Cerved Group S.p.A.

Policy

di Sicurezza Informatica

Approvata in data 1° luglio 2022

Revisione 005

Indice

1 Scopo e campo di applicazione

1.1 SCOPO

L'obiettivo di questo documento è definire le politiche di sicurezza informatica di Cerved Group (di seguito il Gruppo), in termini di principi, linee guida e regole da applicare per la definizione, gestione e governo della sicurezza dei sistemi informativi.
In particolare, questo documento rappresenta lo strumento preferenziale al fine di sensibilizzare i dipendenti e i collaboratori dell'azienda in merito alle norme che devono essere rispettate nella gestione del patrimonio informativo aziendale, con l'obiettivo di garantire la sicurezza del sistema informatico e la tutela dell'immagine di tutte le società del Gruppo.

1.2 CAMPO DI APPLICAZIONE

Le politiche di sicurezza definite nel presente documento devono essere applicate per l'intero insieme di strutture organizzative e tecnologiche che costituiscono i sistemi informativi di tutte le società del Gruppo.
L'infrastruttura che l'azienda fornisce per i propri servizi sia interni (dipendenti, consulenti) che esterni (clienti, fornitori), è così strutturata:

- *Sistemi di applicazioni*: applicazioni e database che supportano i processi aziendali;
- *Sistemi di elaborazione ed archiviazione*: sistemi che forniscono servizi di elaborazione ed archiviazione delle informazioni, quali ad esempio mainframe, sistemi dipartimentali, file server, Storage Area Network, ecc.;
- *Sistemi di infrastruttura*: sistemi che forniscono servizi di rete (ad esempio controller di dominio, Proxy, Mail, DNS, Firewall, ecc.);
- *Sistemi di telecomunicazione*: dispositivi che forniscono servizi di telecomunicazione, come ad esempio router e switch, nonché apparecchiature di telefonia collegate alla rete dati aziendale (ad esempio, smartphone);
- *Workstation*: postazioni di lavoro fisse e mobili attraverso le quali gli utenti accedono alle risorse informative aziendali;
- *Servizi Cloud*: servizi progettati per fornire un accesso facile e conveniente ad applicazioni e risorse, senza la necessità di infrastrutture o hardware interni. Si specifica che anche le politiche di sicurezza per cui non compare un'esplicita sezione di riferimento al cloud vengono altresì applicate ai servizi Cloud.

1.3 DESTINATARI

Le politiche di sicurezza definite nel presente documento devono essere osservate da tutto il personale aziendale appartenente al Gruppo e dal personale di eventuali fornitori esterni che svolgono attività per conto del Gruppo.

2 Riferimenti

2.1 DOCUMENTAZIONE

Le politiche di sicurezza definite nel presente documento sono state strutturate sulla base dello standard internazionale ISO 27001.
Lo Standard UNI CEI ISO/IEC 27001:2013 (Tecnologia delle informazioni - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni - Requisiti) è una norma internazionale che definisce i requisiti per definire e gestire un Sistema di Gestione della Sicurezza delle Informazioni (SGSI o ISMS dall'inglese Information Security Management System) in merito ad aspetti di sicurezza logica, fisica ed organizzativa.
La Norma è stata creata e pubblicata nell'ottobre 2013 a fini certificativi, in modo da costituire un sistema completo per garantire la gestione della sicurezza nella tecnologia dell'informazione: con la sua pubblicazione ha sostituito la norma inglese BS 7799 che fino ad allora rappresentava la principale norma di riferimento per l'applicazione di un Sistema di Gestione per la sicurezza delle informazioni.
L'impostazione dello standard ISO/IEC 27001 è coerente con quella del Sistema di Gestione per la Qualità ISO 9001:2015 ed il Risk management, basandosi su un modello PDCA (plan-do-check-act).
L'obiettivo dello standard è quello di proteggere i dati e le informazioni dalle minacce, al fine di assicurarne l'integrità, la riservatezza e la disponibilità, e fornire i requisiti per adottare un adeguato sistema di gestione della sicurezza delle informazioni.
La norma ISO 27002:2013 è una raccolta di "best practices" che possono essere adottate per soddisfare i requisiti della norma ISO 27001:2013 al fine di proteggere le risorse informative.
Il presente documento è stato definito tenendo anche in considerazione:

- le specifiche e i requisiti definiti nel Regolamento UE 2016/679 – GDPR e successivi provvedimenti emanati dall'Autorità Garante per la protezione dei dati personali;
- le specifiche e i requisiti definiti nello Standard ISO / IEC 27017 chiarendo i ruoli e responsabilità per fornitori di servizi cloud e per i relativi clienti con l'obiettivo di garantire che i dati conservati in cloud siano sicuri e protetti;
- le specifiche e i requisiti definiti nello Standard ISO / IEC 27018 [*Codice di condotta per la protezione delle PII (Personally Identifiable information) nei servizi di public cloud per i cloud provider*] da intendersi come linea guida per i fornitori di servizi cloud pubblici sul miglioramento della gestione dei dati personali al fine di fornire una modalità strutturata, basata sul *privacy by design* dei dati personali in infrastrutture informatiche distribuite (cloud pubblico).

Si faccia riferimento al documento CG_D_0255 – "*Mappa normative applicabili alle società del Gruppo Cerved*" per quanto riguarda il quadro normativo applicato alle diverse società del Gruppo.
Lo standard ISO/IEC 27017:2015, rientrante tra gli standard ISO/IEC 27001, definisce controlli specifici per fornitori e i clienti dei servizi cloud con la finalità di delineare puntualmente i ruoli e responsabilità dei diversi attori coinvolti per garantire la sicurezza e la protezione dei dati personali conservati in cloud. Tale standard fornisce una guida per servizi cloud in aggiunta a quando disciplinato dalla norma ISO/IEC 27002 focalizzati sui nuovi ulteriori aspetti ossia:

- suddivisione delle responsabilità tra fornitore e clienti dei servizi cloud;
- monitoraggio delle attività del cliente all'interno dell'ambiente cloud;
- allineamento degli ambienti virtuale e cloud;
- attività amministrative e procedure connesse con l'ambiente cloud;
- protezione e separazione degli ambienti virtuali;
- configurazione Virtual Machine;

Lo standard ISO/IEC 27018:2020 definisce una serie di contromisure specifiche fondate sui principi internazionali privacy per la corretta progettazione, sviluppo, attuazione, monitoraggio e misurazione di politiche sulla privacy nei servizi di cloud computing.

3 Politiche di Sicurezza Informatica

Il Gruppo ha definito le politiche di sicurezza descritte nel presente documento, in linea con le necessità e gli obiettivi di business, i requisiti di sicurezza e la struttura organizzativa aziendale. Vengono riportati di seguito i principali obiettivi delle politiche di sicurezza informatica:

- garantire che il patrimonio informativo e informatico sia adeguatamente tutelato rispetto ai rischi di compromissione;
- istituire e mantenere un processo strutturato per l'identificazione e la valutazione del rischio informatico, con lo scopo di applicare gli opportuni controlli e di verificane l'efficacia e l'efficienza nell'ottica del miglioramento continuo e riduzione del livello di rischio identificato;
- assicurare la conformità ai requisiti legali, normativi e contrattuali inerenti alla sicurezza delle informazioni.

Le politiche di sicurezza definite nel presente documento sono state strutturate sulla base delle seguenti aree:

1) Standard internazionale ISO 27001:2013 (descritto al paragrafo 2.1 Documentazione):
   - *Organizzazione della sicurezza*: definizione dei ruoli e delle responsabilità per promuovere comportamenti e controlli al fine di garantire la sicurezza informatica;
   - *Gestione degli asset IT*: criteri tecnici e/o organizzativi per la gestione degli apparati informatici e regole per assegnare un profilo di rischio alle informazioni;
   - *Sicurezza del personale*: regole di comportamento cui il personale deve attenersi;
   - *Sicurezza fisica ed ambientale*: protezione per il personale, per i componenti tecnologici, per i locali e gli archivi cartacei;
   - *Sicurezza operativa e delle telecomunicazioni*: controlli sui processi e sulle attività operative come protezione dei dati trasmessi, e controllo degli accessi ai servizi e sistemi informatici disponibili in rete, tra cui i servizi di cloud computing;
   - *Controllo degli accessi*: controllo degli accessi logici al sistema informativo, secondo precise modalità prestabilite;
   - *Gestione delle chiavi crittografiche:* regole per la gestione delle chiavi crittografiche (creazione, distribuzione, memorizzazione, periodo di utilizzo, backup, dismissione, distruzione, protezione)
   - *Acquisizione, sviluppo e manutenzione dei sistemi*: regole per la gestione, modifica, test e messa in produzione di programmi applicativi, software di base e componenti hardware;
   - *Gestione di eventi e incidenti di sicurezza informatica*: procedure per assicurare la tempestiva gestione e risoluzione di incidenti e malfunzionamenti che possano avere un impatto sulla sicurezza informatica;
   - *Gestione della continuità operativa*: regole per governare il processo di erogazione del servizio anche a fronte di un'interruzione dovuta ad un evento critico;
   - *Conformità a leggi e regolamenti*: criteri e procedure necessarie per gli adempimenti previsti da leggi e regolamenti vigenti;
2) Standard internazionale ISO 27017:215 e ISO27018:2020 (descritto al paragrafo 2.1 Documentazione) con specifico riferimento alle Società del Gruppo che utilizzano servizi di cloud computing.
   - *Servizi di Cloud Computing: criteri, processi e attività relativi ai servizi di Cloud Computing come la descrizione della struttura, la definizione di obblighi e diritti del fornitore dei servizi cloud e delle società del Gruppo Cerved.*

3.1 ORGANIZZAZIONE DELLA SICUREZZA

3.1.1 Organizzazione interna (ruoli e responsabilità)

Il Gruppo deve istituire un processo di gestione della sicurezza informatica, basato su attività di identificazione, valutazione e gestione dei rischi di business ed IT inerenti la sicurezza delle informazioni. Tale processo deve essere orientato al miglioramento continuo al fine di controllare e sottoporre a revisione periodica la sicurezza del sistema informatico di Gruppo.
L'attuazione delle politiche di sicurezza definite nel presente documento richiede un'organizzazione di risorse e processi che promuovano azioni, comportamenti e controlli.
A tal fine il Gruppo si deve dotare di idonee strutture organizzative per il governo, la gestione operativa e il controllo della sicurezza delle informazioni. In particolare, le strutture preposte al governo e al controllo della sicurezza devono svolgere le seguenti attività:

- coordinamento con le strutture operative;
- periodica informativa in merito all'evoluzione delle minacce e delle relative soluzioni di sicurezza;
- periodico monitoraggio dell'efficacia operativa dei controlli implementati al fine di garantire la sicurezza delle informazioni.

Le strutture preposte alla gestione operativa della sicurezza informatica devono occuparsi del disegno, della implementazione e della manutenzione delle soluzioni tecniche ed organizzative necessarie a garantire un appropriato livello di sicurezza delle informazioni all'interno delle piattaforme tecnologiche ed applicative in uso presso le società del Gruppo. A tal fine deve essere garantita una adeguata segregazione dei ruoli e delle relative responsabilità tra le attività di governo e controllo della sicurezza e le attività di gestione operativa delle soluzioni informatiche.

Le principali strutture aziendali competenti in materia di sicurezza sono:

- *il Consiglio di Amministrazione*: stabilisce gli obiettivi di sicurezza, i livelli di rischio accettabili, le strategie di prevenzione e mitigazione e approva i piani di investimento per l'implementazione delle strategie identificate;
- *il Comitato della Sicurezza*: ha il compito di valutare, validare e proporre le strategie di sicurezza dell'azienda, autorizzare la pubblicazione delle policy e delle procedure operative, controllare periodicamente lo stato della sicurezza e promuovere la cultura della sicurezza tra il personale;
- *l'Area IT*: ha il compito di individuare, progettare implementare, tramite le strutture tecniche interessate, le misure organizzative e tecnologiche di sicurezza. Inoltre, ha il compito di gestire gli aspetti operativi della sicurezza dei sistemi informativi, nel rispetto delle policy e delle procedure operative definite;
- *i Responsabili di tutte le aree*: hanno il compito di curare e monitorare nelle proprie strutture l'applicazione delle policy e delle procedure operative definite;
- *l'Internal Audit*: ha il compito di controllare l'applicazione delle norme e monitorare il livello di sicurezza nelle diverse Aree aziendali.

3.1.2 Gestione delle Terze Parti

L'acquisto sul mercato di servizi di diversa natura (consulenza, programmazione, servizi generali, outsourcing, ecc.) comporta la possibilità dell'accesso diretto da parte di terzi al patrimonio informativo aziendale. È dunque fondamentale stabilire i requisiti di sicurezza che devono essere rispettati per la regolamentazione contrattuale e gestionale dei rapporti con Terze Parti che, per erogare i servizi concordati, hanno necessità di accedere alle risorse aziendali.
Nel caso di servizi IT gestiti in outsourcing, le società di Terze Parti devono garantire l'adozione di adeguate misure di sicurezza, almeno pari a quelle adottate dal Gruppo.

Gli accordi con terzi devono contenere i requisiti riguardanti la protezione dei dati del Gruppo. In particolare, i soggetti terzi devono essere disponibili a presentare, su richiesta, il loro piano di sicurezza, le misure di sicurezza implementate e consentire controlli di sicurezza informatica da parte del Gruppo. In particolare:

- l'approccio da adottare per la gestione di collaborazioni con terze parti deve prevedere l'accettazione da parte del contraente delle norme aziendali in vigore e di tutte le modalità operative ed i requisiti richiesti nelle regole di ingaggio e nel contratto stipulato con la Terze Parti;
- devono essere sottoscritti accordi di riservatezza o di non divulgazione validi prima, durante e dopo l'ingaggio in base alla criticità delle informazioni e dei servizi coinvolti;
- devono essere definiti e documentati i ruoli e le responsabilità per la sicurezza delle terze parti;
- si devono stabilire degli accordi per lo scambio di informazioni e di software tra l'organizzazione e terze parti;
- deve essere monitorato e verificato che il fornitore predisponga risorse adeguate all'erogazione dei servizi in base alle richieste contrattuali, in particolare per quanto riguarda la sicurezza informatica.

3.2 GESTIONE DEGLI ASSET IT

3.2.1 Governo degli asset IT

Tutti gli asset IT devono essere identificati in termini di ubicazione fisica (ad esempio sedi, filiali, centri dati e magazzini presso i quali sono ospitati) e di proprietà. Il loro valore deve essere valutato al fine di prevedere un adeguato livello di protezione (per il valore delle informazioni fare riferimento al paragrafo 3.2.2 Classificazione delle informazioni).
Le responsabilità per l'utilizzo e la gestione di tutti i dispositivi informatici devono essere definite al fine di garantire il corretto e sicuro funzionamento in un'ottica di gestione dei rischi associati ad errori umani, furto degli asset, tentativi di frode o uso improprio delle risorse aziendali. Inoltre, deve essere mantenuto un censimento delle apparecchiature (asset) e dei dispositivi assegnati agli utenti.
Nel caso di asset IT forniti a entità esterne del Gruppo (quali ad esempio agenti, fornitori servizi, ecc.) devono essere definiti i requisiti minimi di sicurezza che dovranno essere garantiti dall'owner dell'asset. Inoltre, dovranno essere condotte attività di audit periodiche al fine di verificare che le modalità di gestione ed utilizzo delle apparecchiature e dei dispositivi forniti siano in linea con le esigenze di business e le prassi definite.
Gli asset IT devono essere conservati secondo le indicazioni del produttore e in conformità alle normative interne ed esterne (vedi paragrafo 3.12 Conformità alle normative).
Durante le attività di manutenzione, cambio d'uso, cambio di proprietà e dismissione devono essere previsti meccanismi che garantiscano la riservatezza dei dati contenuti all'interno degli asset e, se necessario, devono essere previsti meccanismi che ne impediscano il recupero non autorizzato (compresa la cancellazione sicura dei dati).

Per quanto concerne il servizio cloud, gli asset delle società del Gruppo che si trovano nei locali del fornitore di servizi cloud devono essere rimossi, e restituiti se necessario, in modo tempestivo al termine dell'accordo di servizio cloud.
Le società del Gruppo devono richiedere una descrizione documentata del processo di cessazione del servizio che copra la restituzione e la rimozione delle risorse delle società del Gruppo, seguita dalla cancellazione di tutte le copie di tali risorse dai sistemi del fornitore di servizi cloud.

3.2.2 Classificazione delle informazioni

Le informazioni, intese come aggregazioni strutturate di dati, sono parte integrante del patrimonio del Gruppo e necessitano di precise regole di gestione per assicurare la loro adeguata tutela. Al fine di proteggere tale asset e utilizzarlo al meglio nell'interesse della missione aziendale, è necessario definire un modello di classificazione delle tipologie di informazioni in relazione alla loro criticità, stabilendo gli indirizzi per la loro corretta gestione in tutte le forme disponibili, tangibili e intangibili.
La classificazione delle informazioni aziendali è un'attività propedeutica all'implementazione di idonee soluzioni finalizzate a proteggere i dati e le relative informazioni ad essi associati: tali soluzioni devono essere adeguate al livello di criticità che i dati assumono nel contesto aziendale. L'implementazione di specifiche soluzioni di sicurezza, sulla base al livello di criticità del dato, consente di assicurare una maggior protezione dei dati e delle relative informazioni e di non disperdere risorse nella protezione di dati che invece risultano facilmente reperibili anche al di fuori del perimetro societario.
La classificazione dei dati aziendali consiste nell'assegnazione di un livello di criticità a ciascun dato prodotto, trattato o conservato all'interno del perimetro aziendale. In particolare, il livello di criticità deve essere assegnato in relazione all'importanza per il perseguimento degli obiettivi di business del Gruppo, nonché agli impatti di tipo economico, d'immagine o legali derivanti da una violazione delle loro proprietà di riservatezza, integrità e disponibilità.
La classificazione delle informazioni deve essere effettuata nel momento della creazione di una categoria o istanza del dato, al fine di poter adottare le idonee modalità di protezione.

Per determinare il livello di sicurezza da perseguire e mantenere, deve essere eseguita un'analisi e una classificazione dei rischi al fine di definire quali saranno i meccanismi di sicurezza adeguati, tali da bilanciare costi e benefici.
Deve essere individuato un "proprietario" per ogni classe d'informazione, applicazione, processo, sistema o infrastruttura IT. Il proprietario ha la responsabilità di valutare il rischio associato al venire meno dei requisiti di sicurezza e di assegnare un'appropriata classificazione di sicurezza.
Il livello di protezione dei dati deve essere commisurato al loro grado di riservatezza e rilevanza per il Gruppo. Sulla base di valutazioni riguardanti la criticità del dato, le informazioni dovranno essere classificate secondo il seguente schema:

- *informazioni pubbliche*: informazioni di pubblico dominio e dati destinati alla divulgazione a soggetti esterni al Gruppo, sottoposti a vincoli riguardanti il contenuto;
- *informazioni a uso interno*: dati usati nello svolgimento dell'ordinaria attività lavorativa, destinati alla divulgazione all'interno del perimetro aziendale la cui eventuale fuoriuscita non compromette la posizione dell'azienda e/o la sua immagine, se non in modo marginale. Sono definite ad uso interno tutte le informazioni che non hanno ottenuto l'approvazione alla libera diffusione al di fuori dell'ambito del Gruppo;
- *informazioni a uso riservato aziendale*: dati che forniscono un vantaggio frutto del know-how maturato dal Gruppo, la cui fuoriuscita può comportare un aumento delle attività operative per ripristinare la posizione competitiva o una perdita d'immagine che necessita investimenti economici per essere ripristinata;
- *informazioni strettamente riservate*: dati che forniscono un vantaggio competitivo la cui fuoriuscita può comportare un decremento considerevole della posizione competitiva del Gruppo o compromettere la sua immagine.

È importante che l'accesso e la condivisione delle informazioni avvenga seguendo specifiche misure di sicurezza e sulla base di autorizzazioni necessarie. Inoltre, in base alla classe del dato e quindi al livello di criticità per ciascun obiettivo di sicurezza, è necessario implementare idonee misure di sicurezza. In particolare, devono essere identificate adeguate misure di protezione in caso di:

- archiviazione cartacea ed elettronica;
- distribuzione cartacea ed elettronica;
- dismissione di informazioni e supporti;
- esecuzione di copie cartacee.

3.3 SICUREZZA DEL PERSONALE

I dipendenti del Gruppo, nonché tutti i collaboratori, devono attenersi a precise norme di comportamento al fine di assicurare un livello omogeneo di sicurezza, riducendo i rischi connessi a errori umani, in ottemperanza delle procedure aziendali (a seguito di imperizia e disinformazione) o dolo.

Per avere adeguate garanzie che il personale, interno ed esterno, abbia chiare le proprie responsabilità, sia stato selezionato ed incaricato in modo conforme al ruolo affidatogli e abbia le competenze necessarie per lo svolgimento delle mansioni assegnategli, il Gruppo deve predisporre appropriate misure di sicurezza durante tutto il ciclo di vita aziendale del personale. In particolare:

- all'atto della selezione del personale devono essere effettuati controlli di verifica sui candidati, in proporzione all'inquadramento e al ruolo aziendale, nel rispetto delle leggi e dei regolamenti pertinenti;
- nel momento in cui il personale sottoscrive un contratto con il Gruppo nel rispetto dei loro obblighi contrattuali, devono accettare e sottoscrivere i termini e le condizioni in merito alle loro responsabilità, anche con riferimento agli aspetti di sicurezza informatica;
- nel corso della normale operatività del personale, devono essere verificati, attraverso audit periodici, che tutti gli utenti applichino le misure di sicurezza previste dalle politiche e procedure aziendali;
- nel momento in cui termina il rapporto di collaborazione con il Gruppo, come specificato nel paragrafo 3.2 Gestione degli asset IT.

La concreta attuazione di un sistema di tutela del patrimonio aziendale si consegue anche grazie alla promozione di una relativa cultura aziendale, realizzata mediante un'attività di informazione e l'attuazione di specifici piani di formazione.

Tutti i dipendenti del Gruppo e, ove opportuno, i collaboratori e gli utenti di terze parti, dovranno pertanto ricevere adeguata formazione al fine di essere resi edotti sui rischi che incombono sui dati ed altri asset aziendali, sulle contromisure disponibili per prevenire gli eventi dannosi, sulle responsabilità che ne derivano e sulle modalità di aggiornamento delle misure di sicurezza adottate dal Gruppo.

Particolare attenzione dovrà essere posta nella scelta e nella designazione degli amministratori di sistema, in considerazione dei privilegi di accesso al sistema informatico aziendale. Per l'attribuzione delle funzioni di amministratore di sistema, interno o esterno, dovranno essere valutate l'esperienza, la capacità e l'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di sicurezza. In particolare, la designazione degli amministratori di sistema deve avvenire su base individuale e, contestualmente all'assegnazione delle mansioni, deve essere fornito ad ogni soggetto l'elenco dettagliato degli ambiti di operatività consentiti.

3.4 SICUREZZA FISICA ED AMBIENTALE

Il Gruppo ha la responsabilità di definire, mediante opportuna analisi del rischio e con il supporto delle strutture aziendali preposte, criteri e requisiti di sicurezza fisica e ambientale al fine di impedire e/o limitare perdite di dati e di risorse critiche dovute a vulnerabilità nell'ambito del dominio fisico.

I dispositivi per il controllo degli accessi alle sedi e ai relativi locali sono stabiliti in funzione dei rischi e della natura delle informazioni contenute. L'accesso ai locali ove risiedono gli strumenti di elaborazione e agli archivi cartacei segregati deve essere consentito solo al personale preposto e autorizzato.

L'accesso alle sedi aziendali deve essere consentito solo previa identificazione della persona che necessita di entrare mediante badge o altri meccanismi di pari affidabilità. In particolare, tutti gli accessi ai locali ritenuti critici devono essere registrati, in maniera automatica o manuale, sia in ingresso che in uscita.

Le aree che ospitano i sistemi di maggiore criticità devono essere localizzate in zone sicure e protette al fine di minimizzare il rischio di perdite o danneggiamenti e utilizzi impropri e non consentiti. Tale obiettivo deve essere perseguito attraverso l'adozione del principio della security-in-depth: tecniche di sicurezza progressive al fine di mitigare il rischio che un livello venga compromesso o scavalcato.

I locali che ospitano gli elaboratori elettronici devono disporre di dispositivi che consentono di:

- segregare e tracciare gli accessi effettuati dal personale autorizzato;
- monitorare tentativi di accesso non autorizzato o di effrazione nei locali;
- monitorare il livello della temperatura e dell'umidità presenti nei locali;
- contrastare eventi dannosi quali allagamenti e/o incendi attraverso idonei strumenti di environmental control;
- garantire l'erogazione del servizio in mancanza di energia elettrica primaria attraverso l'implementazione di opportune soluzioni compensative;
- segnalare ad una centrale operativa eventuali malfunzionamenti.

Le abilitazioni relative all'accesso ai locali che ospitano gli elaboratori elettronici devono:

- essere approvate dalle strutture appropriate prima del rilascio;
- revocate in caso di cessazione del rapporto lavorativo o cambio di mansione;
- riviste e valutate con cadenza frequenza periodica.

Inoltre, tutto il personale dipendente deve essere addestrato in materia di prevenzione e di comportamento in caso di incidenti di sicurezza che possano interessare i locali che ospitano i sistemi.

3.5 SICUREZZA OPERATIVA E DELLE TELECOMUNICAZIONI

3.5.1 Sicurezza operativa

L'infrastruttura IT e le sue principali componenti devono essere adeguatamente protette e ne deve essere mantenuta l'efficacia e l'efficienza nel tempo. Pertanto:

- le procedure operative, le architetture definite, le configurazioni applicate, devono essere documentate e mantenute aggiornate per garantire l'utilizzo corretto e sicuro delle risorse IT;
- la documentazione IT con classificazione uso riservato aziendale deve essere custodita adeguatamente e accessibile solo al personale autorizzato;
- devono essere pianificate e messe in atto le misure necessarie a garantire un adeguato livello di efficienza e di prestazioni dei sistemi IT, la prevenzione del rischio di malfunzionamenti o di degrado delle funzionalità di sicurezza applicate. Inoltre, tali misure devono poter assicurare:
  - ✓ il mantenimento dell'efficienza dei sistemi e la loro regolare manutenzione, anche in considerazione del livello di criticità delle informazioni che trattano;
  - ✓ che l'accesso ai sistemi ai fini di amministrazione e manutenzione sia consentito al solo personale preposto e autorizzato;
  - ✓ che il software installato sia provvisto di licenza, conforme alle normative di legge applicabili e fornisca il livello di servizio richiesto.
- deve essere individuata una politica di prevenzione a livello aziendale contro software malevoli (virus informatici, worm, ecc.). Tale politica deve prevedere chiare ed efficaci misure di sicurezza, l'utilizzo e la manutenzione ed il tempestivo aggiornamento di appositi strumenti software e specifici controlli al fine di garantire e mantenere la sicurezza della rete aziendale e delle informazioni condivise attraverso di essa. In particolare, l'efficacia e l'aggiornamento di tali programmi devono essere verificate, in modalità automatica, con frequenza periodica.
- l'uso delle risorse IT deve essere monitorato e devono essere pianificate le esigenze di capacità elaborativa per minimizzare il rischio di prestazioni inadeguate, di malfunzionamenti e di degrado dei livelli di servizio e di sicurezza stabiliti;

I processi operativi di gestione delle risorse informatiche devono essere strutturati e controllati al fine di garantire la sicurezza informatica. In particolare:

- i sistemi hardware e le connesse unità periferiche devono essere controllati e soggetti a un livello di manutenzione adeguato alle esigenze di continuità operativa del Gruppo;
- le operazioni di manutenzione dei sistemi hardware devono essere eseguite, per quanto possibile, con tempistiche compatibili con le elaborazioni per i processi di business, tali da ridurre al minimo le interferenze;
- devono inoltre essere eseguite periodicamente misurazioni delle capacità di elaborazione dei sistemi al fine di soddisfare adeguatamente le esigenze dei processi di business (capacity planning);
- la valutazione di nuovi prodotti, in sostituzione o integrazione del software di base deve comprende le verifiche delle caratteristiche di sicurezza, affidabilità e disponibilità, in ottica di riduzione della probabilità di eventi dannosi e di miglioramento del livello di sicurezza.

3.5.2 Sicurezza delle telecomunicazioni

La progettazione della sicurezza di una rete informatica deve considerare i seguenti aspetti:

- *segregazione*: meccanismi di separazione e filtraggio del traffico tra sottoreti interne al perimetro aziendale;

- *monitoraggio*: modalità e strumenti da utilizzare per controllare il traffico in transito sulle reti, con lo scopo di individuare eventuali scostamenti rispetto all'operatività definita;
- *disponibilità*: modalità e strumenti per garantire la continuità nell'erogazione dei servizi di rete.

La configurazione della sicurezza di una rete informatica deve affrontare i seguenti aspetti:

- *indirizzamento*: regole per l'assegnazione degli indirizzi di rete degli apparati e dei sistemi connessi alle reti;
- *instradamento*: soluzioni tecniche adottate per evitare, data la destinazione delle informazioni da trasmettere, percorsi indesiderati;
- *accesso agli apparati di rete*: meccanismi di controllo e restrizione degli accessi agli apparati di rete che realizzano l'infrastruttura telematica.

Devono quindi essere adottati criteri tecnici e procedurali al fine di garantire che solo gli utenti autorizzati possano accedere ai singoli sistemi informatici o servizi, mediante la rete di telecomunicazione. Analogamente la rete di telecomunicazione deve garantire che i messaggi e i dati trasmessi sulla rete non siano alterati o cancellati e che vi siano sufficienti protezioni al fine di evitare che vengano inseriti dati fraudolenti.

Le componenti della rete telematica devono essere protette attraverso apposite misure:

- gli apparati di rete devono essere dislocati all'interno di armadi opportunamente protetti. L'accesso a tali armadi deve essere consentito solamente ai tecnici interni ed esterni responsabili della gestione della manutenzione;
- gli apparati di rete ritenuti critici devono essere duplicati per gestire eventuali malfunzionamenti degli stessi;
- devono essere redatti e mantenuti costantemente aggiornati i diagrammi della topologia della rete che devono essere trattati come informazioni riservate.

Nella gestione della sicurezza relativa agli accessi remoti devono essere adottate le seguenti contromisure:

- l'accesso ai sistemi da remoto deve essere consentito solo previa autorizzazione e sulla base di motivazioni che lo giustificano;
- le linee di ingresso alla rete di Gruppo adibite al traffico devono essere gestite da apposite apparecchiature che consentono il controllo e assicurano la protezione da accessi non autorizzati;
- l'utilizzo di apparecchiature telematiche collegate direttamente agli elaboratori della rete di Gruppo, deve essere concesso solo previa autorizzazione e su comprovata motivazione.

Le connessioni tra la rete di Gruppo ed Internet devono avvenire solo attraverso dispositivi che presentano requisiti tecnologici in grado di assicurare la protezione dagli accessi non autorizzati (firewall, router, proxy, …).

L'accesso a Internet da parte dei dipendenti e collaboratori aziendali deve essere concesso in funzione dei fabbisogni degli utenti, limitatamente allo svolgimento delle specifiche attività e compiti.

La gestione dell'infrastruttura di rete del Gruppo deve prevedere dispositivi di monitoraggio in grado di esaminare il traffico di rete, di verificare il corretto funzionamento dei dispositivi di sicurezza e di fornire tempestivi segnali di allarme in caso di attacco ai sistemi di protezione.

3.5.3 Backup e gestione dei supporti di memorizzazione

Le operazioni di backup consentono di garantire la disponibilità delle informazioni e dei sistemi anche a seguito di incidenti di sicurezza informatica o di eventi di disastro. In particolare, nell'ambito dell'infrastruttura di Gruppo devono essere sottoposti a procedura di backup e archiviazione:

- i dati necessari e sufficienti a garantire il ripristino completo delle applicazioni ritenute critiche e delle relative basi di dati;

- i dati e programmi che consentano di soddisfare successive richieste di ripristino da parte di Unità di controllo interne o esterne, in coerenza con i tempi di mantenimento (retention) definiti in linea con le normative alle quali il Gruppo è sottoposto (vedi paragrafo 3.12 Conformità alle normative).

Durante tutte le fasi previste dal processo di gestione dei backup devono essere garantite la riservatezza, l'integrità e la disponibilità dei dati trattati. A tal fine:

- devono essere concordate ed attuate opportune frequenze di salvataggio, tecniche di salvataggio e modalità di conservazione delle copie, in linea con i requisiti per garantire il ripristino completo delle applicazioni critiche e delle relative basi di dati;
- devono essere effettuate adeguate verifiche di ripristino dei dati (parziali e totali) sottoposti a backup, al fine di assicurare l'efficacia delle procedure.

Le misure di sicurezza adottate per la protezione dei dati di backup devono essere conformi al livello di criticità delle informazioni contenute nel backup stesso. In particolare:

- l'accesso fisico ai locali ospitanti il sistema di backup deve essere consentito solo a personale autorizzato;
- l'accesso logico ai sistemi di backup deve essere controllato e permesso al solo personale autorizzato;
- l'eventuale accesso da parte di altri soggetti per l'effettuazione di attività diverse da quelle di ordinaria gestione dei sistemi di backup deve essere preventivamente autorizzato;
- eventuali eccezioni devono essere concordate con le strutture di sicurezza preposte.

Le operazioni di backup devono essere documentate al fine di agevolare eventuali richieste di dettagli relative alle attività di salvataggio dei dati. Inoltre, i supporti di memorizzazione utilizzati per effettuare i backup devono essere scelti in base ai tempi di ripristino del backup stesso e devono essere gestiti rispettando i seguenti vincoli:

- i supporti di memorizzazione devono essere conservati in un locale diverso da quello in cui risiedono i dati originali;
- devono essere implementate misure di controllo degli accessi che consentano di limitare l'accesso logico e fisico ai supporti e ai dati in essi contenuti ai soli incaricati alle attività di backup. Le misure di controllo devono essere correlate alla criticità dei dati in essi contenuti;
- i dati presenti sui supporti di memorizzazione devono essere eliminati utilizzando metodi di cancellazione sicura (ad esempio, algoritmi specifici per la cancellazione sicura dei dati);
- i supporti di backup non più necessari devono essere distrutti secondo modalità che non consentano un successivo accesso ai dati contenuti nei supporti stessi;
- i supporti di backup non devono essere mai lasciati incustoditi e devono essere sempre riposti in luoghi adeguatamente protetti, quali ad esempio armadi ignifughi chiusi a chiave e/o casseforti;
- la conservazione di supporti di backup rimovibili deve prevedere la corretta etichettatura degli stessi.

3.5.4 Gestione dei log di sistema

Il tracciamento e la successiva consultazione dei log rappresentano degli elementi essenziali al presidio e la garanzia della sicurezza del sistema informatico aziendale, in quanto permettono di effettuare elaborazioni e analisi (sia in tempo reale che in tempi diversi) sulle attività svolte sui sistemi informativi. In particolare, il tracciamento permette di supportare e ottimizzare le seguenti attività:

- ricostruzione degli eventi;
- attribuzione delle responsabilità;
- analisi e comprensione all'interno del Gruppo di chi utilizza i sistemi e sul tipo di utilizzo effettuato;
- conformità a leggi, norme e standard.

Deve essere inoltre garantita l'integrità, la disponibilità e la riservatezza nel tempo dei log al fine di assicurare una efficace gestione del servizio ai fini della ricostruzione di un evento. Gli utenti del sistema informatico devono essere a conoscenza che l'utilizzo dei sistemi aziendali è sottoposto a sistemi di tracciamento e di consultazione dei log (nel rispetto delle normative in essere riportate nel paragrafo 3.12 Conformità alle normative).

3.5.5 Sicurezza dei servizi cloud

Il cloud multi-tenant permette alle società di Gruppo di condividere i dati in un cloud pubblico o privato. I dati di ogni tenant devono essere isolati e inaccessibili ad altri clienti.
Le società del Gruppo definiscono i requisiti per la segregazione delle reti al fine di ottenere l'isolamento del tenant nell'ambiente condiviso di un servizio cloud e verificano, con l'eventuale supporto del fornitore dei servizi cloud, che siano soddisfatti tali requisiti, tra cui:

- la separazione delle risorse in uso delle società di Gruppo in ambienti multi-tenant;
- la separazione dell'amministrazione interna del fornitore di servizi cloud dalle risorse in uso dalle società di Gruppo.

Nell'attività di configurazione delle macchine virtuali, le società del Gruppo e i fornitori di servizi cloud devono garantire la corretta implementazione di misure tecniche (es. anti-malware e raccolta log) per ogni macchina virtuale utilizzata.
Inoltre, le società di Gruppo devono garantire che:

- siano definite e documentate una politica di sicurezza delle informazioni per la configurazione della rete virtuale, coerente con la politica di sicurezza delle informazioni per la rete fisica;
- venga applicata un'appropriata segregazione logica dei dati delle società di Gruppo, delle applicazioni virtualizzate, dei sistemi operativi, dello storage e della rete;
- siano considerati rischi associati all'esecuzione del software fornito dalle società di Gruppo all'interno delle macchine virtuali offerte dal fornitore di servizi cloud.

3.6 CONTROLLO DEGLI ACCESSI

L'accesso alle informazioni deve rispettare il principio del "need-to-know", ossia la condivisione, l'accesso e la comunicazione delle informazioni deve essere garantita al solo personale che, preventivamente identificato ed autorizzato per un periodo di tempo determinato, ne ha effettiva necessità per lo svolgimento delle proprie mansioni lavorative.
L'accesso ai sistemi dovrà essere consentito a seguito di un'identificazione tramite un codice identificativo utente (userid) e a seguito di un'autenticazione tramite una password. Tali meccanismi dovranno essere corredati qualora necessario da ulteriori strumenti di autenticazione (sistemi di strong authentication).
Le norme di sicurezza esposte in questa sezione si applicano, salvo casistiche particolari da valutare all'occorrenza, a tutte le tipologie di utenti che utilizzano l'infrastruttura tecnologica di Gruppo.

3.6.1 Gestione delle utenze

L'intero ciclo di vita delle abilitazioni di accesso ai sistemi informatici (creazione di account utente, modifica account utente e la rimozione dell'account utente), deve essere definito e formalizzato in modo da ridurre il rischio di accesso non autorizzato alle informazioni. In particolare, al fine di garantire la sicurezza delle informazioni devono essere soddisfatti i seguenti vincoli:

- la richiesta di creazione di una nuova utenza e la relativa generazione deve essere effettuata unicamente da parte del personale preposto;
- le user id devono essere create seguendo uno standard di nomenclatura tale da:
  - non fornire indicazioni sul tipo di attività che viene svolta dalla persona a cui l'utenza si riferisce;
  - non fornire indicazioni sui privilegi associati all'utenza.
- nel limite del possibile dovrà essere evitata la creazione di più utenze assegnate alla stessa persona per l'accesso al medesimo sistema e nel caso di effettiva necessità queste utenze dovranno essere autorizzate e opportunamente censite e documentate;
- la persistenza della validità delle utenze deve essere verificata periodicamente dalle strutture preposte;
- la modifica di una utenza deve essere effettuata unicamente da parte del personale preposto, sotto richiesta esplicita da parte di figure autorizzate. Particolare attenzione deve essere svolta in caso cambiamento dell'impiego dell'utente in modo che, al termine del cambiamento, non permangano le autorizzazioni correlate al precedente profilo autorizzativo;
- le utenze del personale interno dipendente del Gruppo devono essere disattivate al termine del rapporto di lavoro con le Società del Gruppo o qualora il rapporto di collaborazione sia temporaneamente sospeso. Qualsiasi eccezione a questa norma generale dovrà essere formalmente documentata e autorizzata;
- le utenze assegnate al personale esterno al Gruppo devono essere disattivate in caso di recesso dal contratto del servizio o in caso di cessazione del rapporto lavorativo con la Società esterna da parte del lavoratore o sospensione temporanea.

Deve essere limitata la creazione di utenze di servizio, soprattutto laddove utilizzate da più persone fisiche. Qualora sia necessario creare utenze di servizio, queste devono rispettare i seguenti vincoli:

- ottenere l'approvazione dalle strutture di Sicurezza preposte;
- assegnare, formalizzandola, la responsabilità dell'utenza ad un'unica persona fisica;
- definire le modalità per la gestione, l'estensione ad altri utilizzatori, la tracciatura nel tempo, il monitoraggio ed il costante aggiornamento delle assegnazioni;
- consentire, ove possibile, l'accesso solo da determinate postazioni di lavoro.

Per quanto concerne i servizi cloud, le società del Gruppo devono verificare che la procedura del fornitore di servizi cloud per l'assegnazione di informazioni di autenticazione ne soddisfi i requisiti.

Inoltre, le società del Gruppo devono formalizzare una politica di controllo degli accessi che definisca i requisiti per l'accesso degli utenti delle società di Gruppo a ciascun servizio cloud; mentre il fornitore di servizi cloud deve fornire alle società del Gruppo funzioni di registrazione e de-registrazione degli utenti e specifiche per l'uso di queste funzioni.

3.6.2 Tecniche di autenticazione

Al fine di garantire che l'accesso alle informazioni sia permesso esclusivamente al personale autorizzato e per i soli scopi consentiti, devono essere attivate misure per la limitazione dell'accesso ai sistemi informatici del Gruppo. In particolare:

- devono esser predisposti meccanismi di identificazione ed autenticazione che consentano il controllo dell'accesso logico alle risorse IT, al fine di garantire che tali risorse siano accedute e utilizzate solo dal personale autorizzato;
- devono essere previsti sistemi e procedure per l'utilizzo in sicurezza dei servizi forniti dal Gruppo (Posta elettronica, Accesso internet, …) e delle applicazioni e relativi sistemi operativi;

Con specifico riferimento al servizio cloud:

- usare tecniche di autenticazione sufficienti per autenticare gli utenti delle società del Gruppo che accedono alle risorse Cloud. Particolare rilevanza ricoprono in tal senso le tecniche di autenticazione degli amministratori;
- le società del Gruppo devono garantire che l'accesso alle informazioni nel servizio cloud possa essere limitato in conformità alla politica di controllo dell'accesso e che tali restrizioni siano applicate. Ciò include la limitazione dell'accesso ai servizi cloud, alle funzioni del servizio cloud e ai dati degli utenti del servizio cloud mantenuti nel servizio. In particolare, devono essere predisposti controlli di forza sufficiente a mitigare i rischi identificati, sia che tali controlli siano forniti dalle società del Gruppo o dal fornitore di servizi cloud;
- Il fornitore di servizi cloud deve garantire che qualsiasi uso di programmi di utilità in grado di aggirare le normali procedure operative o di sicurezza sia strettamente limitato al personale autorizzato, e che l'uso di tali programmi sia rivisto e controllato regolarmente.

I sistemi delle utenze devono essere predisposti in modo tale da rispettare i seguenti requisiti di sicurezza sulle modalità di gestione della password:

- prevedere la modifica obbligatoria della password iniziale al primo utilizzo;
- prevedere la scelta di una password sicura che rispetti i requisiti legislativi applicabili in termini di lunghezza e complessità (vedi paragrafo 3.12 Conformità alle normative);
- prevedere il cambio periodico della password da parte dell'utente;
- prevedere meccanismi automatici di blocco dell'utenza a seguito di un numero limitato di tentativi di accesso negato;
- mascherare i caratteri della password durante la digitazione;
- impedire accessi non autorizzati ai sistemi di gestione delle utenze e delle relative password.

3.6.3 Gestione dei ruoli e dei privilegi

La definizione dei ruoli deve essere effettuata unicamente da parte delle strutture aziendali preposte. Per lo svolgimento di tale attività strutture aziendali preposte devono valutare, per le utenze associate al personale interno dipendente della Gruppo, perlomeno i seguenti attributi:

- la Società del Gruppo e l'Unità Organizzativa di appartenenza dell'utente;

- la figura professionale (definita da mansioni, ruolo e posizione aziendale all'interno dell'Area Organizzativa di appartenenza) associata all'utente;
- eventuali responsabilità particolari aggiuntive rispetto a quelle previste dalla figura professionale (sostituzioni, delega di alcuni poteri decisionali o autorizzativi, ecc.).

Per la definizione dei ruoli da assegnare alle utenze associate al personale esterno devono essere valutati dalle strutture aziendali preposte almeno i seguenti attributi, sulla base del contratto di fornitura:

- la Società esterna di appartenenza;
- il riferimento al contratto di fornitura, in particolare il periodo di validità del contratto stesso;
- il responsabile di riferimento interno dipendente della Società esterna.

Nella definizione e assegnazione dei ruoli devono essere presi in considerazione almeno i seguenti elementi:

- il principio della separazione dei compiti (Segregation of Duties);
- il principio del minimo privilegio (Need to Know);
- il rispetto dei vincoli di sicurezza e degli eventuali obblighi di origine legislativa o contrattuale (vedi paragrafo 3.12 Conformità alle normative);
- la conformità al modello organizzativo in essere del Gruppo.

I ruoli che regolano l'accesso alle applicazioni devono rispettare i seguenti vincoli:

- essere definiti secondo un modello di autorizzazione in base al livello di responsabilità assegnato a ciascuna figura professionale;
- prevedere ruoli specifici per le operazioni di tipo autorizzativo;
- la modifica dei profili deve essere tracciata e deve essere conservata traccia anche di chi ha effettuato le modifiche sui profili;
- i profili di accesso associati ai diversi utenti devono essere valutati e rivisti con frequenza periodica dalle strutture preposte.

3.7 GESTIONE DELLE CHIAVI CRITTOGRAFICHE

Cerved è responsabile della gestione dei sistemi di cifratura adottati sia per la fornitura di servizi interni che per i clienti, e deve garantire che l'implementazione e le operazioni relative ai sistemi di cifratura siano conformi alle *Linee Guida Crittografia e Gestione delle chiavi*.

È necessario stabilire un processo documentato per la gestione delle chiavi crittografiche che comprenda:

- Generazione di chiavi utilizzando lunghezze di chiavi approvate.
- Metodi sicuri e approvati per la distribuzione, l'attivazione e l'archiviazione, il recupero e la sostituzione / aggiornamento delle chiavi crittografiche.
- Revoca immediata (disattivazione) di chiavi crittografiche, ad esempio quando un dipendente lascia l'organizzazione
- Ripristino di chiavi crittografiche perse, danneggiate o scadute.
- Dismissione delle chiavi crittografiche che potrebbero essere state compromesse, ad esempio mediante divulgazione a una parte esterna
- Backup / archiviazione delle chiavi crittografiche e mantenimento della cronologia delle chiavi crittografiche (ad es. per consentire l'accesso alle informazioni di backup o archiviate).
- Definizione di periodi di retention delle chiavi crittografiche e processi di cambiamento delle chiavi;
- Processi di limitazione dell'accesso alle chiavi crittografiche alle sole persone autorizzate.

La proprietà delle chiavi crittografiche dovrebbe essere assegnata ai proprietari delle chiavi, i quali devono essere consapevoli delle loro responsabilità nell'uso e nella protezione delle chiavi (e ove necessario divulgare le chiavi).
Le chiavi crittografiche devono essere protette contro l'accesso da parte di persone o applicazioni non autorizzate, distruzione accidentale o dannosa e copia non autorizzata.

3.7.1 Riservatezza, Integrità e Autenticazione

I dati, in funzione della tipologia di informazioni trattate e in linea con quanto definito nella “policy di classificazione delle informazioni”, devono essere sottoposti a valutazione, da parte dell’owner degli stessi, al fine di definirne la necessità dell’adozione della cifratura per garantire la riservatezza.
L'integrità dei dati (comprese le chiavi di cifratura) deve essere protetta mediante crittografia sia durante la trasmissione che durante la conservazione, al fine di soddisfare i principi di Security By Design e By Default descritti nelle Linee Guida Security by Design e by Default e Sviluppo Sicuro del Software in funzione del rischio associato alla tipologia di informazioni trattate.
L'uso dei controlli crittografici a fini di autenticazione deve essere conforme ai requisiti di autenticazione, quali il metodo e il protocollo di autenticazione, la memorizzazione e la validità delle credenziali di autenticazione. Pertanto, le credenziali crittografiche di autenticazione (ad esempio, chiavi private) devono essere tenute segrete.

Gli insider sono coloro che possono ottenere l’accesso a dati riservati delle società del Gruppo, compromettendone riservatezza, integrità e disponibilità. Di seguito vengono riportati i principali rischi riconducibili agli insider:

- divulgazione di dati sensibili;
- furto di proprietà intellettuali;
- frode;
- insider trading;

- violazioni della conformità a normative interne ed esterne.

È compito delle società del Gruppo mettere in atto delle operazioni al fine di gestire rischi da parte degli insider, basandosi sui seguenti principi di:

- trasparenza;
- configurabilità;
- usabilità.

3.7.2 Conservazione dei dati

Se richiesta la crittografia a livello di supporto, i supporti di archiviazione devono essere crittografati con cifratura dell'intero disco.
Qualora sia richiesta la cifratura a livello di file, invece, si utilizzano i metodi di cifratura indicati di seguito:

- File-based;
- Strumenti di compressione file (es. WinZip, ecc.) compatibili con FIPS 197, utilizzando il metodo AES a 256 bit.

In alcuni casi, sia il supporto che il file possono essere criptati simultaneamente.

Per quando concerne i servizi cloud, il fornitore di servizi cloud deve informare le società del Gruppo della posizione geografica e dei Paesi in cui può conservare, anche temporaneamente, i loro dati.

3.7.3 Trasmissione dei dati

Quando è richiesta la cifratura della trasmissione, in funzione della tipologia di dato trasmesso, devono essere utilizzati esclusivamente i protocolli presenti nelle *Linee Guida Crittografia e Gestione delle chiavi 6.1 Allegato A*. Se il rischio associato ai dati trasmessi è elevato, sia la trasmissione che il file possono essere criptati simultaneamente.
Nel caso di invii di email al di fuori del perimetro della Società (ad esempio Clienti, Fornitori ecc.) dove la cifratura risulti necessaria ma non supportata dal destinatario, è necessario utilizzare metodi alternativi di scambio di dati sicuri (ad esempio Winzip con password). Le connessioni ai clienti e a terzi devono utilizzare di default un'opportuna crittografia, ove necessario.

3.7.4 Protocolli e versioni

È possibile utilizzare solo i protocolli e le versioni che soddisfino i requisiti, i quali sono specificatamente descritti all'interno del documento *Linee Guida Crittografia e Gestione delle chiavi (paragrafo 4.2.4 Protocolli e versioni e Allegato A)*
Il protocollo deve essere utilizzato al massimo della sua capacità di cifratura su tutti i componenti di trasmissione, al fine di soddisfare i principi di Security By Design e By Default descritti nelle Linee Guida Security by Design e by Default e Sviluppo Sicuro del Software, e comunque in funzione della tipologia di dato trattato e dipendentemente dalla valutazione eseguita dall'owner del dato stesso.

3.8 PROCESSO DI GESTIONE DELLE CHIAVI

Un sistema di gestione delle chiavi deve essere utilizzato per gestire e proteggere centralmente le chiavi crittografiche. L'accesso alle chiavi all'interno del sistema di gestione delle chiavi è consentito solo se necessario o richiesto dal responsabile di funzione dell'utente richiedente. Tutti gli accessi al sistema di gestione delle chiavi e alle chiavi memorizzate devono essere registrati e monitorati. L'efficacia della cifratura dipende dalla corretta gestione delle chiavi, che dovranno essere amministrate in modo sicuro durante tutto il loro ciclo di vita.

- **Creazione delle chiavi**

Le chiavi crittografiche devono essere generate all'interno di un modulo crittografico. I moduli crittografici basati su software e/o firmware devono essere almeno conformi alla FIPS 140-2 livello 1. I moduli crittografici HSM devono essere conformi almeno al FIPS 140-2 livello 2.

- **Distribuzione delle chiavi**

Un sistema di gestione delle chiavi deve affrontare la trasmissione sicura delle chiavi dal loro spazio di memorizzazione al dispositivo che le richiede, conformemente agli algoritmi di cifratura e alle dimensioni delle chiavi. L'avvolgimento delle chiavi (Key Wrapping) deve essere utilizzato quando le chiavi sono scambiate con crittografia simmetrica. Le chiavi private asimmetriche (da utilizzare per la firma o la cifratura) non sono distribuite. È necessario compilare e mantenere aggiornato un inventario di tutte le chiavi utilizzate.

- **Memorizzazione**

Ove tecnicamente fattibile, le chiavi private asimmetriche (da utilizzare per la firma o la cifratura) devono essere generate direttamente sul dispositivo su cui devono essere conservate e protette da una password o da un token hardware. Le chiavi non devono mai essere memorizzate in un formato non criptato. Le chiavi memorizzate in database offline sono criptate con key encryption keys prima dell'esportazione della chiave principale, ove possibile. La lunghezza della key encryption keys (e dell'algoritmo) deve essere equivalente o superiore alla lunghezza della chiave protetta.

- **Periodi di utilizzo, rotazione, archiviazione e revisione**

Le chiavi utilizzate per la crittografia dei dati a breve o a lungo termine devono essere archiviate in base alle esigenze locali di conservazione dei dati e alle esigenze commerciali dei dati crittografati. L'area IT di Cerved è responsabile della definizione e dell'attuazione delle revisioni annuali degli algoritmi e delle procedure relative alle lunghezze delle chiavi.

- **Aggiornamento e rinnovo**

Ogni singola chiave sottoposta ad un processo di rinnovo deve avere un livello di sicurezza pari o superiore a quello della chiave originaria.

- **Backup e ripristino**

In base alle tipologie di dati che Cerved vuole criptare, è necessario determinare le chiavi da includere nel processo di backup. È previsto un meccanismo di recupero delle chiavi per garantire l'accesso ai dati crittografati in caso di perdita della chiave o di danneggiamento della stessa. Tale meccanismo potrebbe includere il backup delle chiavi o l'utilizzo di una chiave master.

- **Dismissione**

Una chiave deve essere dismessa quando è scaduto il suo periodo di validità o quando si sospetta che la chiave sia stata compromessa. Le chiavi in dismissione non devono essere utilizzate e/o rese disponibili in produzione. Se la conservazione delle chiavi ritirate può rappresentare un rischio per la sicurezza, le chiavi ritirate devono essere predisposte per la distruzione dopo che si è stabilito che la chiave non è più necessaria.

- **Distruzione**

Le chiavi devono essere distrutte in modo sicuro quando non è necessario conservare i dati protetti. Le chiavi sono distrutte conformemente alla FIPS 140-2.

- **Protezione**

Le chiavi private devono essere protette dal sistema di gestione delle chiavi per impedirne l'uso, la divulgazione e la modifica non autorizzati. Le chiavi pubbliche devono essere protette dal sistema di gestione delle chiavi per evitare modifiche non autorizzate.

3.9 ACQUISIZIONE, SVILUPPO E MANUTENZIONE DEI SISTEMI INFORMATIVI

Il processo di Change Management prevede l'approvazione per ogni richiesta di cambiamento che riguarda l'infrastruttura informatica a supporto (software, hardware, network, ecc.). L'obiettivo è di assicurare che metodi e procedure standard siano utilizzati per un'efficiente e pronta gestione di tutti i cambiamenti applicativi e d'infrastruttura IT, al fine di minimizzare l'impatto e gli incidenti in capo ai servizi erogati

3.9.1 Norme di sicurezza relative al processo di Change Management

Lo sviluppo e la manutenzione dei sistemi informativi devono essere realizzati in modo da minimizzare il rischio di interruzione dei servizi o malfunzionamento, garantendo, nello stesso tempo, l'integrità, la confidenzialità delle informazioni. Al fine di garantire tali proprietà è necessario valutare in fase di apertura di nuovi progetti l'esecuzione di una analisi per la valutazione di eventuali implicazioni di sicurezza. In particolare, ogni nuovo servizio che richiede l'implementazione di una nuova applicazione o la modifica ad una esistente deve prevedere l'esecuzione delle seguenti fasi ed il rispetto dei relativi vincoli di sicurezza:

- *definizione dei requisiti utente*: prevedere una chiara definizione dei requisiti attraverso l'identificazione dei requisiti utente e dei requisiti di sicurezza;
- *fattibilità tecnica ed economica*: prevedere uno studio di fattibilità tecnica ed economica da parte delle strutture coinvolte, in collaborazione con l'Area IT. In particolare, dovranno essere analizzati i costi e i benefici derivanti dalla nuova applicazione o dalla modifica.
- *analisi funzionale e tecnica*: prevedere una chiara analisi funzionale e tecnica. Tale analisi deve contenere:
  - ✓ i controlli di input;
  - ✓ i controlli di output;
  - ✓ i meccanismi di identificazione e autenticazione per l'accesso alle informazioni;
  - ✓ un'analisi dei rischi ove siano analizzate le possibili minacce alla nuova applicazione o modifica e siano evidenziate le idonee contromisure;
  - ✓ i criteri di sicurezza per configurare in sicurezza le piattaforme di supporto all'applicazione;
  - ✓ i requisiti (modalità e frequenza) di salvataggio dei dati e ripristino delle applicazioni;
  - ✓ il disegno architetturale che ponga in evidenza l'integrazione delle nuove applicazioni e servizi con l'esistente contesto architetturale di riferimento;
- *sviluppo e test delle applicazioni o modifiche*: le attività di test devono essere esaustive al fine di verificare il corretto funzionamento dell'applicazione. I test delle applicazioni o delle modifiche devono essere approvati formalmente dalle appropriate strutture organizzative coinvolte;
- *trasferimento dei programmi in ambiente di produzione*: il trasferimento di una nuova applicazione o di un aggiornamento dall'ambiente di test a quello di produzione deve essere approvato dalle opportune strutture organizzative. In particolare:
  - ✓ il trasferimento di una nuova applicazione o di un aggiornamento dall'ambiente di test a quello di produzione deve essere effettuato dalle appropriate strutture;
  - ✓ il trasferimento di una nuova applicazione o di un aggiornamento in produzione deve essere seguito da prove di dettaglio al fine di assicurare che non vi siano stati errori riguardanti le informazioni, con particolare riferimento all'integrità dei dati;
  - ✓ devono essere adottati criteri tecnici e procedurali al fine di tenere traccia delle diverse versioni delle applicazioni in produzione in modo da poter risalire agevolmente alle versioni precedenti in caso di necessità.

- *modifiche di emergenza*: devono essere consentite laddove si verifichi una criticità bloccante per l'erogazione del servizio in produzione. In particolare, deve essere possibile documentare le motivazioni che hanno portato alla modifica. Completate le modifiche di emergenza e ripristinata l'erogazione del servizio interrotto, devono essere informate le strutture interessate;
- *documentazione*: la documentazione sulle applicazioni deve essere tenuta costantemente aggiornata. Oltre alla documentazione di progetto, occorre prevedere i seguenti documenti:
  - ✓ richiesta;
  - ✓ valutazione della richiesta;
  - ✓ approvazione della richiesta;
  - ✓ esito delle attività di test e relativa accettazione;
  - ✓ approvazione del rilascio in produzione.

Per quanto concerne il servizio cloud, il processo di gestione delle change delle società del Gruppo deve tenere conto dell'impatto di qualsiasi change apportata dal fornitore di servizi cloud, il quale è tenuto a fornire alle società del Gruppo le informazioni riguardanti le modifiche al servizio cloud che possono influenzarlo, mediante una comunicazione che comprende almeno quanto segue:

- categorie di modifiche;
- data e ora previste per le modifiche;
- descrizione tecnica delle modifiche al servizio cloud e ai sistemi sottostanti;
- notifica dell'inizio e del completamento delle modifiche.

3.9.2 Manutenzione dei sistemi (Configurazioni e Patch Management)

Tutta l'infrastruttura aziendale deve essere mantenuta e configurata al fine di ridurre le vulnerabilità infrastrutturali, applicando tutte le opportune misure di sicurezza in base allo specifico sistema. In particolare:

- deve essere effettuata un'analisi delle vulnerabilità che potenzialmente interessano i sistemi, con informazioni sulla loro criticità, sui possibili impatti sull'operatività e sulle contromisure applicabili per la mitigazione del rischio associato alla vulnerabilità;
- i sistemi identificati come critici devono essere sottoposti a test di vulnerabilità su base periodica, al fine di identificare possibili falle di sicurezza nella configurazione del sistema;
- l'identificazione delle vulnerabilità deve avvenire mediante l'esecuzione di Vulnerability Assessment selettivi su un singolo asset o su un perimetro più ampio (effettuati internamente o esternamente) oppure a seguito di rilevazioni di attacchi/segnalazioni provenienti dal processo di Incident Management (vedi paragrafo 3.8 Gestione di eventi e incidenti di sicurezza informatica);
- le vulnerabilità identificate devono essere analizzate al fine di implementare le opportune attività di rimedio per la loro risoluzione e mitigazione. Tali azioni devono essere implementate tempestivamente e verificate al fine di validarne il livello di efficacia;
- devono essere implementati meccanismi per la gestione delle configurazioni dei sistemi in grado di tenere traccia dei cambiamenti apportati ai sistemi stessi;
- gli strumenti e i comandi di amministrazione devono poter essere utilizzati solo dalle utenze aventi profilo di amministrazione;
- devono essere utilizzati dei protocolli sicuri per l'accesso ai sistemi in grado di garantire la riservatezza e integrità delle comunicazioni (es. SSH, Https);

- l'infrastruttura deve prevedere l'utilizzo di strumenti automatici di filtering, al fine di escludere la presenza di virus o altre componenti pericolose e consentire la riduzione dei rischi legati all'utilizzo dei servizi di posta elettronica e di Internet;
- su ciascun sistema, ove applicabile, deve essere installato il software antivirus, che deve essere configurato come segue o con impostazioni più restrittive:
  - ✓ il software non deve poter essere disabilitato da parte dell'utente;
  - ✓ la configurazione del software non deve poter essere modificata da parte dell'utente;
  - ✓ la scansione in tempo reale dei file deve essere sempre attiva;
  - ✓ il software antivirus deve essere aggiornato periodicamente;
  - ✓ devono essere programmate scansioni automatiche periodiche del sistema;
  - ✓ la scansione deve includere la memoria dei processi in esecuzione e se possibile tutti i supporti rimovibili connessi.
- all'atto dell'installazione e configurazione del sistema operativo e/o del software applicativo devono essere seguite delle procedure di hardening del sistema che prevedono tra l'altro la modifica delle credenziali presenti di default;
- il sistema operativo e i software applicativi presenti nei sistemi devono essere aggiornati con le patch di sicurezza rilasciate dai relativi fornitori di cui deve essere accertata la compatibilità con l'operatività dei sistemi stessi. L'installazione delle patch di sicurezza rilasciate deve essere pianificata tenendo conto della gravità della vulnerabilità che viene risolta dalla patch e delle esigenze operative del Gruppo;
- ogni vulnerabilità o patch riscontrata deve essere adeguatamente analizzata e valutata dal punto di vista degli impatti che può avere sugli asset interessati, con l'attribuzione della priorità di intervento in condivisione con le strutture di sicurezza preposte;
- qualora non sia possibile installare gli aggiornamenti deve essere tenuto traccia delle patch non installate e della motivazione per la quale non si è proceduto all'installazione.

Le verifiche effettuate sul software acquistato, sulle nuove versioni e sulle patch di sicurezza devono prevedere almeno i seguenti controlli di sicurezza:

- eventuale presenza di virus o altro codice malevolo sui supporti di memorizzazione contenenti il software;
- test di vulnerabilità per individuare eventuali falle di sicurezza;
- test per assicurarsi che non si presentino incompatibilità che provocano un impatto negativo sulle operazioni dell'organizzazione o sulla sicurezza.

Le verifiche e i controlli di sicurezza effettuati e i relativi esiti devono essere opportunamente documentati.

3.9.3 Norme di sicurezza per lo sviluppo sicuro del codice

Le funzionalità di sicurezza del software devono garantire la riservatezza, l'integrità e la disponibilità dei dati e delle informazioni elaborate in base al relativo livello di criticità. Il software deve offrire funzionalità di tracciamento degli eventi di sicurezza e loro consultazione.

Deve essere implementato un modello di controllo degli accessi al software, alle sue funzionalità e ai dati elaborati.

Nella fase di sviluppo del software devono essere considerate le indicazioni di sicurezza relative alla specifica piattaforma/linguaggio di programmazione utilizzato. In particolare:

- nella fase di sviluppo del software non devono essere utilizzati codici già sviluppati (API, moduli, macro, ecc.) affetti da vulnerabilità note o ritenuti non sicuri;
- il software deve prevedere controlli sulla validità dei dati in ingresso, che devono essere conformi alla tipologia, al formato e al contenuto previsto;

- il software deve essere implementato in modo da prevenire eccezioni non gestite in fase di esecuzione;
- in caso di errore durante l'esecuzione del software devono essere visualizzati all'utilizzatore messaggi generici (laddove possibile), privi di dettagli tecnici che possano fornire informazioni sulle tecnologie utilizzate e sull'architettura del software, tali da mettere a repentaglio la sicurezza;
- devono essere definite procedure e controlli per verificare la presenza di codice potenzialmente dannoso o vulnerabile nelle applicazioni;
- il software deve garantire la separazione delle funzionalità di amministrazione da quelle dell'operatività ordinaria. Le funzionalità di amministrazione devono essere accessibili a seguito di un processo di identificazione, autenticazione e autorizzazione specifico;
- eventuali connessioni a database devono avvenire attraverso accessi seguendo il principio della separazione dei compiti e del minimo privilegio necessario allo svolgimento delle operazioni;
- nel codice sorgente del software (inclusi eventuali commenti al codice) non devono essere memorizzate informazioni riservate, intese come dati personali/sensibili, dati critici per il Gruppo e/o informazioni la cui divulgazione può avere impatti sulla sicurezza.

3.10 GESTIONE DI EVENTI E INCIDENTI DI SICUREZZA INFORMATICA

Il processo di gestione degli incidenti definisce le modalità di gestione degli eventi che impattano sulla normale esecuzione delle attività aziendali. Obiettivo primario del processo è ripristinare la normale operatività nel minor tempo possibile e di minimizzare l'impatto sulle attività operative degli utenti del sistema informativo, indirizzando in maniera tempestiva e opportuna gli incidenti. Devono essere inoltre raggiunti i seguenti obiettivi:

- assicurare la notifica tempestiva al management aziendale dell'apertura e chiusura di ogni evento rilevante;
- salvaguardare il patrimonio aziendale;
- individuare rapidamente una situazione di emergenza, attuando le strategie più adatte per contenerne le conseguenze;
- ridurre il più possibile i falsi allarmi (denominati "falsi-positivi") individuando con certezza le circostanze dell'emergenza;
- raccogliere le informazioni necessarie (evidenze) per supportare un'eventuale azione legale;
- conformarsi alle best practice del settore ed alle normative vigenti;
- analizzare l'accaduto individuando gli errori, le debolezze e le strategie adottate per gestirlo, migliorando la tempestività di intervento e la risposta ad analoghi eventi futuri.

La segnalazione di errori o incidenti di sicurezza IT deve essere sufficientemente tempestiva in modo da mettere in atto le opportune contromisure e limitare i danni. Deve pertanto essere definito e attuato un processo per definire le modalità di rilevazione, classificazione, gestione, trattamento e risoluzione degli incidenti informatici, determinati dal verificarsi di eventi in grado di compromettere una o più caratteristiche di sicurezza in termini di riservatezza, integrità e disponibilità delle informazioni trattate dai sistemi IT.

Tale processo deve includere la definizione dei ruoli e responsabilità nella segnalazione, l'escalation, il contenimento e l'eliminazione della minaccia.

Per ottenere una corretta gestione degli incidenti IT, in primo luogo devono essere identificati e categorizzati gli eventi critici possibili, quali:

- indisponibilità di servizi;
- malfunzionamento o sovraccarico dei sistemi;
- variazione non autorizzata delle configurazioni dei sistemi;
- malfunzionamento/rottura hardware;
- furto;
- perdita di dati;
- violazione di policy e procedure aziendali;
- violazione di normative cogenti;
- violazione delle infrastrutture fisiche;
- violazione degli accessi.

Dopo il ritorno alla normale operatività deve essere predisposta la documentazione dell'incidente e della sua soluzione e devono essere analizzate le cause che hanno prodotto l'incidente, individuando eventuali vulnerabilità per evitare successivi eventi analoghi.

È necessario, inoltre, che tale processo assicuri la corretta raccolta, gestione e storicizzazione delle evidenze e delle principali informazioni, sia per necessità di analisi interna aziendale che, se del caso, per esigenze investigative e/o legali.

Il management aziendale deve essere periodicamente informato con una sintesi degli incidenti di sicurezza rilevanti occorsi nel periodo.

3.11 GESTIONE DELLA CONTINUITÀ OPERATIVA

La gestione della continuità operativa prevede la predisposizione di un piano di emergenza in grado di assicurare la continuità delle operazioni vitali in presenza di eventi che compromettono le funzionalità del sistema informativo, al fine di garantire il ritorno in tempi accettabili alla normale operatività. Tale processo prende input da:

- identificazione dei rischi (ad esempio disastri naturali, indisponibilità dei sistemi IT, ecc.) condotta attraverso attività di Risk Assessment al fine di determinare l'impatto di eventuali interruzioni a causa di eventi disastrosi;
- definizione dei processi critici, attraverso l'analisi di impatto sul business (BIA) che valuta i processi/sistemi aziendali in funzione della loro criticità e fornisce la stima del tempo massimo di indisponibilità sostenibile.

Una delle componenti fondamentali per la gestione della continuità operativa è il Piano di Disaster Recovery (DRP). Tale piano deve considerare gli eventi disastrosi in grado di provocare un danno rilevante nella continuità dei servizi informatici al fine di definire le modalità di riattivazione dei servizi IT ritenuti critici nei tempi di ripristino accettabili. Gli elementi presi in esame dal DRP sono costituiti dalle risorse del sistema informatico tra cui hardware, software, collegamenti, basi di dati, personale IT, documentazione, sito alternativo e organizzazione.

Vengono riportati di seguito i requisiti principali per lo sviluppo, la gestione e la manutenzione di un piano di continuità operativa:

- coinvolgimento dell'Alta Direzione nella predisposizione del piano;
- identificazione dei processi critici, per i quali devono essere garantite elevati livelli di continuità;
- identificazione del personale interno / esterno da coinvolgere nel piano poiché per ogni persona o gruppo coinvolto nell'erogazione del servizio dovrà essere indicato il ruolo e la responsabilità individuale o di gruppo da essere ricoperta;
- identificazione e coinvolgimento di fornitori e controparti rilevanti;
- identificazione dei tempi di ripristino; deve essere formalmente dichiarato in quanto tempo (ore e giorni) sarà ripristinato il servizio;
- definizione delle strategie di ripristino adottate in funzione dell'evento e della tecnologia utilizzata;
- stesura delle procedure operative per il personale coinvolto;
- valutazione del tempo massimo per il quale il servizio potrà essere erogato;
- identificazione degli asset necessari al funzionamento del piano nei tempi stabiliti;
- modalità di ripristino dei dati (backup/restore);
- eventuale polizza assicurativa che copra i maggiori costi dovuti all'esercizio in emergenza e la perdita;
- identificazione di necessità logistiche in termini di spazi e posti lavoro per eseguire le operazioni considerate vitali per la continuità aziendale;
- linee guida per la conservazione dei documenti cartacei e dei supporti di memorizzazione;
- test del piano;
- formazione del personale;
- aggiornamento periodico del piano di continuità operativa.

3.12 CONFORMITÀ ALLE NORMATIVE

Deve essere assicurato il rispetto di leggi, politiche e normative aziendali che esprimono obblighi di sicurezza IT ed attuato un processo strutturato di audit per i sistemi IT. In particolare, deve essere realizzato un processo di IT Security Compliance che consenta di indirizzare e controllare nel tempo il mantenimento della conformità rispetto agli obblighi rilevanti di Sicurezza IT derivanti da:

- leggi nazionali e internazionali;
- direttive delle Autorità;
- regolamenti specifici di settore;
- requisiti di business;
- vincoli contrattuali;
- accordi di servizio;
- standard di riferimento.

Tale processo ha l'obiettivo di consentire all'azienda di gestire le esigenze di IT Security Compliance, come parte del processo di compliance management aziendale, individuando ed armonizzando gli obblighi di conformità, i requisiti e le misure di sicurezza. Il processo deve inoltre definire le esigenze di monitoraggio del mantenimento della conformità nel tempo tramite la realizzazione di procedure e strumenti atti ad eseguire le verifiche di conformità basate sulla raccolta e conservazione delle evidenze.

Per quanto concerne il servizio cloud, le società del Gruppo devono assicurarsi che il fornitore di servizi cloud preveda un processo di risposta alle richieste delle autorità (es. mandato di comparizione, indagini ufficiali o procedimenti legali) e rispettive modalità di condivisione di informazioni di supporto ad indagini e attività forense.

4 Glossario

Amministratore di sistema	La figura professionale incaricata della gestione e della manutenzione di un impianto di elaborazione e/o di suoi componenti.
Asset	Valore materiale e immateriale facente capo ad una proprietà.
Autenticazione	Processo attraverso il quale viene verificata la veridicità dell'identità dichiarata da un soggetto.
Backup	Copie di un insieme di dati effettuate con lo scopo di replicare le informazioni evitandone la perdita accidentale in caso di guasti o manomissioni.
Confidenzialità	Garanzia che i dati e le informazioni siano acceduti solo dal personale autorizzato.
Dato personale (ai sensi del Regolamento 679/2016 -GDPR)	Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
Disponibilità	Proprietà secondo cui un dato è sempre accessibile ed utilizzabile secondo i tempi ed i modi previsti.
Incidente	Evento indesiderato e/o imprevisti in ambito sicurezza che hanno una significativa probabilità di compromettere le operazioni, minacciando la sicurezza delle informazioni.
Integrità	Caratteristica di un dato rispetto alla propria autenticità e completezza.
Log	Registrazione cronologica di determinati eventi che si verificano su un sistema.
Minaccia	Possibile causa di un incidente indesiderato, che può provocare danni ad un sistema o organizzazione.
Segregation of Duties	Principio fondamentale all'interno del modello organizzativo-informatico aziendale. Le responsabilità devono essere definite e debitamente distribuite evitando sovrapposizioni funzionali o allocazioni operative che concentrino le attività su un unico soggetto in modo tale da evitare rischi operativi e/o eventuali conflitti di interesse.
Sistema Informatico	Installazione di Information Technology costituita da più componenti hardware e software in un contesto operativo noto e definito, finalizzato a soddisfare i requisiti di specifici gruppi di utilizzatori (ad esempio: un CED, una LAN, un PC o WS stand-alone, ecc.).
Terze Parti	Socio, Partner, Fornitore di servizi informatici, Cliente, Fornitore.