilizzo di agenti chimici o a clean agent come sistema di soppressione (ad esempio con scarica a gas chimica HFC-22);
- sistemi di soppressione delle fiamme manuali (estintori portatili posizionati all'interno del CED).

Gli impianti di rilevazione e soppressione incendi devono essere collegati al sistema di allarme e devono essere previste delle procedure operative per la gestione di tali eventi. E' inoltre necessario garantire l'efficacia dei presidi antincendio (es. rilevatori di fumo, impianti di spegnimento) predisponendo controlli periodici, le relative procedure di manutenzione anche operando verifiche specifiche in modo periodico e a fronte di cambiamenti significativi delle infrastrutture.

9.7. Smaltimento e riutilizzo delle apparecchiature

Per i dispositivi di memorizzazione che contengono o potrebbero potenzialmente contenere dati sensibili o critici per l'azienda si deve provvedere ad un'attività di distruzione fisica o di riscrittura "sicura" (si faccia anche riferimento a "3 Classificazione delle Informazioni" del presente documento).

Per prevenire l'utilizzo improprio di informazioni critiche memorizzate sulle apparecchiature sono dunque attivati i seguenti controlli:

- la rimozione delle apparecchiature (sia per dismissione che per sostituzione) e dei supporti informatici removibili deve essere documentata e autorizzata dal diretto responsabile dei beni;
- si deve provvedere all'eliminazione fisica dei dati memorizzati e del software installato (incluse le relative licenze) su tutte le unità di memorizzazione delle apparecchiature, prima del loro riutilizzo o dell'inoltro all'esterno dell'organizzazione per riparazione, sostituzione o smaltimento;
- prima del riutilizzo o smaltimento dei supporti informatici removibili come nastri, dischi e cassette si deve procedere alla cancellazione fisica delle informazioni critiche contenute dagli stessi tramite l'utilizzo di strumenti approvati da RSI;
- si deve procedere (ove necessario) alla distruzione fisica dei supporti di vario tipo contenenti informazioni critiche (ad es., stampe, carta carbone, nastri inchiostrati, listati, manuali ecc.) prima del loro smaltimento, in modo tale da rendere impossibile il recupero delle informazioni memorizzate.

9.8. Controlli di sicurezza sulle apparecchiature in ingresso e in uscita

Al fine di evitare perdite e danni derivanti dall'impropria movimentazione di apparecchiature e supporti di memorizzazione in ingresso e in uscita dall'organizzazione, si devono rispettare le seguenti regole:

- deve essere possibile tracciate le movimentazioni delle apparecchiature in ingresso e in uscita dai locali CED;
- devono essere previsti degli adeguati imballaggi e durante la movimentazione di supporti di memorizzazione che contengono dati informatici.

9.9. Clear desk policy

Al fine di evitare che i documenti e i supporti di memorizzazione removibili siano lasciati incustoditi o facilmente accessibili all'interno dei luoghi di lavoro relativi al perimetro del SSIV, è necessario il rispetto delle seguenti regole da parte di tutto il personale che opera all'interno del perimetro del SSIV:

- al termine di ogni giornata lavorativa, o in qualunque momento si lasci incustodita la propria postazione, è necessario lasciare la scrivania priva di documenti o supporti rimovibili, con particolare riguardo a quelli che contengono informazioni confidenziali e esclusive. In questo ultimo caso è necessario chiudere a chiave tali supporti in un armadio o in una cassettiera, o mettere in sicurezza le informazioni utilizzando altri strumenti;
- non lasciare mai i dispositivi mobili o i supporti removibili incustoditi sulla scrivania se questi contengono informazioni aziendali. Inoltre, i supporti removibili che contengono informazioni confidenziali e esclusive devono sempre essere cifrati;
- le stampe e i fax non devono rimanere incustoditi sulla stampante con particolare riferimento a quelli che contengono informazioni confidenziali e esclusive;
- i documenti che contengono informazioni confidenziali e esclusive devono essere smaltiti utilizzando un apposito 'trita documenti' (shredder);
- al termine di una riunione interna o con fornitori/clienti, bisogna assicurarsi che le informazioni eventualmente scritte sulla lavagna siano cancellate, e che le informazioni/note scritte sui flip chart (lavagne a fogli mobili) siano correttamente smaltite o archiviate.

9.10. Clear screen policy

Al fine di evitare che le infrastrutture informatiche (PC, laptop ecc.) siano lasciate accessibili quando non presidiate, VENIS ha definito le seguenti politiche implementate nell'ambito delle Postazioni di Lavoro. Le configurazioni delle Postazioni di Lavoro sono gestite tramite Group Policy del Domain Controller/Active Directory e prevedono:

- Stand-by a 30 minuti di inattività;
- Screen Saver a 10 minuti di inattività che dura 1 minuto per poi passare in black- screen per risparmiare energia elettrica.

Esistono delle eccezioni a tali policy che sono gestite sempre mediante l'associazione delle macchine in oggetto a particolari gruppi a cui sono associate specifiche regole. Tali eccezioni, valutate e approvate dal RSI, possono, a titolo di esempio esplicativo, riguardare:

- postazioni della portineria/guardiania – tali macchine non devono attivare lo screen saver e quindi visto che tale configurazione è legata alle utenze, queste ultime devono essere inserite nei gruppi corretti;
- macchine dedicate alla gestione dell'allarmistica – tali macchine devono poter operare autonomamente e quindi non devono andare in stand-by. Tale configurazione è legata alla macchina (e non all'utente) e quindi è la macchina a dover essere inserita nel gruppo corretto.

Inoltre è necessario il rispetto delle seguenti regole da parte di tutto il personale di VENIS:

- quando si lascia la postazione di lavoro incustodita, bisogna ancorarla tramite l'apposito cavo di sicurezza ed è necessario bloccare anche lo schermo nel modo seguente: premere contemporaneamente i tasti Ctrl_Alt_Canc e successivamente il tasto Enter (oppure il tasto Windows in combinazione al con il tasto 'L'). Verificare sempre che lo schermo sia bloccato prima di allontanarsi dalla postazione di lavoro;
- se ci si allontana dalla postazione di lavoro per l'intera giornata, è necessario portarsi dietro il proprio dispositivo portatile. Se questo non è possibile, bisogna assicurarsi che il PC sia chiuso a chiave in un armadio o in un posto sicuro.

Ulteriori indicazioni sono definite a livello aziendale nel "Disciplinare interno contenente le norme di comportamento per l'accesso e l'utilizzo dei sistemi e delle risorse informatiche, della navigazione internet, della gestione della posta elettronica, nonché della gestione dei documenti analogici di VENIS ("Disciplinare

comportamentale" - VSI- AT-POS-03) e nel capitolo relativo alla Classificazione delle informazioni del presente documento. A tal riguardo è necessario:

- regolamentare e controllare l'uso degli asset ICT in dotazione agli utenti (ad es. computer portatili, smartphone, cellulari, documenti, carta o altro) fuori dalle usuali sedi di lavoro;
- riutilizzare i supporti di memorizzazione contenenti informazioni sensibili solo dopo aver provveduto ad una cancellazione sicura delle stesse. In alternativa tali supporti devono essere fisicamente distrutti.

10. Sicurezza delle attività operative

Al fine di assicurare che le attività operative delle strutture di elaborazione delle informazioni (processi di IT Operations) garantiscano la correttezza e la sicurezza delle informazioni stesse, VENIS ha implementato i presidi di seguito descritti.

10.1. Procedure operative e responsabilità correlate

La Società ha formalizzato le linee guida e le regole per la corretta gestione delle attività di IT Operations. Tali policy e procedure hanno la finalità di supportare il personale interno e esterno coinvolto nella gestione operativa di tali processi, e in particolare di garantire il perseguimento degli obiettivi di sicurezza delle informazioni del SSVI.

10.2. Gestione dei cambiamenti

La società ha definito delle prassi di gestione dei cambiamenti a livello di organizzazione, processi di business e sistemi al fine di garantire la sicurezza delle informazioni. La politica di gestione dei cambiamenti definisce i princìpi, gli obiettivi e le modalità di tracciatura, valutazione, autorizzazione e implementazione di modifiche, sostituzioni o adeguamenti in ambito ai sistemi informatici con l'obiettivo, in particolare, di salvaguardare in qualunque momento la stabilità e l'integrità dell'ambiente di produzione. Obiettivo primario del presente documento è quindi la definizione del processo e delle relative procedure/metodi standard per il trattamento delle richieste di cambiamento che incidono sulle operazioni IT aziendali.

10.3. Gestione della Capacità

La gestione della capacità è il processo che consente di pianificare risorse ICT adeguate a soddisfare esigenze presenti e future ed include la pianificazione di un utilizzo efficiente delle risorse IT esistenti nonché la definizione di qualsiasi modifica nel tipo e nella quantità delle risorse ICT necessarie ad erogare i Servizi.

Al fine di minimizzare la perdita di dati ed informazioni dovuta a sospensioni dei sistemi IT, è necessario che le seguenti linee guida siano rispettate:

- L'utilizzo di risorse e di infrastrutture deve essere monitorato dalla funzione Sistemi IT e Sicurezza Informatica in maniera continuativa al fine di individuare eventuali aspetti di criticità. Tale processo può essere effettuato con il sussidio di uno strumento di monitoraggio.
- La funzione Sistemi IT e Sicurezza Informatica, a fronte delle informazioni raccolte dal monitoraggio, deve identificare potenziali colli di bottiglia e risorse chiave con mansioni critiche che possano presentare una minaccia alla sicurezza delle informazioni e definire un piano di azione al fine di prevenire tali scenari.
- La funzione Sistemi IT e Sicurezza Informatica deve effettuare mensilmente una pianificazione periodica al fine di gestire l'aprovvigionamento preventivo delle infrastrutture.
- L'introduzione di nuovi sistemi informativi deve essere opportunamente proceduta da un'analisi di accettazione degli stessi in termini di performance, capacità, livelli di servizio, aspetti di sicurezza.

Al fine di declinare gli aspetti di tale ambito ad un livello operativo, VENIS ha formalizzato il documento "Gestione della Capacità".

10.4. Separazione degli ambienti di sviluppo, test e produzione

La società, al fine di minimizzare i rischi correlati ad accessi non autorizzati o cambiamenti che inficino la sicurezza delle informazioni ha definito le seguenti prassi:

- Devono essere definiti dei livelli di separazione fra ambienti di sviluppo, test e produzione;
- I passaggi di ambiente devono essere controllati, sottoponendoli ad autorizzazione. La società definisce nelle apposite procedure e checklist il processo di autorizzazione ai passaggi di ambiente;
- La società definisce nell'apposita procedura il corretto governo degli ambienti di di sviluppo, test e produzione, dei dati contenuti e degli utenti

coinvolti nel processo.

- Al fine di declinare gli aspetti di tale ambito ad un livello operativo, VENIS ha

10.5. Protezione dai malware

Al fine di proteggere i sistemi informatici contenenti i dati e le informazioni all'interno del perimetro SSVI la società ha identificato i seguenti presidi di sicurezza:

- La società ha definito delle misure di protezione anti-malware per qualsiasi pc, server o altro asset che possa essere interessato da tale minaccia attraverso l'utilizzo di un antivirus. Tali soluzioni sono opportunamente e periodicamente aggiornate;
- La società ha adottato delle soluzioni di protezione a livello di navigazione web e posta elettronica al fine di garantire la sicurezza delle informazioni.
- La società al fine di presidiare le minacce derivanti da malware sia a livello client che server, ha predisposto la procedura dove sono indirizzati i temi concernenti le piattaforme antimalware, il monitoraggio e altre informazioni di carattere operativo.

10.6. Backup

La società ha definito delle prassi relative al backup al fine di assicurare che i dati aziendali siano protetti e possano essere ripristinati in seguito ad eventi quali: guasti hardware, distruzione intenzionale del dato o situazioni di disaster. In particolare, sono state definite le seguenti linee guida:

Devono essere effettuate copie di backup delle informazioni, del software e delle immagini dei sistemi e quindi sottoposte a test periodici secondo una politica di backup concordata.

Deve essere stabilita una politica di backup per definire i requisiti dell'organizzazione relativamente al backup delle informazioni, del software e dei sistemi.

La politica di backup deve definire i requisiti di conservazione e protezione.

Devono essere predisposte adeguate strutture dì backup per assìcurare che tutte le informazioni essenziali e il software possano essere recuperate in seguito a un disastro o ad un malfunzionamento dei supporli.

Nella progettazione di un piano di backup, VENIS ha tenuto in considerazione quanto segue:

- Devono essere prodotte registrazioni accurate e complete relative alle copie di backup nonché procedure documentate per il ripristino;
- L'estensione (per esempio backup completo o differenziale) e la frequenza dei backup devono riflettere i requisiti di business dell'organizzazione, i requisiti di sicurezza delle informazioni interessate e la crìticità delle informazioni per la continuità operativa dell'organizzazione;
- I backup devono essere archiviati in un sito remoto, ad una distanza sufficiente per evitare ogni danno in caso di disastro al sito principale;
- Alle informazioni di backup deve essere garantito un livello di sicurezza fisica e ambientale coerente con gli standard applicati nel sito principale;
- I supporti di backup devono essere sottoposti a test periodici per assicurare la loro affidabilità in caso dì emergenza quando necessario; questo dovrebbe essere associato alla verifica delle procedure di ripristino e confrontato con il tempo di ripristino richiesto. I test sul ripristino dei dati di backup dovrebbero avvenire su supporti dedicati, non sovrascrivendo i supporti originali, nel caso in cui i processi di backup o di ripristino falliscano e causino danni irreparabìli ai dati o una loro perdita:
- In situazioni in cui la riservatezza è importante, i backup devono essere protetti con mezzi crittografici.

L'esecuzione dei backup deve essere regolata da procedure operative di monitoraggio che indirizzino i malfunzionamenti nei backup programmati e assicurino la completezza dei backup stessi nel rispetto della politica di backup.

Soluzioni di backup predisposte per singoli sistemi e servizi devono essere sottoposte a test periodici per assicurare che soddisfino i requisiti dei piani di continuità operativa. Nel caso di sistemi e servizi critici, le soluzioni di backup

devono coprire tutte le informazioni dei sistemi stessi, le applicazioni e i dati necessari e ripristinare completamente il sistema in caso di disastro.

Il periodo di conservazione delle informazioni dì business essenziali deve essere definito, prendendo in considerazione i requisiti per la conservazione permanente dicopie di archivio. Al fine di presidiare quanto definito, VENIS ha introdotto la procedura di Gestione del Backup". Si rimanda quindi a tale documento per indicazioni di carattere operativo.

10.7. Monitoring e log management

Per VENIS l'informazione rappresenta un patrimonio la cui attenta gestione è strategica per la tutela e lo sviluppo del business aziendale. Al tal riguardo, VENIS si è dotata di una policy di Sicurezza delle Informazioni (Rif. VSI-SI-PS-01), enunciante i principi che si prefigge di osservare e far rispettare. In accordo a tale politica e in considerazione delle disposizioni normative vigenti applicabili, VENIS ha pertanto definito regole di sicurezza delle informazioni con l'obiettivo di fornire indicazioni in merito ai requisiti minimi di sicurezza ed alle necessarie misure di attuazione.

La società prevede l'adozione di misure di monitoraggio dell'utilizzo e della gestione dei sistemi, che devono essere realizzati secondo le seguenti regole:

- L'adozione di misure di monitoraggio deve essere effettuata nel rispetto delle normative applicabili, in particolare ai requisiti del GDPR;
- I tracciamenti devono essere adottati per rilevare elementi informativi in grado di aumentare il livello di protezione dei dati e delle informazioni;
- I log di sicurezza prodotti devono essere altresì protetti da accessi non autorizzati e /o da modifiche;
- Le misure di tracciamento devono almeno prevedere le seguenti informazioni: sistema, attività, autore dell'attività, timestamp;
- La corretta produzione dei log deve essere periodicamente verificata, al fine di accertarsi della completezza e della correttezza degli stessi;
- L'accesso ai suddetti log deve essere opportunamente regolamentata in termini di casistiche di verifica degli stessi, responsabilità, modalità di

accesso, etc. .

La società indirizza gli elementi operativi con riguardo alle attività di monitoring e log management relativamente agli apparati di rete ed alla infrastruttura nel documento "VSI- SSI-POS-14 - Gestione del Logging e del Monitoring".

10.8. Controllo dei software operativi

Al fine di assicurare l'integrità dei sistemi e garantire quindi la sicurezza delle informazioni, la società ha definito delle prassi circa i controlli sui software operativi. In particolare, sono implementate le seguenti procedure:

- L'aggiornamento dei software, applicativi e librerie è eseguito solamente da
- amministratori di sistema qualificati, previa autorizzazione del management;
- I sistemi operativi contengono solo codice eseguibile approvato e non codice di sviluppo;
- Gli applicativi ed i sistemi operativi sono implementati successivamente a test con esito positivo. Tali test riguardano l'usabilità, la sicurezza, gli effetti su altri sistemi e la facilità d'uso. Deve inoltre essere effettuata su sistemi separati.
- Precedentemente ad ogni implementazione su sistemi rilevanti viene stabilita una strategia di rollback.
- Deve essere utilizzato un sistema di controllo delle configurazioni durante l'implementazione di nuovi software.
- Deve essere tenuto un log di controllo di tutti gli aggiornamenti delle librerie dei programmi operativi.
- Le versioni precedenti del software applicativo devono essere mantenute come misura di emergenza.
- Le vecchie versioni del software devono essere archiviate, insieme a tutte le informazioni e parametri richiesti, procedure, dettagli di configurazione e software di supporto per tutto il tempo in cui i dati sono conservati in archivio.

10.9. Gestione delle vulnerabilità tecniche

Eventuali vulnerabilità tecniche dei sistemi devono essere opportunamente monitorate e gestite, mediante l'attuazione delle seguenti regole:

- Attribuire la specifica responsabilità di gestione e mantenimento dei sistemi in merito agli aspetti di vulnerabilità di sistema (patch management, hardening, ecc.);
- Monitorare le informazioni tecniche che periodicamente sono emesse dai soggetti preposti (vendor, centri istituzionali di sicurezza, ecc.);
- Garantire che le vulnerabilità tecniche rilevate siano analizzate e gestite, mediante opportune attività di patching, che prevedano una loro valutazione ed una successiva eventuale adozione.

10.10. Considerazioni sugli audit ai sistemi informativi

Al fine di minimizzare gli impatti delle attività di audit sui sistemi operativi aziendali, la società ha individuato le seguenti linee guida da rispettare:

- I requisiti di audit e le attività di verifica dei sistemi operativi devono essere attentamente monitorati, pianificati e concordati per ridurre al minimo le interruzioni dei processi aziendali.
- I test di audit devono essere limitati all'accesso in sola lettura al software e ai dati.
- L'accesso diverso da quello di sola lettura deve essere consentito solo per copie isolate di file di sistema, che devono essere cancellate al termine dell'audit, o protetto adeguatamente se esiste l'obbligo di tenere tali fascicoli sotto il controllo della documentazione richiesta.
- I test di audit che potrebbero influire sulla disponibilità del sistema devono essere eseguiti al di fuori dell'orario di lavoro.
- Tutti gli accessi devono essere monitorati e registrati per produrre una traccia di riferimento e azioni correttive.

11. Sicurezza delle comunicazioni

11.1. Obiettivi di Sicurezza delle Reti

L'obiettivo di VENIS, relativamente alla sicurezza dei servizi di rete, è quello di garantire la riservatezza, l'integrità e la disponibilità delle informazioni trasmesse da e verso i sistemi e i Servizi ICT da questa erogati. A tal fine VENIS, ove opportuno e applicabile:

- Assicura che la trasmissione informatica delle informazioni scambiate nell'ambito dei Servizi ICT avvenga mediante canali di comunicazione sicuri, proteggendo la riservatezza delle informazioni condivise e garantendo l'autenticità dell'identità del mittente e del destinatario delle comunicazioni elettroniche tramite la definizione di responsabilità e procedure per la gestione delle apparecchiature di rete.
- Protegge dalle minace esterne, mediante opportuni strumenti tecnologici, l'utilizzo della rete Internet, dalla Posta Elettronica e dai diversi servizi che esse possono offrire.
- Garantisce la separazione della responsabilità operativa delle reti dalle operazioni informatiche;
- Sono istituiti controlli per salvaguardare la riservatezza e l'integrità dei dati che transitano su reti pubbliche o su reti wireless al fine di proteggere i sistemi e le applicazioni connesse; Altri controlli speciali possono essere implementati al fine di mantenere la disponibilità dei servizi di rete. In particolare VENIS ha stabilito dei Service Level Agreements (SLA) con i propri Internet Service Provider (ISP) al fine di garantire la continuità di erogazione dei servizi. VENIS regolarmente effettua dei monitoraggi al fine di verificare che tali SLA siano rispettati.
- Garantisce adeguati processi di logging e monitoraggio al fine di consentire la registrazione e il rilevamento delle azioni che possono influire sulla sicurezza dell'informazione o che sono rilevanti per la sicurezza dell'informazione;
- Garantisce l'ottimizzazione del servizio offerto e contemporaneamente che i controlli siano applicati in modo coerente sull' infrastruttura di elaborazione delle informazioni;

- Garantisce un sistema di autenticazione agli apparati di rete;
- Garantisce una connessione limitata agli apparati di rete.

11.2. Segregazione delle Reti

VENIS ha adottato un sistema di divisione delle reti in domini separati al fine di garantirne la sicurezza e rispettare i criteri di riservatezza, integrità e disponibilità delle informazioni trasmesse. Il perimetro di ogni dominio è ben definito, inoltre l'accesso tra domini di rete è consentito, ma controllato al perimetro utilizzando un gateway.

I criteri per la segregazione delle reti in domini e l'accesso consentito attraverso i gateway si basano su una valutazione dei requisiti di sicurezza di ciascun dominio. La valutazione è effettuata in modo conforme alla politica di controllo dell'accesso, ai requisiti di accesso, al valore e alla classificazione delle informazioni trattate e tenendo conto anche del costo relativo e dell'impatto sulle prestazioni dell'incorporazione di una tecnologia di gateway adeguata.

11.3. Trasferimento delle Informazioni

VENIS ha definito delle linee guida al fine di garantire, relativamente alla sicurezza dei servizi di rete, la riservatezza, l'integrità e la disponibilità delle informazioni trasmesse attraverso l'uso di tutti i tipi di strumenti di comunicazione. Tali linee guida nell'utilizzo di strutture di comunicazione per il trasferimento di informazioni, presidiano i seguenti elementi:

- Protezione di informazioni trasferite da intercettazione, copia, modifica, mis-routing e distruzione;
- Individuazione e protezione contro malware che possono essere trasmessi attraverso l'uso delle comunicazioni elettroniche;
- Protezione di informazioni elettroniche sensibili scambiate tramite posta elettronica comunicate sotto forma di allegato;
- Definizione di linee guida per l'uso accettabile dei mezzi di comunicazione;
- Responsabilizzazione del personale al fine di prendere le precauzioni appropriate per non rivelare informazioni riservate;

- Adozione di tecniche crittografiche, al fine di proteggere la riservatezza, l'integrità e l'autenticità delle informazioni A tal proposito si veda quanto dettagliato al capitolo 8 di tale documento;
- Conservazione ed eliminazione di tutta la corrispondenza commerciale, compresi i messaggi, in conformità con con la legislazione e i regolamenti nazionali e locali in materia;
- Controlli e restrizioni associate all'uso dei mezzi di comunicazione, ad esempio l'inoltro automatico di posta elettronica agli indirizzi di posta esterna;
- Non lasciare messaggi contenenti informazioni riservate sulle segreterie telefoniche, in quanto possono essere riprodotti da persone non autorizzate, memorizzati su sistemi condivisi o memorizzati in modo errato a causa di un'errata digitazione;
- Consigliare il personale sui eventuali problemi legati all'uso di fax o servizi che possano compromettere la sicurezza delle informazioni.

VENIS ha adottato dei requisiti circa gli accordi di riservatezza e non divulgazione che riflettono le esigenze dell'organizzazione in materia di protezione delle informazioni. Tali requisiti sono identificati, documentati e rivisti regolarmente. Gli accordi di riservatezza o di non divulgazione riguardano l'obbligo di proteggere le informazioni riservate utilizzando termini legalmente applicabili. Gli accordi di riservatezza o di non divulgazione sono applicabili a parti esterne o ai dipendenti dell'organizzazione. Gli elementi vengono selezionati o aggiunti in considerazione del tipo di controparte e dell'accesso o del trattamento delle informazioni riservate. Per identificare i requisiti per gli accordi di riservatezza o di non divulgazione, vengono presi in considerazione i seguenti elementi:

- Definizione delle informazioni da proteggere;
- Durata prevista di un accordo, compresi i casi in cui potrebbe essere necessario mantenere la riservatezza a tempo indeterminato;
- Azioni necessarie in caso di risoluzione di un accordo;
- esponsabilità e azioni dei firmatari per evitare la divulgazione non autorizzata delle informazioni;
- Proprietà delle informazioni, dei segreti commerciali e della proprietà

intellettuale e il modo in cui ciò si riferisce alla protezione delle informazioni riservate;

- Uso consentito delle informazioni riservate e il diritto del firmatario di utilizzare le informazioni;
- Diritto di controllare e monitorare le attività che comportano informazioni riservate;
- Processo di notifica e segnalazione di divulgazione non autorizzata o di fuga di informazioni riservate;
- Modalità di restituzione o distruzione delle informazioni al momento della cessazione dell'accordo;
- Azioni da intraprendere in caso di violazione dell'accordo;
- Gli accordi di riservatezza e di non divulgazione devono essere conformi a tutte le leggi e i regolamenti applicabili per la giurisdizione a cui si applicano;
- I requisiti per gli accordi di riservatezza e di non divulgazione dovrebbero essere rivisti periodicamente e quando si verificano cambiamenti che influenzano tali requisiti.

12. Acquisizione, sviluppo e manutenzione dei sistemi informativi

12.1. Premessa

L'obiettivo del SSIV adottato da VENIS, relativamente a tale area, è quello di garantire che tutti gli aspetti di sicurezza e di protezione delle informazioni siano presi in considerazione in tutte le fasi di vita dei sistemi informativi quali la progettazione, lo sviluppo, l'esercizio, la manutenzione (ordinaria e straordinaria) nonché la dismissione. Tale protezione è effettuata attraverso l'adozione da parte di VENIS di misure tecniche, organizzative e procedurali relative alle seguenti specifiche tematiche.

12.2. Requisiti di Sicurezza per i Sistemi Informatici e Sicurezza nelle Applicazioni

12.2.1. Analisi e specifica dei requisiti per la sicurezza delle informazioni

I requisiti di sicurezza delle informazioni sono identificati utilizzando vari metodi, quali la definizione di requisiti di conformità in base a politiche e regolamenti, la modellizzazione delle minacce, l'esame degli incidenti o l'uso di soglie di vulnerabilità. I risultati dell'identificazione devono essere documentati ed esaminati da tutte le parti interessate. I requisiti e i controlli in materia di sicurezza delle informazioni devono riflettere il valore commerciale delle informazioni in questione e il potenziale impatto negativo che potrebbe derivare dalla mancanza di un'adeguata sicurezza. L'individuazione e la gestione dei requisiti di sicurezza delle informazioni e dei processi associati devono essere integrati nelle prime fasi dei progetti relativi ai sistemi informativi. Di seguito sono riportati i principali principi da seguire per la gestione dei requisiti di sicurezza:

- Devono essere individuate le fonti per l'identificazione dei requisiti di sicurezza, come ad esempio standard internazionali, best practices, leggi o normative di altro genere.

- Devono essere identificati i ruoli chiave di sicurezza IT per il progetto di sviluppo/acquisizione del nuovo sistema. La pianificazione delle attività di sicurezza deve essere integrata già nella fase iniziale del progetto.

- Devono essere identificate le tipologie di dati e di informazioni che sono trattati classificandone la criticità in ottica aziendale, individuando i vincoli di sicurezza derivanti da tale classificazione e selezionando i relativi controlli.

- Devono essere analizzati e integrati i requisiti esistenti per individuare eventuali conseguenze dal punto di vista della sicurezza (es. in termini di riservatezza, integrità e disponibilità del servizio erogato nonché dei servizi ad esso collegati).

- Le iniziative progettuali IT devono essere sottoposte a un'analisi della criticità e dei rischi atta ad identificare e definire l'adeguato livello di sicurezza e i relativi controlli da implementare.

- Deve essere effettuata una classificazione del sistema in cui si devono considerare tutti gli aspetti di sicurezza in termini di riservatezza, integrità e disponibilità.

- All'interno della fase di definizione delle specifiche, devono essere verificati/definiti gli eventuali controlli di sicurezza da effettuarsi.

- Al fine di garantire la conformità alle normative sulla protezione dei dati personali deve essere valutato e identificato se il sistema tratterà tali dati e in che cosa consiste la finalità e la modalità del trattamento. Inoltre devono essere identificati i rischi privacy e adottate in fase di design (privacy-by- design) le idonee misure di sicurezza. La sicurezza dei dati personali deve essere assicurata end-to-end; in particolare, per i dati personali deve essere garantito che i dati non siano leggibili e modificabili da soggetti non autorizzati.

12.2.2. Sicurezza dei Servizi Applicativi su Reti Pubbliche

Le informazioni coinvolte nei servizi applicativi che transitano su reti pubbliche devono essere protette da attività fraudolente, da dispute contrattuali, da divulgazioni e da modifiche non autorizzate. In particolare, le considerazioni relative alla sicurezza delle informazioni per i servizi applicativi forniti attraverso reti pubbliche devono includere i seguenti punti:

- Il livello di fiducia richiesto da ogni parte in ogni dichiarazione di identità (ad esempio atttraverso autenticazione);
- I processi di autorizzazione relativi a chi può approvare contenuti, a chi emana o firma transazioni chiave;
- Assicurarsi che i partner con cui si comunica siano completamente informati delle loro autorizzazioni per la fornitura o per l'utilizzo del servizio;
- Definire e soddisfare i requisiti di riservatezza, integrità, prova di inoltro e di ricezione dei documenti chiave ed il non ripudio dei contratti;
- Il livello di fiducia richiesto per l'integrità dei documenti chiave;
- I requisiti di protezione di ogni informazione riservata;
- La riservatezza e l'integrità di ogni ordine di transazione, delle informazioni di pagamento, dei dettagli sull'indirizzo di consegna e delle conferme di ricezione;
- Il livello di verifica appropriato per verificare le informazioni di pagamento fornite da un cliente;
- Scegliere la più approppriata modalità di pagamento per premunirsi contro le frodi;
- Il livello di protezione richiesto per mantenere la riservatezza e l'integrità delle informazioni sugli ordini;
- Evitare la perdita o la duplicazione delle informazioni delle transazioni;

- La responsabilità associata ad ogni transazione fraudolenta;
- I requisiti assicurativi.

12.2.3. Protezione delle transazioni dei servizi applicativi

Le informazioni coinvolte nelle transazioni dei servizi applicativi dovrebbero essere protette al fine di prevenire trasmissioni incomplete, errori di instradamento, alterazione non autorizzata di messaggi, divulgazione non autorizzata, duplicazione non autorizzata di messaggi o attacchi di tipo "replay".

Le considerazioni relative alla sicurezza delle informazioni legate alle transazioni dei servizi applicativi dovrebbero includere i seguenti punti:

- L'utilizzo di firme elettroniche per ognuna delle parti incluse nella transazione;
- Tutti gli aspetti della transazione, per esempio assicurare che:
- le informazioni segrete di autenticazione degli utenti di tutte le parti siano valide e verificate;
- la transazione resti riservata;
- sia mantenuta la privacy associata a tutte le parti coinvolte;
- I percorsi di comunicazione tra tutte le parti coinvolte siano crittografati;
- I protocolli utilizzati per comunicare tra tutte le parti coinvolte siano messi in sicurezza;
- Assicurare che la memorizzazione dei dettagli della transazione sia effettuata al di fuori di ogni ambiente pubblicamente accessibile, per esempio su una piattaforma di archiviazione esistente sulla intranet dell'organizzazione, e non conservata ed esposta su supporti di archiviazione direttamente accessibili da Internet;
-

- Quando viene utilizzata un'autorità di fiducia (per esempio preposta ad emettere e mantenere firme digitali o certificati digitali), la sicurezza è integrata e incorporata all'intero processo end-to-end di gestione della certificazione/firma.

12.3. Sicurezza nei processi di sviluppo e supporto

L'obiettivo di VENIS in tale ambito consiste nell'assicurare che la sicurezza delle informazioni sia progettata ed attuata all'interno del ciclo di sviluppo dei sistemi informativi.

12.3.1. Politica per lo sviluppo sicuro

Al fine di garantire che tutti gli aspetti di sicurezza siano considerati nei processi di progettazione e sviluppo dei sistemi informatici è necessario rispettare le seguenti indicazioni:

- La sicurezza dell'ambiente di sviluppo;
- I requisiti dì sicurezza nella fase di progettazione;
- I punti di controllo di sicurezza nelle milestone di progetto.

12.3.2. Procedure per il controllo dei cambiamenti di sistema

I cambiamenti ai sistemi all'interno del ciclo di vita devono essere tenuti sotto controllo attraverso l'utilizzo di procedure formali di controllo dei cambiamenti.

Devono essere documentate e fatte rispettare delle formali procedure di controllo dei cambiamenti al fine di garantire l'integrità dei sistemi dalle fasi iniziali di progettazione fino a tutte le successive attività di manutenzione. L'introduzione di nuovi sistemi ed i cambiamenti maggiori sui sistemi esistenti devono seguire un processo formale di documentazione, raccolta e validazione delle specifiche, test, e implementazione gestita. Questo processo deve comprendere la valutazione del rischio, l'analisi degli impatti dei cambiamenti e la specifica dei controlli di sicurezza necessari. Questo processo deve anche assicurare che non siano compromesse le esistenti procedure di sicurezza e di

controllo e che sia ottenuto un accordo e un'approvazione formali per ogni cambiamento. Le procedure per il controllo dei cambiamenti devono includere i seguenti requisiti minimi:

- Mantenere una registrazione dei livelli di autorizzazione concordati;
- Garantire che i cambiamenti siano inviati dagli utenti autorizzati;
- Riesaminare i controlli e le procedure per l'integrità per assicurare che non saranno compromesse dai cambiamenti
- Ottenere l'approvazione formale per le proposte dettagliate di cambiamento prima di iniziare il lavoro;
- Garantire che gli utenti autorizzati accettino i cambiamenti prima dell'implementazione;
- Garantire che l'insieme della documentazione di sistema definita sia aggiornata a seguito del completamento di ogni cambiamento e che la vecchia documentazione sia archiviata o dismessa;
- Mantenere il controllo di versione per tutti gli aggiornamenti del software;
- Mantenere un audit trail per tutte le richieste di cambiamento;
- Assicurare che la documentazione operativa (vedere punto 12.1.1) e le procedure utente siano modìficate in modo appropriato affinché rimangano adeguate;
- Assicurare che l'implementazione dei cambiamenti sia effettuata al momento giusto e non disturbi i processi di business coinvolti.

12.3.3. Riesame tecnico delle applicazioni in seguito a cambiamenti nelle piattaforme operative

Quando avvengono dei cambiamenti nelle piattaforme operative, le applicazioni critiche per il business dovrebbero essere riesaminate e sottoposte a test per assicurare che non ci siano impatti negativi sulle attività operative dell'organizzazione o sulla sua sicurezza.

Tale processo dovrebbe comprendere:

- Il riesame dei controlli applicativi e delle procedure a garanzia dell'integrità, per assicurare che non siano stati compromessi dai cambiamenti nelle piattaforme operative:
- Assicurare che le informazioni sui cambiamenti delle piattaforme di produzione siano fornite in tempi tali da permettere che i test e i riesami appropriati possano essere effettuati prima dell'implementazione;
- Assicurare che siano effettuati i cambiamenti appropriati al piano di continuità operativa.

12.3.4. Limitazioni ai cambiamenti dei pacchetti software

La modifica dei pacchetti software deve essere disincentivata e limitata ai cambiamenti necessari; inoltre, tutti i cambiamenti devono essere strettamente controllati. Per quanto possibile e praticabile, i pacchetti software forniti dal produttore dovrebbero essere utilizzati senza modifiche.

12.3.5. Principi per l'ingegnerizzazione sicura dei sistemi

VENIS definisce nel presente capitolo le principali linee guida per l'ingegnerizzazione di sistemi sicuri; tali principi si applicano, previa la loro declinazione allo specifico contesto progettuale e normativo, alla progettazione e all'implementazione dei servizi e dei sistemi ICT.

La sicurezza deve essere progettata in tutti i livelli dell'architettura (funzionale, dati, applicazioni e tecnologia), bilanciando le necessità di sicurezza delle informazioni con le necessità di accessibilità. Le nuove tecnologie devono

essere analizzate per valutarne i rischi di sicurezza e la progettazione deve essere riesaminata in relazione agli attacchi conosciuti.

Questi principi, insieme alle procedure di progettazione definite, devono essere regolarmente riesaminati per assicurare che contribuiscano efficacemente all'attuazione degli standard di sicurezza all'interno dei processi di ingegnerizzazione. Essi devono essere riesaminati periodicamente per assicurare che rimangano aggiornati al fine di contrastare ogni nuova potenziale minaccia e restino applicabili alla luce dell'innovazione delle tecnologie e delle soluzioni che vengono applicate.

I principi di ingegneria di sicurezza definiti devono essere applicati, quando possibile, ai sistemi informativi affidati all'esterno mediante contratti e altri accordi tra l'organizzazione e i fornitori ingaggiati. L'organizzazione deve confermare che il rigore dei principi di ingegneria di sicurezza applicati dai fornitori esterni sia paragonabile con quello da essa applicato.

12.3.6. Ambiente di sviluppo sicuro

VENIS definisce ed identifica delle linee guida al fine di garantire la protezione appropriata anche agli ambienti inferiori a quelli di produzione, utilizzati per l'erogazione dei Servizi ICT. Un ambiente di sviluppo sicuro include personale, processi e tecnologie relative allo sviluppo, e all'integrazione dei sistemi. VENIS è tenuta a valutare i rischi associati alle singole iniziative di sviluppo dei sistemi e definire ambienti di sviluppo sicuro per particolari iniziative di sviluppo dei sistemi, considerando:

- La criticità dei dati da elaborare, archiviare e trasmettere dal sistema;
- I requisiti interni ed esterni applicabili, per esempio derivanti da regolamenti o politiche;
- I controlli di sicurezza già attuati dall'organizzazione che supportano lo sviluppo del sistema;
- L'affidabilità del personale che lavora nell'ambiente;
- Il grado di esternalizzazione dello sviluppo del sistema;

- Le necessità di separazione tra diversi ambienti di sviluppo;
- Il controllo degli accessi all'ambiente dì sviluppo;
- Il monitoraggio dei cambiamenti all'ambiente e al codice in esso archiviato;
- L'archiviazione dei backup in luoghi remoti sicuri;
- Il controllo sulla movimentazione dei dati da e verso l'ambiente.

Una volta determinato il livello di protezione per un particolare ambiente di sviluppo, le organizzazioni devono documentare i corrispondenti processi in procedure di sviluppo sicuro e fornirli a tutti coloro che ne hanno necessità.

- Accordi per le licenze, diritti di proprietà del codice e di proprietà intellettuale relativi ai contenuti affidati all'esterno;
- Requisiti contrattuali per la progettazione, la programmazione e le prassi di test sicure;
- Consegna del modello delle minacce approvato agli sviluppatori esterni;
- Test di accettazione di qualità ed accuratezza dei prodotti consegnati;
- Fornitura dell'evidenza che sono state utilizzate delle soglie di sicurezza per stabilire il livello minimo accettabile di qualità per sicurezza e privacy;
- Messa a disposizione dell'evidenza che sono stati effettuati un numero sufficiente di test per tutelarsi sull'assenza di contenuti malevoli sia intenzionali che non intenzionali nei prodotti consegnati;
- Messa a disposizione dell'evidenza che sono stati applicati un numero sufficiente di test per premunirsi contro le vulnerabilità conosciute;
- Diritto contrattuale di effettuare audit sui processi e sui controlli di sviluppo;
- Efficace documentazione dell'ambiente di sviluppo utilizzato per realizzare prodotti da rilasciare;

VENIS deve restare responsabile della conformità alle norme applicabili e della verifica dell'efficienza dei controlli.

12.3.7. Sviluppo affidato all'esterno

VENIS è tenuta a supervisionare e monitorare l'attività di sviluppo dei sistemi affidata a società terze in outsourcing. Al fine di garantire e preservare la sicurezza delle informazioni, i seguenti punti devono essere considerati nell'intera filiera di approvvigionamento dell'organizzazione:

- Accordi per le licenze, diritti di proprietà del codice e di proprietà intellettuale relativi ai contenuti affidati all'esterno;
- Requisiti contrattuali per la progettazione, la programmazione e le prassi di test sicure;
- Consegna del modello delle minacce approvato agli sviluppatori esterni;
- Test di accettazione di qualità ed accuratezza dei prodotti consegnati;
- Fornitura dell'evidenza che sono state utilizzate delle soglie di sicurezza per stabilire il livello minimo accettabile di qualità per sicurezza e privacy;
- Messa a disposizione dell'evidenza che sono stati effettuati un numero sufficiente di test per tutelarsi sull'assenza di contenuti malevoli sia intenzionali che non intenzionali nei prodotti consegnati;
- Messa a disposizione dell'evidenza che sono stati applicati un numero sufficiente di test per premunirsi contro le vulnerabilità conosciute;
- Diritto contrattuale di effettuare audit sui processi e sui controlli di sviluppo;
- Efficace documentazione dell'ambiente di sviluppo utilizzato per realizzare prodotti da rilasciare;
- VENIS deve restare responsabile della conformità alle norme applicabili e della verifica dell'efficienza dei controlli.

La definizione delle linee guida di sicurezza nei confronti dei fornitori sono definite in modo maggiormente specifico nella procedura Gestione delle relazioni con i fornitori ICT".

12.3.8. Test di sicurezza dei sistemi

La società ha stabilito che i test relativi alle funzionalità di sicurezza devono essere effettuati durante lo sviluppo. I nuovi sistemi e quelli aggiornati richiedono accurati test e verifiche durante il processo di sviluppo, inclusa la predisposizione di una pianificazione di dettaglio delle attività, degli input per i test e dei risultati attesi rispetto a un insieme di condizioni. Come per gli sviluppi effettuati all'interno dell'organizzazione, tali test devono essere effettuati inizialmente dal gruppo di sviluppo e poi devono essere effettuati test di accettazione indipendenti (sia per gli sviluppi effettuati internamente sia per quelli affidati all'esterno) per garantire che i sistemi funzionino come previsto e solo come previsto. L'estensione dei test deve essere proporzionale all'importanza e alla natura dei sistemi.

12.3.9. Test di accettazione dei sistemi

VENIS stabilisce dei programmi di test e di accettazione ed i criteri ad essi relativi per i nuovi sistemi informativi, per gli aggiornamenti e per le nuove versioni. Tali test di accettazione dei sistemi devono comprendere il test dei requisiti relativi alla sicurezza delle informazioni e l'aderenza alle prassi di sviluppo sicuro dei sistemi. I test devono essere anche effettuati sui componenti ricevuti e sui sistemi integrati. Le organizzazioni possono utilizzare strumenti automatici, come prodotti per l'analisi del codice o strumenti per la scoperta delle vulnerabilità, e devono verificare le azioni per la correzione dei problemi relativi alla sicurezza. I test devono essere eseguiti in un ambiente di test realistico per assicurare che il sistema non introdurrà vulnerabilità nell'ambiente dell'organizzazione e che i test siano affidabili.

12.4. Dati di test

In tale ambito VENIS definisce delle linee guida al fine di assicurare la protezione dei dati usati per il test.

12.4.1. Protezione dei dati di test

I dati di test devono essere necessariamente scelti con attenzione, protetti e tenuti sotto controllo. Deve essere evitato l'utilizzo dei dati di produzione, contenenti informazioni personali o ogni altra informazione riservata, per condurre i test. Se i dati personali o ogni altra informazione riservata sono utilizzati per scopi di test, tutti i dettagli critici ed i contenuti.

Le seguenti linee guida devono essere applicate per proteggere i dati di produzione quando sono utilizzati a fini di test:

- Le procedure di controllo degli accessi che si applicano ai sistemi applicativi di produzione devono essere anche applicate ai sistemi applicativi di test;
- Devono esserci delle autorizzazioni separate ogni volta che le informazioni di produzione sono copiate su un ambiente di test;
- Le informazioni di produzione devono essere cancellate dall'ambiente di test immediatamente dopo il suo completamento;
- La copia e l'utilizzo delle informazioni operative deve essere tracciato per finalità di audit.

13. Relazione con i fornitori

L'obiettivo del SSIV adottato da VENIS, relativamente alla sicurezza delle informazioni nei rapporti con i fornitori, è quello di assicurare la protezione degli asset di VENIS accessibili da parte dei fornitori. A tal fine è necessario il rispetto delle seguenti regole:

- Le relazioni fra VENIS ed i fornitori ICT che gestiscono asset ICT e informazioni aziendali devono essere regolamentate da contratti che contengano anche elementi di sicurezza;
- La gestione da parte dei fornitori degli asset ICT di VENIS deve essere preventivamente valutata da un punto di vista dei rischi che potrebbero essere introdotti dall'attività; nello specifico, ogni qualvolta si ritenga necessario, devono essere valutati i rischi connessi a tale attività ed implementate eventuali misure preventive anche introducendo opportune clausole specifiche nei contratti di fornitura;
- Devono essere stipulati appositi contratti formali con tutti i fornitori ICT, tali da includere i livelli di servizio attesi nonché il monitoraggio continuo delle prestazioni degli impegni pattuiti;

I contratti stipulati con i fornitori ICT devono assicurare il diritto di VENIS di condurre regolari attività di verifica finalizzate a monitorare i livelli di qualità dei servizi attesi, nonché il rispetto dei requisiti identificati dalle normative interne aziendali; nello specifico ogni funzione di VENIS è responsabile del monitoraggio delle prestazioni dei fornitori ICT di propria competenza rispetto ai livelli di servizio attesi;

- L'accesso a reti o sistemi ICT da parte di fornitori ICT, ivi inclusi gli accordi di outsourcing, deve essere disciplinato da un apposito contratto scritto che includa opportuni presidi per garantire la riservatezza;
- La regolamentazione tra le parti e i requisiti di sicurezza presenti nei contratti deve poter essere estesa e garantita dal fornitore a tutti i suoi sub- fornitori;

- Qualora si verifichino variazioni delle norme interne aziendali relative ai servizi offerti dai fornitori ICT, queste devono essere necessariamente comunicate ai fornitori ICT e integrate in appositi contratti aggiornati. Deve essere prevista la possibilità di rivedere le condizioni e le clausole contrattuali di sicurezza al verificarsi di particolari eventi;

Ulteriori indicazioni sulla sicurezza delle informazioni all'interno delle relazioni con i fornitori sono dettagliate nel documento "VSI-SSI-POS-01 Gestione delle relazioni con i fornitori ICT".

14. Gestione degli incidenti di sicurezza delle informazioni

14.1. Premessa

L'obiettivo del SSIV adottato da VENIS, relativamente a tale ambito, è assicurare che le anomalie e gli incidenti aventi ripercussioni sui Servizi ICT e quindi sulle informazioni da questi trattate, siano tempestivamente riconosciuti e correttamente gestiti attraverso efficienti sistemi di prevenzione, comunicazione e reazione, al fine di minimizzare l'impatto sul business.

14.2. Gestione degli incidenti relativi alla sicurezza delle informazioni e dei miglioramenti

14.2.1. Responsabilità e procedure

VENIS stabilisce delle linee guida circa le responsabilità e le procedure per la gestione degli incidenti relativi alla sicurezza delle informazioni. Tali linee guida devono essere concordate con la direzione ed allineate con gli obiettivi per la gestione per la gestione degli incidenti. In particolare, VENIS al fine di presidiare tale controllo introduce la procedura "*VSI-SSI-POS-11- INCIDENT & PROBLEM MANAGEMENT*".

Tale procedura è stata sviluppata e comunicata in maniera adeguata all'interno dell'organizzazione ed include:

- La pianificazione e la preparazione della risposta agli incidenti;
- Il monitoraggio, per la rilevazione, per l'analisi e per la segregazione degli eventi e degli incidenti relativi alla sicurezza delle informazioni;
- La raccolta di log delle attività di gestione degli incidenti;
- Procedure per la valutazione e la presa di decisione sugli eventi relativi alla sicurezza delle informazioni e per la valutazione dei punti di debolezza della sicurezza delle informazioni;
- Procedure per la risposta, che includano quelle per l'escalation, il ripristino controllato dall'incidente e la comunicazione verso persone

od organizzazioni interne ed esterne;

Devono essere inoltre definiti dei ruoli e delle responsabilità al fine di assicurare che:

- Coloro che sono responsabili per la gestione degli incidenti relativi alla sicurezza delle informazioni comprendano le priorità dell'organizzazione per il trattamento degli incidenti relativi alla sicurezza delle informazioni;
- Le questioni collegate ad incidenti relativi alla sicurezza delle informazioni dell'organizzazione siano gestiti da personale competente;
- Sia attivato un punto di contatto per la rilevazione e la segnalazione degli incidenti relativi alla sicurezza delle informazioni;
- Siano mantenuti contatti appropriati con le autorità, con gruppi di interesse esterni o forum che gestiscono questioni collegate agli incidenti relativi alla sicurezza delle informazioni.

Le procedure di segnalazione devono includere:

- La preparazione dei modelli di documento per gli eventi relativi alla sicurezza delle informazioni per supportare l'attività di segnalazione e per aiutare il personale incaricato della segnalazione a ricordare tutte le azioni necessarie in caso di evento relativo alla sicurezza delle informazioni;
- La procedura da seguire in caso di evento relativo alla sicurezza delle informazioni, per esempio: annotare immediatamente tutti i dettagli come il tipo di non conformità o violazione, il malfunzionamento avvenuto, i messaggi sullo schermo e segnalare immediatamente al punto di contatto e intraprendere solo azioni coordinate;
- Il riferimento ad un processo disciplinare definito e formale per il personale che commette violazioni alla sicurezza;
- Adeguati processi di raccolta delle informazioni di ritorno per assicurare che il personale incaricato della segnalazione dell'evento relativo alla sicurezza delle informazioni riceva notifica dei risultati dopo che l'incidente è stato affrontato e chiuso.

15. Aspetti relativi alla sicurezza delle informazioni nella gestione della continuità operativa

15.1. Premessa

L'obiettivo del SSIV adottato da VENIS, relativamente a tale ambito, è quello di garantire la continuità operativa dei Servizi ICT erogati a fronte di eventi anomali di una certa gravità nonché il loro eventuale ripristino tempestivo, riducendo le conseguenze per il business.

- Gli elementi rilevanti ai fini della continuità operativa dei Servizi ICT devono essere opportunamente analizzati.
- È necessario che siano definite delle strategie di continuità, definite in un piano di continuità, nonché, ove opportuno, delle eventuali procedure operative correlate necessarie.
- È necessario che siano predisposti eventuali piani di ripristino delle componenti tecnologiche, incluse ove opportuno, eventuali procedure correlate.
- Il corretto funzionamento dei modelli e dei piani di continuità adottati devono essere periodicamente verificati e testati.

15.2. Continuità della sicurezza delle informazioni

VENIS deve determinare i propri requisiti per la sicurezza delle informazioni e per la continuità della gestione della sicurezza delle informazioni in situazioni avverse, per esempio durante crisi o disastri. In particolare, VENIS deve garantire che la continuità della sicurezza delle informazioni sia inserita all'interno del processo di gestione della continuità operativa oppure all'interno del processo di gestione del disaster recovery.

I requisiti per la sicurezza delle informazioni devono essere determinati durante la pianificazione per la continuità operativa ed il disaster recovery.

A tal fine, VENIS ha definito il proprio Disaster Recovery Plan allo scopo di gestire l'emergenza nel caso di indisponibilità dei sistemi informativi, rivolto sia

al personale operativo impegnato nelle procedure di ripristino dei sistemi, sia ai livelli direttivi, ovvero al responsabile del coordinamento delle attività sui sistemi e ai responsabili della gestione della crisi. Il Disaster Recovery Plan descrive i processi necessari per ripristinare le funzionalità del sistema informatico di VENIS, qualora eventi di natura disastrosa ne abbiano definitivamente compromesso la disponibilità. Il DRP è parte integrante delle procedure di continuità operative contenute nel Business Continuity Plan (BCP) di VENIS. Il Disaster Recovey Plan è collaudato attraverso dei test ripetuti con una frequenza almeno annuale e che coprono gli scenari e le modalità previste dalla da normativa.

15.2.1. Attuazione della continuità della sicurezza delle informazioni

VENIS deve stabilire, documentare, attuare e mantenere processi, procedure e controlli per assicurare il livello di continuità richiesto per la sicurezza delle informazioni durante una situazione avversa.

In particolare, VENIS deve assicurarsi che:

- Esista un'adeguata struttura gestionale per prepararsi, mitigare e rispondere ad eventi avversi, usando personale con la necessaria autorità, esperienza e competenza;
- Sia nominato del personale per la risposta agli incidenti con la necessaria responsabilità, autorità e competenza per gestire un incidente e mantenere la sicurezza delle informazioni;
- Siano sviluppati e approvati piani documentati, procedure di risposta e ripristino, dettagliando come l'organizzazione gestirà un evento avverso e come manterrà la sicurezza delle informazioni ad un predeterminato livello, sulla base di obiettivi approvati di gestione della continuità della sicurezza delle informazioni.

Secondo i requisiti di continuità della sicurezza delle informazioni, l'organizzazione deve stabilire, documentare, attuare e mantenere:

- Controlli per la sicurezza delle informazioni all'interno dei processi delle procedure e dei sistemi nonché degli strumenti a supporto della

continuità operativa o del disaster recovery;

- Processi, procedure e modifiche delle implementazioni per mantenere i controlli esistenti per la sicurezza delle informazioni durante una situazione avversa;
- Controlli compensativi per i controlli per la sicurezza delle informazioni che non possono essere mantenuti durante una situazione avversa.

15.3. Ridondanze

15.4. Verifica, riesame e valutazione della continuità della sicurezza delle Informazioni

L'obiettivo di VENIS in tale ambito risulta assicurare la disponibilità delle strutture per l'elaborazione delle informazioni, ovvero, le strutture per l'elaborazione delle informazioni devono essere realizzate con una ridondanza sufficiente a soddisfare i requisiti di disponibilità. VENIS deve identificare i requisiti di business per la disponibilità dei sistemi informativi. Quando la disponibilità non può essere garantita usando l'esistente architettura dì sistema, dovrebbero essere considerati componenti o architetture ridondanti.

Quando applicabile, i sistemi informativi ridondati devono essere sottoposti a test per assicurare che il passaggio in caso di malfunzionamento da un componente ad un altro funzioni come atteso.

16. Conformità

16.1. Premessa

L'obiettivo del SSIV adottato da VENIS, relativamente a tale ambito, è quello di garantire che, oltre a quanto imposto a livello di normativa, le attività correlate al SSIV e più in generale alle informazioni appartenenti all'ambito del SSIV devono essere effettuate nel rispetto della normativa predisposta nell'ambito di VENIS. Ovvero, evitare violazioni a obblighi cogenti o contrattuali relativi alla sicurezza delle informazioni e di qualsiasi requisito di sicurezza.

16.2. Conformità ai requisiti cogenti e contrattuali

16.2.1. Identificazione della legislazione applicabile e dei requisiti contrattuali

Per ogni sistema informativo e per l'organizzazione si devono esplicitamente definire, documentare e mantenere aggiornati tutti i requisiti cogenti e contrattuali pertinenti, oltre all'approccio stesso dell'organizzazione per soddisfarli. Analogamente, si devono definire e documentare i controlli specifici e le singole responsabilità per soddisfare tali requisiti.

I responsabili dell'organizzazione devono identificare tutta la legislazione applicabile alla loro organizzazione, al fine di soddisfare i requisiti relativi al loro tipo di business. Se l'organizzazione svolge la sua attività in altri Paesi, i responsabili devono considerare tale conformità per tutti i paesi interessati.

16.2.2. Diritti di proprietà intellettuale

Devono essere attuate delle procedure adeguate a garantire la conformità ai requisiti cogenti e contrattuali relativi a diritti di proprietà intellettuale e per l'uso di prodotti software proprietari.

Si devono prendere in considerazione le seguenti linee guida per proteggere il materiale che possa essere considerato proprietà intellettuale:

- Acquistare software solo da fonti conosciute e affidabili, per garantire che il diritto d'autore non sia violato;
- Mantenere la consapevolezza delle politiche per proteggere i diritti di proprietà intellettuale, e dare notifica dell'intento di prendere provvedimenti disciplinari nei confronti del personale che li infrange;
- Mantenere registri appropriati degli asset ed identificare tutti gli asset con requisiti di tutela dei diritti di proprietà intellettuale;
- Mantenere prove ed evidenze della titolarità delle licenze, dischi originati, manuali, ecc.;
- Attuare controlli per garantire che il numero massimo di utenti autorizzati dalle licenze non venga superato;
- Effettuare riesami del fatto che siano installati solo software autorizzati e con licenza;
- Fornire una politica per il mantenimento delle appropriate condizioni di licenza;
- Fornire una politica per lo smaltimento o il trasferimento di software a terzi;
- Conformarsi ai termini e alle condizioni relativi a informazioni e software ottenuti da reti pubbliche;
- Non duplicare, convertire in un altro formato o estrarre registrazioni commerciali (filmati, audio) al di fuori di quanto permesso dalla legge sul diritto d'autore;
- Non copiare in tutto o in parte libri, articoli, rapporti od altri documenti se non per quanto permesso dalle leggi sul diritto d'autore.
- I prodotti software proprietari sono solitamente forniti con un contratto di licenza d'uso che specifica i termini e le condizioni di licenza, per esempio, limitando l'uso del prodotto su macchine specifiche o limitando la duplicazione solo per la creazione di copie di backup. L'importanza e la consapevolezza dei diritti di proprietà intellettuale relativi al software sviluppato dall'organizzazione deve

essere comunicata al personale.

16.2.3. Protezione delle registrazioni

Le registrazioni devono essere protette da perdita, distruzione, falsificazione, accesso non autorizzato e rilascio non autorizzato in conformità da requisiti cogenti, contrattuali e di business.

La classificazione di specifiche informazioni aziendali documentate, adottata a partire dallo schema di classificazione dell'organizzazione, deve essere considerata quando si deve decidere sulla loro protezione. Le registrazioni dovrebbero essere suddivise in categorie secondo il tipo; ad esempio, scritture contabili, record di database, log delle transazioni, log di audit e procedure operative, ognuna di esse con dettagli sul periodo di conservazione e sul tipo di supporto di memorizzazione, per esempio carta, microfiche, supporto magnetico, supporto ottico. Eventuali chiavi crittografiche e programmi associati ad archivi crittografati o a firme digitali dovrebbero essere memorizzati per consentire la decodifica delle registrazioni per lo stesso tempo di conservazione delle registrazioni stesse.

Si deve prendere in considerazione la possibilità di deterioramento dei supporti utilizzati per la memorizzazione delle registrazioni. Si devono attuare delle procedure per il trattamento e la memorizzazione in conformità alle raccomandazioni del produttore.

Ove siano scelti supporti di conservazione elettronica, per proteggersi contro la perdita dovuta a futuri cambiamenti della tecnologia, devono essere stabilite delle procedure per assicurare la possibilità di accedere ai dati (sia per la leggibilità del supporto sia per quella del formato) per tutto il periodo di conservazione.

Il sistema di conservazione e trattamento deve assicurare una chiara identificazione delle registrazioni e del loro periodo di conservazione, come definiti dalla legislazione o dai regolamenti nazionali o locali, se applicabili. Tale sistema deve consentire un'appropriata distruzione delle registrazioni

dopo tale periodo se non sono più necessarie per l'organizzazione. Per realizzare questi obiettivi per la protezione delle registrazioni, si devono intraprendere i seguenti passi all'interno di un'organizzazione:

- Devono essere emesse delle linee guida su conservazione, memorizzazione, trattamento e smaltimento di registrazioni e informazioni;
- Deve essere redatto uno schema di conservazione che identifichi le registrazioni ed il periodo di tempo per il quale dovrebbero essere conservate;
- Deve essere mantenuto un inventario delle fonti di informazioni chiave.

16.2.4. Privacy e protezione dei dati personali

VENIS deve assicurare la privacy e la protezione dei dati personali, come richiesto dalla legislazione e dai regolamenti pertinenti, per quanto applicabile.

Si deve sviluppare ed attuare una politica sulla protezione dei dati personali e sulla privacy. Questa politica deve essere comunicata a tutto il personale coinvolto nel trattamento dei dati personali.

Il rispetto di tale politica, nonché di tutta la legislazione e dei regolamenti in materia di tutela della sfera privata delle persone e dei dati personali, richiede una struttura adeguata di gestione e controllo. Spesso lo si può conseguire al meglio con la nomina di un soggetto responsabile, come per esempio un responsabile per la privacy, che dovrebbe offrire una guida ai responsabili dell'organizzazione, agli utenti e ai fornitori di servizi sulle responsabilità individuali e sulle procedure specifiche che dovrebbero essere seguite. La responsabilità per il trattamento dei dati personali e per assicurare la consapevolezza dei principi relativi alla privacy deve essere allocata in conformità con le leggi ed i regolamenti pertinenti. Si devono attuare misure tecniche e organizzative appropriate per proteggere i dati personali.

16.2.5. Regolamentazione sui controlli crittografici

I controlli crittografici devono essere utilizzati in conformità a tutti gli accordi, la legislazione e i regolamenti pertinenti. Per la conformità ad accordi, leggi e regolamenti pertinenti, si devono prendere in considerazione i seguenti elementi:

- Limitazioni a importazione o esportazione di hardware e software per svolgere funzioni crittografiche;
- Limitazioni su importazione o esportazione di hardware e software progettati con la possibilità di aggiungervi funzioni crittografiche;
- Limitazioni sull'uso della crittografia;
- Metodi di accesso obbligatori o discrezionali da parte delle autorità nazionali alle informazioni crittografate, da hardware o software, per tutelare la riservatezza dei contenuti.

16.3. Riesami della sicurezza delle informazioni

L'obiettivo di VENIS in tale ambito risulta di assicurare che la sicurezza delle informazioni sia attuata e gestita in conformità alle politiche e alle procedure dell'organizzazione.

16.3.1. Riesame indipendente della sicurezza delle informazioni

L'approccio di VENIS alla gestione della sicurezza delle informazioni e la sua attuazione (ossia gli obiettivi di controllo, i controlli, le politiche, i processi e le procedure per la sicurezza delle informazioni) devono essere riesaminati in modo indipendente ad intervalli pianificati oppure quando si verificano cambiamenti significativi.

I responsabili dell'organizzazione devono avviare un riesame indipendente, necessario per garantire la continua idoneità, adeguatezza ed efficacia dell'approccio dell'organizzazione alla gestione della sicurezza delle informazioni. Il riesame deve comprendere la valutazione delle opportunità di

miglioramento e la necessità di modifiche all'approccio alla sicurezza, includendo politiche e obiettivi di controllo.

Tale riesame deve essere effettuato da soggetti indipendenti dall'area in esame, per esempio, la funzione di audit interno, un responsabile indipendente dell'organizzazione o un organismo esterno di terza parte specializzato in questi riesami. I soggetti che svolgono tali riesami devono avere competenze ed esperienza adeguate.

I risultati del riesame indipendente devono essere registrati e comunicati al responsabile che li ha avviati. Tali registrazioni devono essere conservate. Se il riesame indipendente identifica che l'approccio dell'organizzazione e l'attuazione della gestione della sicurezza delle informazioni sono inadeguati, per esempio se obiettivi documentati e requisiti non sono soddisfatti o non conformi con gli indirizzi per la sicurezza delle informazioni indicati nel documento di politica di sicurezza delle informazioni, i responsabili devono prendere inconsiderazione delle azioni correttive.

16.3.2. Conformità alle politiche e alle norme per la sicurezza

I responsabili dell'organizzazione devono riesaminare regolarmente la conformità dei processi di elaborazione delle informazioni a delle procedure che rientrano nella loro area di responsabilità rispetto alle politiche, alle norme e a ogni altro requisito appropriato per la sicurezza.

I responsabili dell'organizzazione devono identificare come riesaminare la soddisfazione dei requisiti di sicurezza delle informazioni definiti nelle politiche, nelle norme e negli altri regolamenti applicabili. Misurazioni e strumenti di reporting automatici dovrebbero essere presi in considerazione per un efficiente riesame periodico.

Nel caso in cui si riscontrino non conformità come risultato del riesame, i responsabili devono:

- Determinare le cause della non conformità;
- Valutare la necessità di azioni volte a garantire la conformità;

- Attuare le misure correttive appropriate;
- Riesaminare le azioni correttive adottate per verificarne l'efficacia e individuare le eventuali carenze o debolezze.

I risultati dei riesami e delle azioni correttive effettuate dai responsabili devono essere registrati e tali registrazioni devono essere conservate. I responsabili devono riportare i risultati al personale che svolge i riesami indipendenti quando un riesame indipendente viene svolto nell'area di loro competenza.

16.3.3. Verifica tecnica della conformità

I sistemi informativi devono essere regolarmente riesaminati per conformità con le politiche e con gli standard di sicurezza dell'organizzazione.

La verifica tecnica della conformità deve essere eseguita preferibilmente con l'ausilio di strumenti automatizzati, che generano relazioni tecniche per una successiva interpretazione da parte di un tecnico specializzato. In alternativa, può essere eseguito un controllo manuale (supportato da adeguati strumenti software, se necessario) da un tecnico di sistema di esperienza.

Nel caso in cui vengano eseguiti penetration test e vulnerability assessment, si deve prestare attenzione in quanto tali attività potrebbero avere conseguenze sulla sicurezza del sistema. Tali attività devono essere pianificate, documentate e ripetibili.

Ogni verifica tecnica della conformità deve essere effettuata solo da persone competenti e autorizzate oppure sotto la toro supervisione.