OpNet S.r.l.
Sede Legale Via Monte Rosa, 91 - 20149 Milano (MI)
PEC opnetwork@legalmail.it

opnet.it

CF/P.IVA 17502511003 **REA** MI-2738750
Capitale sociale EUR € 20.000,00 interamente versato

TLP: GREEN

TLP	Diffusione	Impatti	A chi condividere	Tipo di dato
CLEAR	• Documento ad uso *pubblico*	• La diffusione non comporta nessun impatto per OPNET	• A soggetti terzi	• Finanziario
GREEN	• Documento ad uso *interno*	• La diffusione non comporta nessun impatto per OPNET	• Ai partner e all'organizzazione	• Operativo
AMBER	• Documento ad uso *ristretto*	• La diffusione potrebbe avere impatti in termini di privacy, reputazione o deterioramento	• Solo all'organizzazione	• Personale
RED	• Documento ad uso *confidenziale*	• La diffusione potrebbe avere impatti in termini di privacy, reputazione o interruzione della normale operatività	• Solo ai destinatari	• Strategico

OpNet S.r.l.
Sede Legale Via Monte Rosa, 91 - 20149 Milano (MI)
PEC opnetwork@legalmail.it
opnet.it
CF/P.IVA 17502511003 **REA** MI-2738750
Capitale sociale EUR € 20.000,00 interamente versato

Politica per la Sicurezza delle Informazioni

Indice

1 SCOPO E CAMPO DI APPLICAZIONE

Il presente documento descrive la Politica aziendale adottata da Opnet per la sicurezza delle informazioni in conformità ai requisiti dello standard ISO/IEC 27001:2017 e risponde alla necessità di proteggere il patrimonio informativo della Società da tutte le minacce, interne o esterne, intenzionali o accidentali.

La presente Politica si applica all'intero patrimonio informativo e a tutte le strutture organizzative di Opnet nell'ambito del perimetro definito dal Sistema di Gestione della Sicurezza delle Informazioni (di seguito SGSI); l'attuazione è obbligatoria per tutto il personale interno e valevole per quello esterno.

Per questi ultimi, all'interno degli accordi contrattuali sono specificate le direttive adottate da Opnet da applicare ogniqualvolta trattino informazioni della stessa che rientrano nel campo di applicazione del SGSI.

2 RIFERIMENTI

- OpNet Intranet (disponibile al link: https://intranet.myopnet.way)
- Organigramma aziendale (disponibile al link: https://intranet.myopnet.way sezione risorse umane)
- D. Lgs. 231/2001 e s.m.i. - Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 20 settembre 2000 n. 300 e successive modifiche e integrazioni.
- Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/2001 (disponibile nella intranet aziendale, nella sezione "Modello 231").
- Codice Etico adottato dalla Società.
- Codice di Condotta per la prevenzione delle discriminazioni e la tutela della dignità delle donne e degli uomini del Gruppo.
- Policy Anticorruzione vigente
- Procedura Regolamento generale sulla protezione dei dati personali.
- GDPR: Regolamento (Ue) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE, entrato in vigore il 25 maggio 2018.
- D.Lgs. 196/03: Codice in materia di protezione dei dati personali così come modificato dal Decreto legislativo n.101/2018 emanato il 10 agosto 2018 ed entrato in vigore il 19

settembre 2018.

- ISO27001: 2017: Sistemi di gestione per la sicurezza delle informazioni – Requisiti.
- Politica di Cybersecurity Clean Desk.

3 TERMINOLOGIA E DEFINIZIONI

CEO: Chief Executive Officer.

Disponibilità: Attributo di sicurezza di una informazione, si realizza quando entità autorizzate possono accedere all'informazione e alle risorse associate nei tempi e nei luoghi previsti.

Integrità: Attributo di sicurezza di una informazione, si realizza quando sono salvaguardate l'accuratezza e la completezza dell'informazione e dei metodi per processarla.

Miglioramento continuo: Attività ricorrente mirata ad accrescere la capacità di soddisfare i requisiti.

Politica per la Sicurezza delle Informazioni: Obiettivi e indirizzi strategici di un'organizzazione, relativi alla gestione della sicurezza delle informazioni, espressi in modo formale dal CEO.

Riservatezza: Attributo di sicurezza di una informazione, si realizza quando l'informazione non è accessibile o divulgata ai soggetti (individui, entità, processi) non autorizzati, garantendone la confidenzialità.

Risorse informative: Collettivamente, l'insieme delle Informazioni e delle risorse di varia natura (tecnologiche, informatiche, organizzative, ecc.) che concorrono al loro trattamento.

Sicurezza delle Informazioni: Mantenimento dei requisiti di riservatezza, integrità e disponibilità delle informazioni oltre al coinvolgimento di altre proprietà quali l'autenticità, il non ripudio e l'affidabilità.

Sistema di Gestione della Sicurezza delle Informazioni (SGSI): Sistema di gestione adottato da Opnet in conformità alla normativa ISO/IEC 27001 di riferimento, basata su un approccio rivolto al rischio relativo al business e volta a stabilire, attuare, monitorare, riesaminare e migliorare la sicurezza delle informazioni.

Statement Of Applicability (SOA): Dichiarazione di applicabilità documentata che descrive gli obiettivi di controllo e i controlli pertinenti e applicabili al SGSI dell'Organizzazione.

4 DISTRIBUZIONE

Copia di questa procedura è data in distribuzione a tutte le risorse e messa a disposizione sulla intranet aziendale.

5 POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

Il dipartimento Information Security Office, responsabile del sistema di gestione, è costantemente impegnato nel miglioramento del SGSI adottato, nell'emissione e nell'aggiornamento della Politica per la Sicurezza delle Informazioni e si impegna a mantenerne attiva la comunicazione a tutti i livelli dell'Organizzazione.

Allo scopo di garantirne nel tempo l'idoneità, l'adeguatezza e l'efficacia, la Politica aziendale per la Sicurezza delle informazioni è aggiornata in caso di variazione degli indirizzi di fonte normativa, dei requisiti di business aziendali e degli standard di riferimento in materia di Information Security e in relazione al miglioramento costante del Sistema di Gestione. La stessa può essere aggiornata anche a seguito dei risultati di precedenti riesami o in funzione dei cambiamenti organizzativi o, più in generale, dai cambiamenti che possono influenzare l'approccio dell'Organizzazione alla gestione della sicurezza delle informazioni.

Contribuiscono all'implementazione della presente Politica procedure specifiche e policy di dettaglio volte a disciplinarne i requisiti ivi previsti. La Politica si applica indistintamente a tutte le strutture organizzative e ai livelli dell'Organizzazione nell'ambito del perimetro definito nel campo di applicazione del SGSI. La sua attuazione è obbligatoria per tutto il personale e la comunicazione e la diffusione verso l'esterno è autorizzata solo per il corretto svolgimento delle attività aziendali che devono avvenire nel rispetto delle regole e delle norme cogenti.

5.1 Obiettivi di sicurezza

La salvaguardia del Patrimonio Informativo aziendale è una scelta strategica manageriale volta a consentire e favorire il raggiungimento degli obiettivi di business di Opnet attraverso:

- la tutela delle risorse informative, nel rispetto dei principi di riservatezza, integrità e disponibilità venendo incontro ai requisiti delle parti interessate interne ed esterne;
- la garanzia dell'erogazione del servizio;
- la garanzia della continuità operativa, prevenendo la non interruzione del business anche in condizioni estreme;

- la conformità alle disposizioni normative (nazionali, internazionali e specifiche per le diverse aree di business di Opnet), in materia di sicurezza del patrimonio informativo e di cybersecurity;
- la gestione delle minacce che gravano sulle informazioni e sui sistemi di Opnet.

Gli obiettivi di sicurezza espressi nella presente politica fanno riferimento alla necessità di contenere, entro limiti accettabili predefiniti, il rischio di compromissioni della riservatezza, dell'integrità e della disponibilità delle risorse informative nonché della riservatezza dei dati memorizzati, trattati o trasmessi mediante l'utilizzo delle risorse informatiche stesse.

Sulla base della determinazione del profilo di rischio, in caso di superamento dei limiti di accettabilità definiti, il framework di analisi e gestione del rischio informatico adottato in Opnet prevede l'individuazione delle opportune misure di trattamento al fine di ridurre il rischio riportandolo entro i limiti di accettabilità e costruendo un sistema di contromisure tale da non poter essere eluso, se non intenzionalmente.

Tali contromisure organizzative, tecniche e operative sono distribuite su diversi livelli, secondo il principio della defense in depth, così che un'eventuale debolezza o fallimento di una contromisura sia compensato dalla presenza di ulteriori contromisure, anche di diversa natura, per consentire un'adeguata protezione dell'intero sistema informativo.

In particolare:

- la tutela della riservatezza deve attuarsi mediante interventi idonei a contrastare il verificarsi di accessi non autorizzati alle risorse informative e ai dati memorizzati, trattati o trasmessi mediante l'utilizzo delle risorse informatiche o la diffusione non controllata dei dati stessi;
- la tutela dell'integrità deve attuarsi mediante interventi idonei a contrastare il verificarsi di modifiche non autorizzate o il danneggiamento del formato fisico e/o del contenuto semantico dei dati memorizzati, trattati e trasmessi mediante l'utilizzo delle risorse informatiche;
- la tutela della disponibilità deve attuarsi mediante interventi idonei a garantire, ai soggetti autorizzati, l'accesso alle risorse in tempi utili al compimento della propria missione ovvero la riduzione del rischio che l'accesso ai dati, alle informazioni e ai sistemi possa essere impedito ai soggetti autorizzati.

Tale sistema di gestione deve consentire di svolgere adeguatamente tutti i processi di prevenzione

e gestione dei rischi informatici e di sicurezza individuati in termini di:

- prevenzione delle minacce e degli attacchi, onde ridurre al minimo la possibilità del verificarsi di accessi non autorizzati, di perdite dell'integrità dei dati e di indisponibilità dei dati e/o dei sistemi/servizi funzionali ai loro trattamenti;
- identificazione degli eventi potenzialmente in grado di materializzare il verificarsi di un rischio alla sicurezza delle informazioni;
- individuazione dei requisiti di sicurezza (security by design) da prevedere per contrastare rischi specifici con impatto sulla riservatezza, integrità e disponibilità dei dati, sin dalle fasi di progettazione e sviluppo di nuovi servizi/soluzioni, anche in ambito cloud;
- monitoraggio della sicurezza delle nuove tecnologie;
- studio delle strategie emergenti per il trattamento dei rischi della sicurezza delle informazioni anche in ambito cloud;
- sensibilizzazione diffusa del personale – a ogni livello - sulle tematiche, sulle regole comportamentali e sulle politiche di Sicurezza Informatica adottate presso Opnet;
- registrazione e conservazione degli eventi verificatisi per la loro analisi anche ex post e delle informazioni a essi correlate anche a fini di accountability;
- reazione agli eventi di rischio, onde evitarne, contenerne o minimizzarne i danni;
- ripristino della situazione antecedente al verificarsi dell'evento;
- investigazione attraverso l'analisi degli eventi registrati per l'identificazione delle responsabilità e per la valutazione dei danni subiti.

La realizzazione e la conseguente gestione di tale sistema richiede l'indirizzamento di un insieme eterogeneo di interventi, di natura sia tecnologica che organizzativa, atti a garantire il raggiungimento e il mantenimento nel tempo dei livelli di sicurezza ritenuti adeguati secondo quanto definito nell'ambito del framework di gestione del rischio.

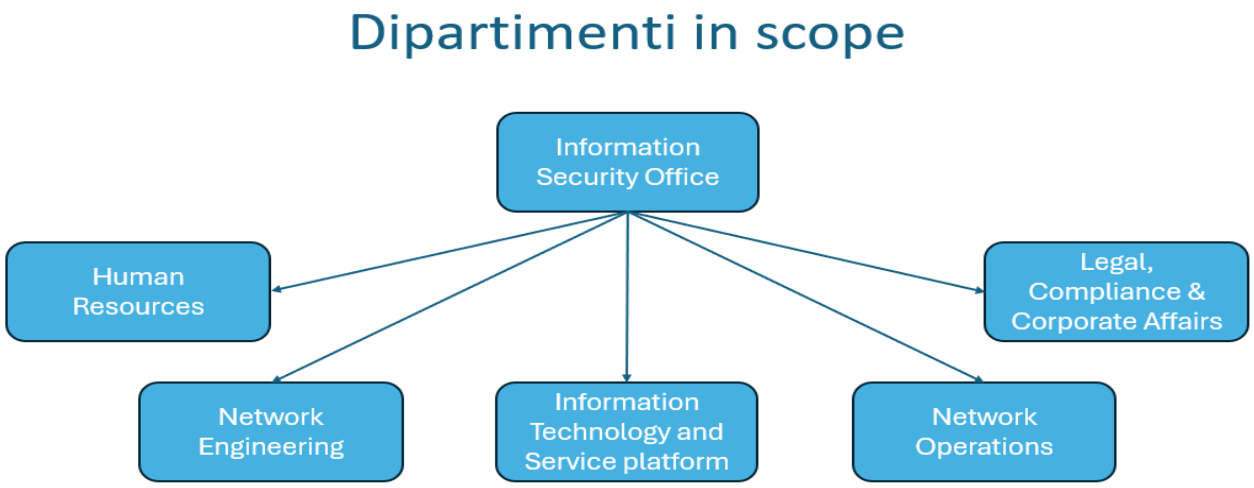
L'insieme di tali interventi si configura come un processo continuo di identificazione, analisi e valutazione dei rischi, nonché di selezione delle migliori strategie di prevenzione e gestione degli stessi, volto a consentire il governo complessivo della sicurezza del Patrimonio Informativo di Opnet.

Inoltre, al fine di garantire un opportuno livello di assurance circa l'adeguatezza delle misure di trattamento del rischio implementato e, ancor più in generale di tutto il sistema di gestione della Sicurezza delle Informazioni, sono posti in atto dei processi correlati di monitoraggio, di audit interni, di gestione degli eventi rilevanti ai fini della sicurezza e degli incidenti, nonché verifiche e audit di terza parte funzionali all'avvio e al mantenimento dei processi di certificazione in base agli

standard internazionali di riferimento in modo da intraprendere le opportune azioni di rimedio anche nell'ottica del miglioramento continuo.

5.2 Ruoli e Responsabilità

Devono essere definiti ruoli e responsabilità per la sicurezza delle informazioni in maniera completa ed esaustiva così da assicurare il conseguimento degli obiettivi prefissati; la struttura dell'organizzazione è rappresentata all'interno del sistema di gestione con il supporto di strumenti operativi di condivisione dei ruoli e delle responsabilità quali ad esempio organigrammi aziendali, in cui sono tracciati i ruoli dei soggetti che vi operano, organigrammi, comunicazioni organizzative nonché descrizione dei processi in cui sono delineate le relative responsabilità.



6 IL SISTEMA NORMATIVO E ORGANIZZATIVO

Opnet ha definito e strutturato il sistema documentale di Sicurezza delle Informazioni aziendali che consente di istanziare e governare i processi e le attività inerenti alla protezione dei dati, delle informazioni aziendali e delle tecnologie e servizi ICT a supporto.

A partire dalla presente Politica per la sicurezza delle informazioni, tale sistema si sostanzia in Manuali illustrativi dei sistemi di gestione, Procedure, Documenti tecnici, oltre a comunicazioni organizzative:

- Manuali illustrativi dei sistemi di gestione – documenti redatti dai Responsabili dei sistemi di gestione aziendali in conformità agli standard internazionali di riferimento per rispondere agli specifici requisiti richiesti dalla norma.
- Procedure:
  - societarie - documenti normativi volti a declinare le modalità operative di dettaglio ovvero le peculiarità riferite ad uno specifico processo di Opnet.
- Documenti tecnici: descrizioni delle soluzioni tecniche, delle configurazioni, documenti di progetto.
- Comunicazioni organizzative - documenti interni volti a definire o a modificare la macrostruttura organizzativa, definirne le responsabilità nonché a comunicare disposizioni organizzative di carattere generale di notevole importanza oppure modificare l'articolazione e le aree di responsabilità delle strutture e nominare i relativi Responsabili dei livelli organizzativi successivi al primo. Possono avere come ulteriore oggetto iniziative e progetti speciali che vedono il coinvolgimento di diverse business unit aziendali.

6.1 Sicurezza delle risorse informatiche

6.1.1 Gestione delle risorse ICT

Tutte le risorse informatiche che supportano i trattamenti di dati e informazioni digitali contribuiscono al perseguimento degli obiettivi strategici dell'organizzazione e devono pertanto essere adeguatamente censite e classificate al fine di identificare i requisiti di protezione; deve essere predisposto e mantenuto sempre aggiornato l'inventario delle risorse informatiche (hardware e software) aziendali al fine di garantirne la appropriata protezione, in termini di integrità, disponibilità e riservatezza dei dati memorizzati, trattati o trasmessi, mediante l'implementazione di adeguati livelli di sicurezza definiti sulla base del loro valore (classificazione).

L'inventario deve comprendere:

- Informazioni: database, documentazione di sistema, manuali per l'utente, materiale per l'addestramento, procedure operative o di supporto, piani di continuità, ecc.;
- Risorse software: software di base e applicativo, strumenti di sviluppo, programmi di utilità, ecc.;
- Risorse hardware: apparecchiature informatiche, fisiche e/o virtualizzate (ad es. server, client - PC fissi e portatili - monitor, sistemi di backup e restore, ecc.), apparecchiature di comunicazione (ad es. router, fax, segreterie telefoniche, ecc.), supporti magnetici (ad es. nastri e dischi), altre apparecchiature tecniche (ad es. alimentazioni elettriche, unità di climatizzazione, mobili, ecc.);
- Punti di accesso esterni: siti web, applicazioni Internet, WIFI, accesso remoto e altre modalità attraverso le quali le terze parti e i dipendenti potrebbero accedere ai sistemi ICT interni;
- Location: i luoghi fisici ove sono custodite le informazioni, le risorse software e hardware e dove vengono effettuate le elaborazioni.

6.1.2 Utilizzo delle risorse informatiche

Il personale aziendale utilizza le risorse informatiche di proprietà di Opnet nei limiti del profilo autorizzativo assegnato in linea con il ruolo ricoperto e le mansioni assegnate, e per le finalità previste dalle procedure sulle dotazioni informatiche vigenti.

Tale utilizzo deve sempre ispirarsi ai principi di diligenza e correttezza che sono alla base di ogni atto o comportamento posto in essere nell'ambito del rapporto professionale, in coerenza con le vigenti previsioni normative.

Sono predisposte e diffuse idonee regole, rif. 1, per il personale aziendale contenenti indicazioni circa le modalità da osservare sul corretto utilizzo delle risorse informatiche nonché le responsabilità, anche civili e penali, derivanti in caso di inosservanza. Per il corretto utilizzo delle postazioni di lavoro si rimanda alla Policy di Clean Desk.

Devono essere predisposti opportuni allegati ai contratti con le terze parti che utilizzano le risorse informatiche di Opnet contenenti indicazioni e prescrizioni per il corretto utilizzo delle stesse e dei loro dispositivi che a questi si connettono in virtù degli accordi contrattuali.

6.1.3 Classificazione delle risorse informatiche

Le risorse informatiche utilizzate nell'ambito delle attività di Opnet devono essere tutelate e gestite

sulla base del loro valore, che viene valutato in termini di impatti conseguenti alla perdita della disponibilità, integrità e riservatezza delle informazioni da queste memorizzate, trattate o trasmesse.

Tutte le risorse informatiche devono essere classificate attribuendo alle stesse un grado di impatto e, quindi, una classe di rischio utile a determinarne il livello di protezione (rischio residuo).

Il personale interno o esterno che svolge attività lavorative al di fuori della sede di Opnet deve utilizzare esclusivamente le dotazioni aziendali assegnate (pc portatile, smartphone e VPN) attenendosi al rispetto di quanto riportato nelle procedure sulle dotazioni informatiche vigenti. L'assegnatario è tenuto a custodire tali strumenti con diligenza e a garantire la riservatezza delle informazioni aziendali come indicato in rif.1. Tuttavia, esistono possibilità di deroga in caso di necessità che Opnet comunicherà ai propri dipendenti con l'utilizzo di comunicati specifici.

Devono essere predisposte, per il personale interno, delle specifiche policy nella quale riportare le indicazioni e le prescrizioni a cui il dipendente deve attenersi durante lo svolgimento delle attività lavorative al di fuori delle sedi aziendali. Devono essere altresì predisposti specifici allegati ai contratti di servizio e/o fornitura tra Opnet e le terze parti che hanno necessità di accedere all'infrastruttura tecnologica sia dall'interno delle sedi Aziendali sia dal di fuori; tali contratti devono contenere indicazioni e prescrizioni per il corretto utilizzo delle risorse informatiche di Opnet e dei loro dispositivi utilizzati per svolgere l'attività oggetto degli accordi.

6.2 Sicurezza nella gestione del personale

SELEZIONE DEL PERSONALE

Tutto il personale aziendale, in particolare quello destinato a ricoprire ruoli all'interno dei processi di gestione della sicurezza e/o delle risorse ICT con profilo privilegiato di accesso a informazioni sensibili o a sistemi informativi critici, deve essere attentamente selezionato sulla base di criteri di fiducia, affidabilità e competenza, in modo da limitare il più possibile il rischio di integrare nell'organizzazione soggetti che possano aumentare il rischio di violazioni della sicurezza delle informazioni e delle risorse, cartacee e informatiche, utilizzate ai fini del trattamento delle stesse.

RESPONSABILITA' DEL PERSONALE

I rapporti e i comportamenti, a tutti i livelli aziendali, devono essere improntati a principi di onestà, correttezza, trasparenza, riservatezza, imparzialità, diligenza, lealtà e reciproco rispetto, in accordo

con quanto previsto dal Contratto Collettivo Nazionale di Lavoro e dal Codice Etico.

FORMAZIONE E AWARENESS

È necessario che vengano definiti opportuni programmi di formazione per sensibilizzare il personale aziendale sul tema della Sicurezza Informatica indirizzando le differenti esigenze del personale. I programmi di formazione devono essere finalizzati ad accrescere le competenze, la consapevolezza e il senso di responsabilità delle risorse umane, con particolare riferimento alle minacce di natura cyber e ai rischi informatici di sicurezza specifici per il ruolo.

6.2.1 Gestione delle terze parti

ACCESSO E UTILIZZO DELLE RISORSE INFORMATIVE

È necessario garantire la sicurezza delle Risorse Informatiche aziendali, ivi compresi i dati e le informazioni trattate, accedute e utilizzate dai soggetti terzi (fornitori, consulenti, partner) ai fini dell'esecuzione degli specifici obblighi contrattuali e nei limiti dell'autorizzazione assegnata.

Al riguardo, devono essere predisposte specifiche politiche e procedure aziendali contenenti i criteri e le modalità per la gestione delle risorse informatiche da parte dei soggetti terzi, in conformità alle esigenze di business e alle normative vigenti.

Le politiche e le procedure devono risultare adeguate rispetto ai rischi, accidentali e/o intenzionali, di distruzione, perdita, divulgazione, alterazione e accesso non autorizzato delle risorse informatiche aziendali. All'interno delle stesse devono essere presenti indicazioni circa le modalità di corretto utilizzo delle risorse Informatiche nonché le responsabilità, anche giuridiche, derivanti in caso di inosservanza.

CLAUSOLE CONTRATTUALI

Devono essere previste specifiche clausole e procedure per garantire: la riservatezza e la non-divulgazione delle informazioni aziendali, il rispetto della normativa vigente e la tutela dei diritti di proprietà intellettuale applicabili alle Risorse Informative accedute e utilizzate dai soggetti terzi (fornitori, consulenti, partner).

Tali accordi devono necessariamente contemplare tutti i requisiti aziendali definiti per assicurare la protezione delle Risorse Informative.

6.3 Sicurezza fisica e ambientale

Tutte le risorse informatiche di Opnet, custodite e gestite presso le proprie sedi o presso sedi di terze parti ivi compresi sedi dei Cloud Service provider, devono essere protette dai rischi di accesso non autorizzato, sottrazione, manomissioni e danneggiamento derivanti da minacce di tipo fisico e ambientale anche attraverso specifiche clausole contrattuali.

6.3.1 Sicurezza delle aree

Il perimetro di sicurezza fisico delle aree tecniche (sedi e datacenter che ospitano sistemi ICT di Opnet) deve essere chiaramente definito e protetto.

Tutte le uscite di sicurezza del perimetro devono essere allarmate e tenute chiuse ovvero non apribili dall'esterno previo utilizzo di apposite chiavi. Le stesse uscite, se rientranti nel piano di evacuazione, devono essere munite di appositi presidi che ne consentono l'apertura dall'interno senza l'utilizzo di chiavi, secondo quanto previsto dalla vigente normativa in materia di sicurezza nei luoghi di lavoro.

Quando non presidiate, le aree devono essere tenute chiuse e controllate periodicamente.

6.3.2 Controllo degli accessi

L'accesso fisico alle strutture aziendali deve essere controllato e consentito solo al personale previamente identificato e autorizzato.

Il personale che fornisce servizi di supporto e di manutenzione è autorizzato all'accesso nelle aree laddove necessario e in maniera limitata (anche temporalmente).

I visitatori delle aree (ad esempio i dipendenti di imprese esterne e/o i consulenti) devono essere preventivamente identificati e registrati agli ingressi e alle uscite delle sedi aziendali. Il loro accesso deve essere consentito solo per i compiti specifici e limitati alle attività di competenza.

I diritti di accesso devono essere regolarmente verificati e revocati al personale aziendale o agli esterni (dipendenti di imprese esterne e/o consulenti) che lasciano gli incarichi per i quali era previsto l'ingresso alle aree stesse.

6.3.3 Sicurezza degli uffici, delle stanze e degli strumenti di lavoro

L'accesso agli uffici e alle stanze deve essere consentito solo al personale aziendale autorizzato e ai dipendenti di società esterne e/o ai consulenti preventivamente identificati, registrati e autorizzati

agli ingressi della sede aziendale.

Gli strumenti di lavoro devono essere fisicamente e logicamente protetti dai rischi di accesso non autorizzato e/o da conseguenti manomissioni o furti.

Devono essere predisposte idonee procedure organizzative per la regolamentazione e il controllo degli accessi agli strumenti da parte del personale autorizzato alla gestione/manutenzione degli stessi.

6.3.4 Protezione minacce esterne e ambientali

Presso le sedi Opnet e presso i Datacenter che ospitano sistemi, ivi compresi quelli dei Cloud Service provider, devono essere progettati e implementati idonei sistemi di sicurezza fisica, in funzione della rilevanza delle attività e dei dati gestiti, per la protezione delle aree, degli uffici, delle stanze e degli impianti dai danni derivanti da incendi, allagamenti, esplosioni, azioni terroristiche e altre forme di disastro naturale o umano. Qualora necessario le misure di protezione in oggetto devono essere inserite in specifiche clausole contrattuali che vincolano le terze parti alla loro implementazione, manutenzione e verifica costante.

I sistemi di sicurezza adottati devono essere regolarmente verificati e manutenuti.

Devono essere predisposte idonee procedure organizzative per la regolamentazione e il controllo dell'accesso ai sistemi da parte del personale autorizzato alla gestione/manutenzione degli stessi.

6.3.5 Lavoro in aree sicure

Devono essere progettati e implementati idonei sistemi di sicurezza fisica per la protezione e il controllo delle aree sicure (centri elaborazione dati e laboratori); in particolare devono essere attuati controlli fisici volti a prevenire l'accesso alle aree sicure da parte del personale non autorizzato.

Devono essere definite procedure organizzative per la gestione dell'accesso alle aree sicure da parte del personale aziendale, dei dipendenti di imprese esterne e/o dei consulenti.

Devono essere, altresì, definite linee guida e policy per la regolamentazione delle attività lavorative e dell'utilizzo delle risorse informatiche all'interno delle aree sicure.

6.3.6 Sicurezza delle aree di carico e scarico

Le aree di carico e scarico merci, laddove necessarie, devono essere controllate e isolate dagli ambienti operativi e di elaborazione delle informazioni.

Le porte di accesso alle aree di carico e scarico devono essere allarmate e sorvegliate. L'accesso alle aree di carico e scarico deve essere limitato al personale interno e esterno previamente identificato e autorizzato.

Tutto il materiale in uscita e in arrivo deve essere sempre registrato all'entrata del sito. Il materiale in arrivo deve essere sempre esaminato prima di venire trasportato dall'area di carico e scarico al punto di utilizzo.

6.3.7 Equipaggiamento di sicurezza

Tutti i locali tecnici aziendali devono essere dotati di equipaggiamento di sicurezza come rilevatori di fumo, allarmi antincendio, controllo delle temperature, attrezzature per l'estinzione e uscite di sicurezza, sistemi antiallagamento, sistemi di protezione dalle interferenze nella fornitura elettrica e radiazioni elettromagnetiche.

Tali equipaggiamenti devono essere controllati periodicamente per accertarne lo stato di conservazione e l'efficienza seguendo le istruzioni dei costruttori e dei responsabili preposti.

Tutte le informazioni sulla collocazione degli equipaggiamenti devono essere riportate su planimetrie opportunamente dislocate all'interno dei locali.

Tutto il personale aziendale che opera in tali locali deve essere istruito all'uso di tali equipaggiamenti. Le procedure di emergenza devono essere documentate e regolarmente testate.

6.3.8 Sicurezza del cablaggio

È necessario proteggere la linea elettrica e il cablaggio della rete informatica da minacce di tipo fisico, ambientale e organizzativo, pertanto, presso le sedi Opnet e presso i datacenter che ospitano sistemi Opnet, ivi compresi quelli dei Cloud Service provider, il cablaggio relativi alla rete informatica deve essere collocato in posizione priva di rischi dovuti a perdita di fluidi e/o disturbi elettromagnetici indotti da altri sistemi e tale da consentirne un'agevole e sicura manutenzione.

Deve essere garantita la protezione fisica dei cavi di dorsale, dei cavi orizzontali e dei locali tecnici.

6.4 La sicurezza nella gestione dei sistemi

Opnet deve garantire la sicurezza nei processi interni ed esterni di gestione dei propri sistemi informatici a supporto della gestione dei dati e delle informazioni.

6.4.1 Procedure operative e responsabilità

Le procedure operative inerenti ai processi di gestione dei sistemi informatici aziendali devono essere documentate, classificate, manutenute e rese facilmente disponibili a tutto il personale incaricato di attuarle.

Qualsiasi modifica inerente i sistemi e gli strumenti di gestione delle informazioni deve essere autorizzata, controllata e documentata.

Le responsabilità del controllo devono essere affidate a strutture o a personale esterno alle aree operative onde ridurre le opportunità di modifiche non autorizzate o accidentali e manomissioni delle risorse informative aziendali.

Gli ambienti di non produzione e quelli di produzione devono essere separati, ovvero segregati, al fine di ridurre al minimo i rischi di accessi o modifiche non autorizzate o anche accidentali dei sistemi operativi.

6.4.2 Insourcing

In caso di insourcing, deve essere garantita la sicurezza dei processi di gestione dei sistemi informatici aziendali. In particolare, le informazioni, i documenti, i dati e le conoscenze sono acquisite, usate o comunicate solo da personale autorizzato in considerazione del ruolo ricoperto oppure specificatamente incaricato.

Devono essere definiti contrattualmente con l'insourcer, in accordo con i requisiti, le procedure e le istruzioni di sicurezza aziendali, i controlli da attuare, i livelli di servizio da rispettare per garantire una adeguata protezione delle Risorse Informative, nonché le relative responsabilità, anche giuridiche, derivanti in caso di inosservanza.

Inoltre, l'insourcer dovrà essere informato sulle politiche, le procedure e le istruzioni di sicurezza aziendali relativamente al tipo di attività che dovrà svolgere in Opnet.

La conformità dell'operato dell'insourcer rispetto alle condizioni contrattuali definite deve essere regolarmente verificata e documentata.

6.4.3 Software non autorizzato

È vietato, nell'ambito del perimetro tecnologico di Opnet, l'utilizzo di software non espressamente autorizzato. Tale prevenzione mira a garantire da un lato gli adeguati livelli di sicurezza interni, dall'altro a osservare le normative di riferimento sui diritti di proprietà intellettuale.

Il software installato sui sistemi informativi deve essere conforme ai brevetti e/o ai termini delle

licenze (vincoli d'uso) e utilizzato esclusivamente per finalità lavorative.

Al riguardo è necessario impedire l'incauto prelievo di software e/o di file da computer e/o siti remoti e/o la loro installazione non autorizzata in computer aziendali. Tutto il personale deve essere reso consapevole dei danni potenziali arrecati alle risorse informatiche aziendali dall'introduzione di software non autorizzati.

Devono essere definite idonee procedure di sicurezza e implementati strumenti per la prevenzione e l'individuazione di software non autorizzato nel sistema informatico nonché per il ripristino delle risorse eventualmente danneggiate.

6.4.4 Outsourcing

Nel caso di affidamento in outsourcing della gestione dei processi e dei sistemi aziendali, deve essere garantita l'adeguata Sicurezza delle informazioni oggetto di tali servizi/attività.

Devono essere definiti contrattualmente con l'outsourcer, in accordo con le politiche, le procedure di sicurezza aziendali nonché le normative cogenti, i controlli da attuare per assicurare un adeguato livello di protezione delle informazioni trattate, i livelli di servizio da garantire ai fini della continuità operativa, nonché le relative responsabilità, anche giuridiche, derivanti in caso di inosservanza.

Inoltre, l'outsourcer dovrà essere informato sulle politiche, le procedure e le istruzioni di sicurezza aziendali relativamente al tipo di attività che dovrà svolgere in Opnet.

6.4.5 Protezione da malware

L'integrità delle informazioni e delle risorse informatiche deve essere preservata dalla possibile compromissione da parte di malware.

Tutto il personale deve essere reso consapevole dei danni potenziali arrecati alle risorse informatiche aziendali dall'introduzione di malware.

Devono essere definiti idonei requisiti e procedure di sicurezza e implementati strumenti per la prevenzione, il monitoraggio e l'individuazione di malware nel sistema informatico nonché per il ripristino delle risorse eventualmente danneggiate.

I programmi antivirus e gli strumenti di protezione anche automatizzati, devono essere gestiti e controllati in maniera tale da assicurarne una capillare diffusione e un frequente aggiornamento.

Devono essere definite idonee procedure atte a gestire e contenere gli eventi dannosi (isolamento,

ripristino) e a fornire supporto agli utenti coinvolti.

6.4.6 Protezione dei sistemi informatici

I sistemi informatici devono essere opportunamente aggiornati ("patching"), in tutti gli ambienti, inclusi quelli di non produzione, in maniera tale da non essere esposti da eventuali difetti di sviluppo o vulnerabilità emergenti. Tuttavia, per i sistemi di non produzione, in cui l'esposizione ai rischi è bassa è consentito prevedere dei tempi di aggiornamento meno stringenti.

L'adeguatezza dei processi di hardening e patching deve essere periodicamente verificata mediante attività di vulnerability assessment dei sistemi e/o penetration test.

I dati classificati, in funzione del livello di impatto complessivo, come medio o superiori (dati di transazioni e/o dati ricadenti nell'ambito privacy) presenti negli ambienti di produzione non devono essere replicati su ambienti degradati (non di produzione) ma devono essere offuscati ovvero soggetti a processo di data masking al fine di garantirne la riservatezza e la compliance alle norme cogenti.

6.4.7 Back-up e restore

Devono essere previste, anche in conformità alle normative vigenti, adeguate politiche di back-up e restore per preservare l'integrità e garantire la disponibilità delle informazioni aziendali (ad esempio in caso di manomissioni, atti vandalici, contaminazione da malware, perdita o distruzione anche involontaria). La policy deve prevedere inoltre che le procedure di Back-up devono essere sottoposte periodicamente a verifica attraverso processi di restore al fine di garantirne l'efficacia e l'integrità del dato salvato.

6.4.8 Sicurezza della rete dati

La rete dati interna (cd "intranet") deve essere adeguatamente gestita e controllata. I sistemi e le applicazioni utilizzati nella rete devono essere mantenuti in sicurezza, incluse le informazioni in transito.

Tutte le attività di manutenzione devono essere tracciate e verificate. Gli aggiornamenti di sicurezza, i livelli di servizio e i requisiti per la gestione dei servizi di rete devono essere identificati e formalizzati in specifici accordi contrattuali sia per i servizi in insourcing che di outsourcing.

Le prestazioni della rete devono essere controllate per verificare la conformità della gestione ai parametri contrattualizzati.

6.4.9 Sicurezza nello scambio di informazioni

Devono essere predisposte opportune procedure e controlli per lo scambio di informazioni e di software tra le organizzazioni al fine di evitarne la perdita, la modifica o l'uso improprio. In particolare, è necessario:

- Prevedere controlli specifici a protezione del trasferimento delle informazioni, per tutte le tipologie di comunicazione.
- Formalizzare, in appositi accordi, i trasferimenti sicuri di informazioni tra l'organizzazione e le parti esterne.
- Proteggere le informazioni trasmesse attraverso messaggistica elettronica in modo appropriato in relazione al rischio di accesso non autorizzato, alterazione, violazione di riservatezza.
- Prevedere accordi di riservatezza o di non divulgazione (N.d.A.), in base alle necessità di proteggere le informazioni rilevanti per la sicurezza e il business di Opnet nei contratti e accordi con le terze parti.

Anche i dati critici per l'azienda contenuti nei messaggi elettronici devono essere protetti dai rischi di accesso non autorizzato, alterazioni o distruzione mediante l'adozione di idonei sistemi di sicurezza identificando specifiche regole e opportune policy e procedure operative.

6.4.10 Gestione dei supporti rimovibili

Devono essere definite procedure di sicurezza per l'utilizzo, il riutilizzo, la custodia e la dismissione dei supporti rimovibili, anche in conformità alle normative vigenti in materia di protezione dei dati personali.

I supporti rimovibili utilizzati per la conservazione delle informazioni devono essere protetti dai rischi di accesso non autorizzato e/o manomissioni.

6.4.11 Monitoraggio / log

Nell'ambito della gestione dei sistemi, degli apparati e dei meccanismi di sicurezza devono essere registrati gli eventi rilevanti, anche nel caso si utilizzino cloud provider, ai fini del monitoraggio e del rispetto della normativa cogente in materia.

La registrazione dei log degli eventi, delle attività degli utenti, delle eccezioni, dei malfunzionamenti e degli eventi relativi alla sicurezza delle informazioni deve essere effettuata, mantenuta e riesaminata periodicamente in funzione degli obiettivi definiti per le attività di monitoraggio.

In particolare, in conformità agli adempimenti normativi applicabili in materia, devono essere definite e implementate opportune registrazioni delle operazioni effettuate sui sistemi informatici (ad esempio i file di log) inerenti le attività degli utenti, e in particolar modo le attività svolte dagli Amministratori di Sistema (AdS) e dagli operatori che hanno privilegi amministrativi sui sistemi e sui DB, al fine di poter tracciare gli eventi che possono compromettere la sicurezza delle risorse informatiche e dei dati da queste trattati.

Le registrazioni devono essere memorizzate e conservate per un periodo di tempo ritenuto idoneo (anche in conformità alle normative vigenti) a supportare le attività di monitoraggio e verifica anche ex-post, garantendo la piena SOD ("Segregation of Duties") tra chi svolge attività IT (operation, sviluppo, ecc.) e chi svolge le attività di verifica, audit e sicurezza.

Devono essere previsti sistemi e servizi di monitoraggio della Sicurezza per verificare l'utilizzo dei sistemi informativi. Gli strumenti di monitoraggio devono essere protetti contro i rischi di accesso non autorizzato e/o di alterazione, garantendo l'integrità dei dati e dei log. I guasti e i malfunzionamenti devono essere tracciati e analizzati e devono essere intraprese opportune azioni correttive.

Le strutture per la raccolta dei log e le informazioni di log sono protette da manomissioni e accessi non autorizzati.

6.5 Controllo degli accessi logici

L'accesso alle risorse informatiche aziendali deve essere adeguatamente, autorizzato, protetto e controllato in conformità alle normative vigenti, con particolare riferimento a quelle in materia di protezione dei dati personali.

6.5.1 Iter autorizzativo per gli accessi alle risorse informative

Devono essere definiti e approvati specifici profili di autorizzazione per l'accesso da parte degli utenti ai dati e al sistema informatico (personale aziendale, nonché dipendenti di imprese esterne e/o i consulenti cui l'accesso è consentito per l'esecuzione degli specifici obblighi contrattuali).

I profili di autorizzazione devono consentire di individuare a quali informazioni l'utente può accedere nonché quali azioni può compiere. Al riguardo, le elaborazioni/operazioni devono essere limitate a quelle strettamente necessarie allo svolgimento delle mansioni assegnate, conformemente ai principi del "need to know", "need to do", "segregation of duties".

In particolare, l'accesso mediante le varie applicazioni ai dati e alle risorse necessarie dovrebbe essere ridotto al minimo indispensabile secondo il principio del "least privilege" e "need to know".

Ai dipendenti di imprese esterne e/o ai consulenti deve essere consentito l'accesso alle informazioni aziendali solo ed esclusivamente in funzione del proprio incarico. Devono essere definite procedure di gestione e controllo del ciclo di vita dei profili di autorizzazione degli utenti (assegnazione, creazione, aggiornamento, disattivazione e revoca).

Devono essere inoltre definite specifiche politiche e procedure per l'assegnazione, la gestione e il controllo dei profili a elevati privilegi che prevedono, oltre ai requisiti descritti sopra, un'assegnazione formale del profilo, una verifica dell'affidabilità e delle competenze dell'assegnatario del profilo privilegiato e un monitoraggio periodico dell'utilizzo delle utenze con tali profili.

6.5.2 Gestione delle credenziali di accesso

Devono essere definite politiche e procedure per la gestione delle credenziali di accesso in conformità alle normative vigenti, con particolare riferimento a quelle in materia di protezione dei dati personali.

Il codice identificativo (user-id) deve essere univoco, nominale e non assegnabile neppure in tempi diversi a utenti diversi.

6.5.3 Revisione dei diritti di accesso alle risorse informatiche

Tutti i diritti di accesso assegnati al personale aziendale, nonché ai dipendenti di imprese esterne e/o i consulenti cui l'accesso è consentito per l'esecuzione degli specifici obblighi contrattuali, devono essere regolarmente controllati e aggiornati, anche attraverso procedure automatizzate.

Deve essere prevista la modifica/disattivazione dei diritti d'accesso in caso di revisione/revoca dei profili autorizzativi assegnati (ad esempio a seguito della cessazione del rapporto lavorativo).

Devono essere adottati controlli e procedure di sicurezza in grado di revocare, tramite automatismi, i diritti di abilitazione degli utenti del sistema informatico, con particolare riferimento agli utenti che non sono più dipendenti aziendali e/o consulenti che non hanno più un contratto di lavoro attivo.

6.5.4 Responsabilità utente

Gli utenti sono responsabili della salvaguardia delle loro informazioni e strumenti di autenticazione. Devono essere definite idonee regole da attuare in merito alla scelta e all'utilizzo delle password e

sulle cautele per assicurarne la segretezza.

Devono essere formulate policy che definiscono le modalità per il corretto utilizzo delle postazioni di lavoro e degli strumenti informatici e telematici.

Il personale aziendale deve essere informato delle conseguenze, disciplinari e anche giuridiche, derivanti in caso di disapplicazione/violazione (volontaria o involontaria) delle policy.

6.5.5 Controllo degli accessi alla rete e relativi servizi

L'accesso alla rete e ai servizi di rete deve essere consentito solo al personale aziendale autorizzato nonché ai dipendenti di imprese esterne e/o i consulenti cui l'accesso è consentito per l'esecuzione degli specifici obblighi contrattuali.

Gli accessi devono essere monitorati e regolarmente verificati.

Devono essere adottati appropriati sistemi di autenticazione per il controllo degli accessi remoti alla rete e devono essere raccolti e analizzati i relativi log.

Devono essere controllati gli accessi fisici e logici per la diagnostica e la configurazione delle porte. Devono essere attuati idonei controlli atti a impedire l'accesso alla rete da parte di utenti non autorizzati.

6.5.6 Controllo degli accessi al sistema operativo

L'accesso ai sistemi operativi deve essere controllato da una idonea procedura di sicurezza.

L'accesso al sistema operativo deve essere consentito solo al personale aziendale autorizzato nonché ai dipendenti di imprese esterne e/o i consulenti cui l'accesso è consentito per l'esecuzione degli specifici obblighi contrattuali.

Gli accessi devono essere monitorati e regolarmente verificati.

Sono state definite procedure atte ad assicurare la creazione di codici per l'identificazione utenti (user-id univoche).

I sistemi devono essere configurati in modo da prevedere la chiusura automatica della sessione lavorativa dopo un periodo predefinito di inattività e la riattivazione della stessa solo previa autenticazione informatica.

I sistemi devono raccogliere gli eventi di accesso e i comandi che gli utenti eseguono su audit log,

questi devono essere acquisiti e conservati al di fuori dei sistemi che li hanno generati al fine di prevenire eventuali azioni di compromissione degli stessi volti a eliminare le tracce dell'operato degli utenti.

6.5.7 Controllo degli accessi a dati e applicazioni

L'accesso ai dati e alle applicazioni deve essere limitato al solo personale aziendale autorizzato nonché ai dipendenti di imprese esterne e/o i consulenti cui l'accesso è consentito per l'esecuzione degli specifici obblighi contrattuali.

Devono essere definite regole di "segregation of duties" da verificare periodicamente, e gli accessi devono essere monitorati e regolarmente verificati.

Devono essere definite idonee procedure e controlli di sicurezza per proteggere le informazioni e le applicazioni dai rischi derivanti dall'utilizzo di computer portatili e di strumenti di comunicazione.

Nel caso in cui si utilizzino soluzioni per il telelavoro devono essere definite e attuate specifiche politiche e procedure di sicurezza.

6.6 Acquisizione, sviluppo e manutenzione dei sistemi informatici

L'acquisizione, lo sviluppo e la manutenzione dei sistemi deve garantire la protezione delle informazioni da errori, perdite, modifiche non autorizzate o alterazioni.

Devono essere definite politiche e procedure per la gestione dei cambiamenti e linee guida per lo sviluppo sicuro per i sistemi informativi di Opnet al fine di implementare un modello di governance dei cambiamenti che comprenda i principi di "Security by Design" e "Privacy by Design" e garantire che i requisiti di sicurezza siano parte integrante dei processi di acquisizione, evoluzione e mantenimento dei sistemi informativi.

6.6.1 Requisiti di sicurezza dei sistemi

L'acquisizione e lo sviluppo di nuovi servizi/applicazioni/sistemi da parte di Opnet e l'aggiornamento di quelli esistenti devono includere, in accordo con i requisiti di business e le politiche di sicurezza aziendali, la definizione di specifici requisiti, controlli di sicurezza e gli standard di sviluppo sicuro previsti aziendalmente.

I sistemi e le applicazioni devono essere protetti in modo da impedire errori, perdite, modifiche non autorizzate o alterazioni non autorizzate delle informazioni.

Tutte le misure di sicurezza definite e applicate per i sistemi e le applicazioni devono essere sottoposte a test per garantire la loro robustezza ed efficacia.

6.6.2 Crittografia

Al fine di garantire la protezione della sicurezza delle informazioni è necessario garantire un uso corretto ed efficace della crittografia.

Devono essere definite procedure di gestione del ciclo di vita delle chiavi in conformità alle vigenti normative nazionali e agli standard internazionali in materia.

Nell'ipotesi di trasferimento dei dati deve essere garantita la:

- **Cifratura dei canali di autenticazione:** per la protezione delle credenziali utente in transito, devono essere implementati canali cifrati di comunicazione, eventualmente implementati anche tramite l'utilizzo di certificati self-signed emessi da una Certification Authority interna Opnet. Tali certificati digitali utilizzano chiavi crittografiche RSA.
- **Cifratura canali web**: per la protezione dei dati in transito su web, devono essere implementati canali cifrati di comunicazione, tramite l'utilizzo di protocolli sicuri.

In particolare:

- in caso di servizi accessibili da Internet, devono essere utilizzati certificati pubblici emessi da una Certification Authority Pubblica. Tali certificati devono essere basati su una crittografia RSA con chiavi di almeno 2048 bit.
- In caso di servizi accessibili solo dalla rete aziendale Intranet possono essere utilizzati certificati privati di tipo Self-Signed, emessi da una Certification Authority interna Opnet. Tali certificati possono utilizzare chiavi di tipo RSA di almeno 2048 bit.

- **Cifratura database:** In caso di specifiche necessità derivanti dalla tipologia dei dati trattati, devono essere utilizzati meccanismi nativi di cifratura dei dati su database.
- **Trasferimento dati e files:** Il trasferimento dei dati sia da e verso l'interno che da e verso l'esterno deve essere effettuato utilizzando protocolli sicuri, eventualmente basati su SSH (Secure Shell) e SFTP (Secure Shell File Transfer Protocol), tramite l'utilizzo dei pacchetti OpenSSL forniti nativamente dai sistemi operativi.

Per lo scambio di dati con business partner, ovvero partner non occasionali, Opnet dovrà far soluzioni con protocolli di sicurezza standard relativi al trasferimento dei dati (es. VPN). La soluzione deve prevedere controlli che garantiscano la riservatezza, l'integrità e la disponibilità dei flussi di dati trattati, deve permettere di profilare gli utenti in base a regole di segregation of duties e deve avere un adeguato sistema di registrazione degli eventi tale da garantire l'auditabilità e il non ripudio dei flussi ricevuti.

Il sistema dovrà anche prevedere la gestione di flussi cifrati al fine di garantire l'adeguato livello di sicurezza anche per i dati considerati riservati o confidenziali.

6.6.3 Sicurezza dei file di sistema

L'installazione del sistema operativo e l'aggiornamento dei firmware deve essere controllata e testata attraverso la predisposizione di idonee procedure.

I risultati del test devono essere controllati e conservati secondo le procedure in materia.

6.6.4 Sicurezza nei processi di change management

Tutte le modifiche apportate ai sistemi e alle applicazioni devono essere oggetto di un processo formale di change management che garantisca che le modifiche siano state correttamente ideate, testate, documentate e autorizzate, così da ridurre al minimo le alterazioni dei sistemi informativi e gestire le modifiche in modo controllato.

Sulla base delle modifiche effettuate e delle minacce alla sicurezza osservate, devono essere previste attività di Vulnerability Assessment periodici al fine di monitorare il mantenimento degli adeguati e previsti livelli di rischio. In fase di rilascio di modifiche ai sistemi devono essere preventivamente testate e previste specifiche procedure di rollback per il ripristino della situazione ex-ante in caso di problemi.

Devono essere definite idonee procedure e strumenti per il tracciamento delle modifiche e per la successiva verifica, soprattutto quando trattasi di modifiche effettuate in emergenza.

6.6.5 Sicurezza nella manutenzione dei sistemi informatici e patch management

Devono essere adottate procedure e misure per la regolamentazione delle attività di approvazione, autorizzazione e manutenzione dei sistemi. Le procedure devono definire:

- i criteri e le modalità per l'aggiornamento periodico dei prodotti utilizzati;
- la pianificazione e l'attuazione di interventi di manutenzione programmata (dismissione, sostituzione, ecc.);

- il collaudo dell'operatività dei sistemi dopo gli interventi di aggiornamento e manutenzione;
- l'aggiornamento della configurazione del sistema in funzione delle modifiche apportate all'ambiente.

Tutte le attività di manutenzione devono essere tracciate e regolarmente verificate.

6.7 Gestione degli incidenti

Devono essere identificati, classificati, gestiti e segnalati, in accordo con le normative nazionali e aziendali, gli incidenti rilevanti ai fini della Sicurezza Informatica.

Sono state definite procedure per la gestione e la comunicazione degli incidenti rilevanti ai fini della Sicurezza Informatica in conformità alle vigenti normative nazionali, di settore e aziendali e ai Service Level Agreement (SLA) concordati con il cliente interno, secondo le normative di riferimento.

Tali procedure descrivono le finalità, le modalità, i criteri di protezione, di utilizzo e i tempi di tenuta dei log rilevanti ai fini della ricostruzione degli incidenti.

Devono essere previste sanzioni disciplinari in caso di violazione volontaria o dolosa dei vincoli di sicurezza da parte del personale aziendale.

Devono essere, altresì, previste sanzioni in caso di violazione dei vincoli di sicurezza da parte dei dipendenti di imprese esterne e/o dei consulenti che accedono e utilizzano le Risorse Informative aziendali per l'esecuzione degli specifici obblighi contrattuali. I vincoli contrattuali per la comunicazione e gestione degli incidenti di sicurezza devono essere estesi anche ai provider dei servizi in cloud, sempre attraverso specifiche prescrizioni contrattuali.

6.7.1 Attività di verifica dello stato della sicurezza

Devono essere attuati processi mirati alla protezione dei sistemi aziendali dai rischi relativi alla Sicurezza Informatica finalizzati alla riduzione del grado di esposizione degli stessi a livelli coerenti con gli obiettivi di business e con le normative vigenti.

A tale fine devono essere definite e implementate attività periodiche di assessment sui sistemi, finalizzate all'identificazione delle minacce informatiche e delle vulnerabilità, e all'elaborazione di piani di remediation per il rientro delle stesse prevedendo almeno le seguenti iniziative:

- Vulnerability Assessment: attività di analisi delle caratteristiche tecniche delle

configurazioni e dei servizi attivi sui singoli host finalizzate al rilevamento sistematico di eventuali vulnerabilità presenti negli ambienti.

- Penetration Test: insieme di attività e tecniche basate sulla simulazione controllata delle strategie di attacco informatico atte a sfruttare le vulnerabilità presenti sui sistemi in esercizio.

6.8 Sicurezza dei servizi di cloud computing

Devono essere definiti i requisiti di sicurezza per la progettazione, l'implementazione e la gestione dei servizi di Cloud Computing erogati a Opnet da parte dei fornitori esterni (CSP),

Tali attività, infatti, devono essere condotte con modalità idonee a garantire il raggiungimento e il mantenimento nel tempo dei seguenti obiettivi generali di sicurezza:

- protezione del business aziendale;
- conformità alle vigenti normative nazionali;
- conformità alle norme settoriali, agli standard internazionali e alle linee guida di riferimento;
- conformità alle politiche di sicurezza aziendali in vigore.

In particolare, devono essere definiti i requisiti di sicurezza per le seguenti tipologie di erogazione dei servizi di Cloud Computing:

- SaaS - Software as a Service;
- PaaS - Platform as a Service;
- IaaS - Infrastructure as a Service.

Tali requisiti devono, inoltre, tener conto del livello di condivisione delle risorse e delle infrastrutture tra i soggetti che usufruiscono dei servizi di Cloud Computing, al fine di identificare le misure di sicurezza più adeguate. Nello specifico possono essere definiti i seguenti livelli di condivisione delle risorse e delle infrastrutture:

- Private Cloud;
- Public Cloud;
- Hybrid Cloud;
- Community Cloud.

Il Cloud Service Provider deve basarsi su infrastruttura e su servizi conformi, ovvero certificati dalla

Cloud Security Alliance (https://cloudsecurityalliance.org/).

Tutte le prescrizioni della presente politica che sono applicabili anche ai servizi in cloud acquisiti da Opnet devono essere concordate con il service provider all'interno degli specifici accordi contrattuali.

6.9 Gestione della continuità operativa aziendale

Deve essere garantita la continuità operativa aziendale per la gestione di situazioni di crisi conseguenti a incidenti di portata settoriale, aziendale o catastrofi estese che colpiscono Opnet, secondo livelli coerenti rispetto alle esigenze aziendali e alle norme vigenti.

A tale scopo, deve essere definito e implementato un piano di continuità operativa aziendale basato su un'appropriata identificazione dei sistemi maggiormente critici, delle potenziali minacce che possono realizzarsi su di essi e delle contromisure da adottare. Tale piano deve, quindi, descrivere i criteri, le procedure, le misure tecniche e organizzative e gli strumenti adottati per la gestione delle emergenze e per il ripristino delle condizioni operative antecedenti il verificarsi di un evento dannoso in conformità con i parametri RTO e PRO concordati.

Per garantirne l'efficacia nel tempo, il piano di continuità operativa deve essere testato e aggiornato con frequenza periodica e a fronte di rilevanti innovazioni organizzative, tecnologiche e infrastrutturali e nel caso in cui vengano riscontrate lacune e carenze e in tutti quelle situazioni in grado di generare nuovi rischi.

Roma, 01/08/2024

La Direzione