

Linee guida sulla qualità dei beni e dei servizi ICT per la definizione ed il governo dei contratti della Pubblica Amministrazione

Manuale operativo

Dizionario delle Forniture ICT

Classe di Fornitura

Gestione della sicurezza logica
SIL

INDICE

1.	GENERALITÀ SUL DOCUMENTO.....	4
2.	DESCRIZIONE DELLA CLASSE DI FORNITURA.....	4
3.	MODALITÀ DI DEFINIZIONE DELLA FORNITURA	5
3.1.	OBIETTIVI	6
3.2.	UTENZA	7
3.3.	DIMENSIONE, ARCHITETTURA E COMPLESSITÀ	7
3.4.	VINCOLI E REQUISITI.....	8
3.5.	RELAZIONE CON ALTRE CLASSI.....	8
3.6.	STANDARD E NORME.....	8
4.	MODALITÀ DI STIMA DEI COSTI ANCHE IN FUNZIONE DELLA QUALITÀ RICHIESTA	9
5.	DESCRIZIONE DELLE ATTIVITÀ E DEI PRODOTTI.....	10
5.1.	ANALISI DEI REQUISITI	ERRORE. IL SEGNALIBRO NON È DEFINITO.
5.2.	PROGETTAZIONE	13
5.3.	PROGETTAZIONE COLLAUDO	14
5.4.	REALIZZAZIONE DEL SERVIZIO	15
5.5.	AVVIAMENTO DEL SERVIZIO.....	15
5.6.	MONITORAGGIO DI SICUREZZA.....	16
5.7.	GESTIONE OPERATIVA DELLE EMERGENZE	17
5.8.	AGGIORNAMENTO	17
5.9.	RENDICONTAZIONE.....	18
5.10.	DESCRIZIONE DEI PRODOTTI.....	19

6.	DESCRIZIONE DEI PROFILI PROFESSIONALI COINVOLTI.....	22
7.	INDICATORI/MISURE DI QUALITÀ	28
8.	GLOSSARIO	38

1. GENERALITÀ SUL DOCUMENTO

Questo documento descrive uno dei lemmi del Manuale operativo “Dizionario delle forniture ICT” delle Linee guida sulla qualità dei beni e dei servizi ICT per la definizione ed il governo dei contratti della Pubblica Amministrazione. Ogni lemma del Dizionario rappresenta una classe di fornitura ICT elementare. Il Dizionario contiene tutte le classi di forniture che si sono ritenute necessarie per rappresentare compiutamente i contratti ICT delle pubbliche amministrazioni. Ogni lemma del Dizionario è autoconsistente e indipendente; esso prevede

- **la descrizione della classe di fornitura ICT elementare**, che ha lo scopo di definirne univocamente l'ambito di applicazione;
- **l'esplicitazione di “regole” per l'uso della classe di fornitura**, utile a proporre al lettore suggerimenti sull'uso del lemma per la stesura dell'oggetto contrattuale;
- **la descrizione delle attività** relative alla classe di fornitura e dei relativi prodotti, utile al lettore come traccia riutilizzabile per scrivere contratti e capitolati tecnici;
- **una tabella che riassume attività, prodotti e indicatori di qualità**, utile al lettore come quadro sinottico che riassume il legame tra attività e relativi prodotti da queste realizzati ed identifica, in relazione ad entrambi, gli indicatori di qualità adottati per la classe di fornitura;
- **una scheda per ogni indicatore di qualità** (presente nella tabella di cui sopra), utile al lettore come traccia riutilizzabile, per scrivere contratti e capitolati tecnici;
- **un glossario** (ove necessario) specifico per la classe di fornitura.

Nell'ambito della complessa attività di scrittura di contratti e capitolati tecnici, i lemmi possono essere intesi come “ricette contrattuali” di immediato utilizzo mediante processi di copia e incolla, per rappresentare le esigenze della stazione appaltante.

Nell'ottica del riuso, particolare attenzione dovrà essere prestata alle imprescindibili e necessarie attività di specificazione e taratura delle classi di fornitura ICT elementari utilizzate e, successivamente, all'integrazione delle diverse classi di fornitura scelte in un unico e coerente contratto ICT.

La versione digitale di ogni lemma è singolarmente scaricabile dal sito CNIPA in formato editabile (.doc) che ne permette il riutilizzo anche parziale.

Per maggiori informazioni sull'utilizzo integrato delle classi di fornitura e dei processi trasversali si rimanda agli esempi contenuti nel Manuale applicativo “Esempi di applicazione”.

2. DESCRIZIONE DELLA CLASSE DI FORNITURA

Un servizio di Gestione della Sicurezza Logica (SIL) realizza e gestisce le contromisure di tipo tecnologico volte alla difesa perimetrale e di contenuto del sistema informativo. Un sistema SIL è un insieme di servizi aventi lo scopo di:

- attuare la politica per la sicurezza ai flussi di rete in termini di tipo e/o contenuto del traffico;
- monitorare e verificare l'efficacia delle misure di sicurezza adottate per i flussi di rete;
- valutare e gestire il rischio associato alle minacce di tipo informatico;
- acquisire strumenti tecnologici e competenze in grado di affrontare e risolvere rapidamente ed efficacemente eventuali incidenti di sicurezza.

Il SIL si concretizza attraverso la realizzazione e la gestione di uno o più dei seguenti servizi:

Servizio di gestione dei dispositivi di sicurezza perimetrale

Il servizio consente di attuare la politica per la sicurezza sui dispositivi di difesa perimetrale dell'Amministrazione (per es. Firewall, VPN, RAS), provvedendo anche alla loro gestione sistemistica ed alla manutenzione.

Servizio di gestione IDS (Intrusion Detection System)

Il servizio fornisce la valutazione di eventi, situazioni anomale od allarmi che possono rappresentare una minaccia per la sicurezza dell'infrastruttura, attraverso opportuni strumenti di rilevazione, provvedendo anche alla loro gestione sistemistica e manutenzione.

Servizio di content filtering

Il servizio permette di ottimizzare l'uso delle risorse infrastrutturali, quali la capacità di banda verso Internet od il sistema di posta elettronica, controllando l'ammissibilità dei contenuti in transito rispetto alle politiche di sicurezza definite. Il servizio prevede anche la gestione sistemistica e manutenzione dei dispositivi utilizzati (es. proxy).

Servizio di content security

Il servizio provvede ad una gestione efficace delle contromisure atte a contrastare la diffusione dei codici malevoli, quali virus o worm su sistemi sia client (postazione di lavoro) che server. Il servizio prevede anche la gestione sistemistica e la manutenzione dei componenti utilizzati.

Servizio security host hardening

Il servizio provvede alla definizione, manutenzione e controllo delle politiche di configurazione e di aggiornamento dei sistemi server rilevanti per l'Amministrazione, in termini di sistema operativo e applicazioni di base.

I servizi descritti raggiungono la migliore efficacia se calati all'interno di un processo generale di gestione della sicurezza, all'interno della struttura dell'Amministrazione, definendo un contesto organizzativo e procedurale, attraverso la definizione di responsabilità specifiche, di obiettivi e politica per la sicurezza.

3. MODALITÀ DI DEFINIZIONE DELLA FORNITURA

Le principali attività che caratterizzano il SIL, comuni a tutti i tipi di servizi offerti, possono essere riassunte in

- Monitoraggio degli eventi significativi per la sicurezza, evidenziati durante l'erogazione del servizio;
- Gestione delle emergenze attraverso l'uso efficace degli strumenti adottati per l'erogazione del servizio;
- Aggiornamento delle componenti critiche per il servizio.

Le attività sono descritte in dettaglio più avanti nel capitolo Descrizione delle attività e dei prodotti. Di seguito si riporta una tabella riepilogativa con la correlazione tra i tipi di servizio e le attività necessarie per la sua erogazione.

Servizio	Attività		
	Monitoraggio	Gestione emergenze	Aggiornamento
Gestione dispositivi di sicurezza perimetrale	🚨	🚨	---
Gestione sistemi IDS	🚨	✓	🚨
Content security	✓	🚨	🚨
Content filtering	✓	✓	✓
Security host hardening	✓	🚨	🚨

Il simbolo 🚨 indica un'attività critica, in termini di priorità, tempestività ed efficienza, ha impatto sulla scelta dei valori soglia degli indicatori. Il simbolo ✓ indica un'attività ordinaria, che non ha particolari esigenze di tempestività.

Tabella 1 - Correlazione tra tipo di servizio ed attività

Per esempio, si ha la necessità di realizzare e gestire un sistema di monitoraggio delle intrusioni, realizzabile per mezzo di dispositivi IDS. La stesura dell'oggetto contrattuale utilizzerà le descrizioni delle attività e dei relativi indicatori specifici del servizio *Gestione sistemi IDS* (a partire dalla Tabella 1), ossia *Monitoraggio*, *Gestione emergenze* ed *Aggiornamento*. In questo caso, le attività di *Monitoraggio* ed *Aggiornamento* hanno una valenza critica che è evidenziata dai valori soglia definiti per l'indicatore di qualità associato. La descrizione dello strumento "IDS" (v. par. 5.10 "Descrizione dei prodotti"), darà le indicazioni per la scelta del tipo di dispositivo maggiormente aderente alle proprie esigenze.

Si noti che tutte le attività per la gestione e la manutenzione dei sistemi, intesi come l'insieme di componenti hardware e software per l'erogazione di un servizio, sono definite all'interno delle classi *Gestione sistemi (GSI)* e *Manutenzione sistemi (MSI)*.

3.1. OBIETTIVI

Il sistema SIL provvede a

- reagire prontamente ed efficacemente agli eventi di sicurezza segnalati dai canali stabiliti (monitoraggio, help desk, canale esterno);
- attivare tempestivamente i processi di escalation per il supporto decisionale;

- fornire le statistiche sugli eventi registrati al fine di identificare carenze di sicurezza e definire le azioni necessarie alla riduzione del rischio;
- mettere tempestivamente in atto gli aggiornamenti necessari per l'efficace funzionamento delle componenti fornite;
- accogliere le richieste inoltrate dal supporto di 1° livello e risolvere i problemi di assistenza;
- migliorare l'efficacia e l'efficienza nelle modifiche alle configurazioni richieste;
- controllare ed analizzare, in modalità centralizzata, i dati (ad esempio i log dei sistemi) e gli allarmi di tipo automatico.

3.2. UTENZA

Il servizio è offerto ai seguenti tipi di utenza:

- la funzione Information Technology dell'Amministrazione (personale tecnico ICT operante presso l'Amministrazione);
- l'insieme del personale operativo dell'Amministrazione, attraverso l'interfaccia di un Call Center.

3.3. DIMENSIONE, ARCHITETTURA E COMPLESSITÀ

Le variabili che impattano su costi, rischi e qualità sono essenzialmente le seguenti:

- il numero e l'estensione del perimetro e delle aree soggette a protezione;
- la dimensione del bacino di utenza;
- il numero di dispositivi e sistemi forniti o da gestire;
- la finestra temporale richiesta per l'erogazione del servizio, differenziando tra presidio fisso o reperibilità telefonica.

I costi della fornitura devono inoltre tenere conto di

- a) risorse per l'avvio del servizio nonché per l'acquisto e la manutenzione delle componenti hardware e software impiegate;
- b) numero e tipo di figure professionali impiegate a regime.

Il costo associato al punto a) è direttamente proporzionale al numero di componenti hardware e software richiesti. Il costo per l'acquisto di una singola componente (hardware o software) dipende generalmente:

- dalla tecnologia scelta per l'implementazione del servizio.
- dal numero di elementi protetti dalla componente (ad esempio, per un sistema antivirus, il costo può dipendere dal numero delle postazioni di lavoro protette; mentre per un sistema di content filtering, il costo può dipendere dal numero di utenti che accedono al servizio). Solitamente i fornitori applicano uno sconto progressivo sui prodotti il cui costo è basato sul numero di utenti, postazioni lavoro e simili.

I costi della realizzazione delle contromisure di sicurezza, vanno inoltre valutati sulla base dei risultati di un'**analisi del rischio**.

3.4. VINCOLI E REQUISITI

Per usufruire in maniera ottimale dei servizi di sicurezza descritti, l'Amministrazione dovrebbe dotarsi di un'organizzazione interna e di una politica per la sicurezza in conformità alla direttiva "Sicurezza Informatica e delle Telecomunicazioni nelle Pubbliche Amministrazioni Statali" del Ministero per l'Innovazione e le Tecnologie, e successive modifiche ed integrazioni (G.U. n. 69 del 22 marzo 2002), o comunque quanto più possibile in linea con le norme ISO 17799.

La misura della validità delle contromisure di sicurezza che si intendono adottare, a livello organizzativo, procedurale e tecnologico, è data dai risultati dell'**analisi del rischio** condotta dal Committente. Tali risultati dovrebbero essere utilizzati come elementi-guida nella progettazione di qualsiasi sistema di sicurezza.

3.5. RELAZIONE CON ALTRE CLASSI

Gli aspetti di gestione della sicurezza trattati in questa classe sono in stretta relazione con gli aspetti complementari trattati nella classe di fornitura Gestione della sicurezza fisica (SIF).

Gli aspetti, le attività ed i processi inerenti la gestione degli apparati utilizzati per l'erogazione dei servizi di sicurezza logica sono trattati nelle classi Manutenzione sistemi (MSI) e Gestione sistemi (GSI) per gli indicatori di disponibilità dei sistemi gestiti.

Le attività di progettazione, realizzazione e collaudo dei servizi di gestione della Sicurezza Logica sono descritte nell'ambito della classe Sviluppo dei Sistemi (SSI).

Si hanno ulteriori relazioni con la classe Gestione e manutenzione postazioni di lavoro (GPL), dove è prevista l'interazione con le postazione di lavoro degli utenti.

Hanno significativi punti di contatto anche le classi Assistenza in locale e in remoto (ASS) e Gestione e manutenzione reti (GMR).

3.6. STANDARD E NORME

ISO/IEC 17799: Information Security Management - Part 1: Code of practice for information security management, 2000

BS7799: Information Security Management - Part 2: Specification for information security management systems, 2000

Ministero per l'Innovazione Tecnologica – La sicurezza Informatica e delle Telecomunicazioni (ICT Security) – Allegato 2, Gennaio 2002

AIPA – Linee guida per la definizione di un piano per la sicurezza dei sistemi informativi automatizzati nella Pubblica Amministrazione

4. MODALITÀ DI STIMA DEI COSTI ANCHE IN FUNZIONE DELLA QUALITÀ RICHIESTA

La qualità del servizio offerto può essere valutata attraverso i seguenti tre fattori:

- a) tipo di presidio (per i servizi che richiedono un presidio on-site);
- b) livello professionale delle risorse impiegate;
- c) competenza della Società appaltante.

La qualità del servizio e, proporzionalmente, il costo rispetto al tipo di presidio può essere valutata utilizzando la seguente scala:

- 1) presidio fisso di 8 ore per i giorni lavorativi dal lunedì al venerdì (base);
- 2) presidio fisso di 12 ore per i giorni lavorativi dal lunedì al venerdì, sabato presidio di 6 ore (esteso);
- 3) presidio fisso 24 ore sette giorni/settimana (H24).

I vari tipi di presidio possono essere integrati (specialmente i tipi 1 e 2) con un servizio di reperibilità telefonica H24, con conseguente aumento dei costi e della qualità del servizio.

Naturalmente, se il servizio è erogato presso centri specializzati, il costo della fornitura può essere ridotto in funzione della condivisione delle risorse infrastrutturali e tecnologiche.

Qualità e costo del servizio sono inoltre proporzionali all'esperienza professionale ed alla capacità del personale impiegato per l'erogazione del servizio. Questi parametri possono essere stimati, anche se non in modo esaustivo, sulla base della valutazione dei curricula professionali del personale impiegato nell'erogazione del servizio e delle certificazioni professionali ottenute su argomenti pertinenti il servizio.

È compito dell'Amministrazione indicare nel capitolato le richieste minime per le figure professionali previste.

La qualità dei servizi erogati può inoltre essere determinata sulla base del numero di requisiti rilevanti per la sicurezza soddisfatti dal Fornitore, come per esempio:

- precedenti esperienze nel settore della sicurezza, specialmente in ambito pubblico;
- erogazione dei servizi da un centro certificato secondo standard internazionali;
- utilizzo di metodologie formalizzate conformi agli standard internazionali, per l'erogazione dei servizi.

A titolo indicativo, si fornisce un grafico che relaziona il costo della fornitura, il numero di elementi gestiti (che si assume siano tra loro omogenei) ed il tipo di presidio offerto.

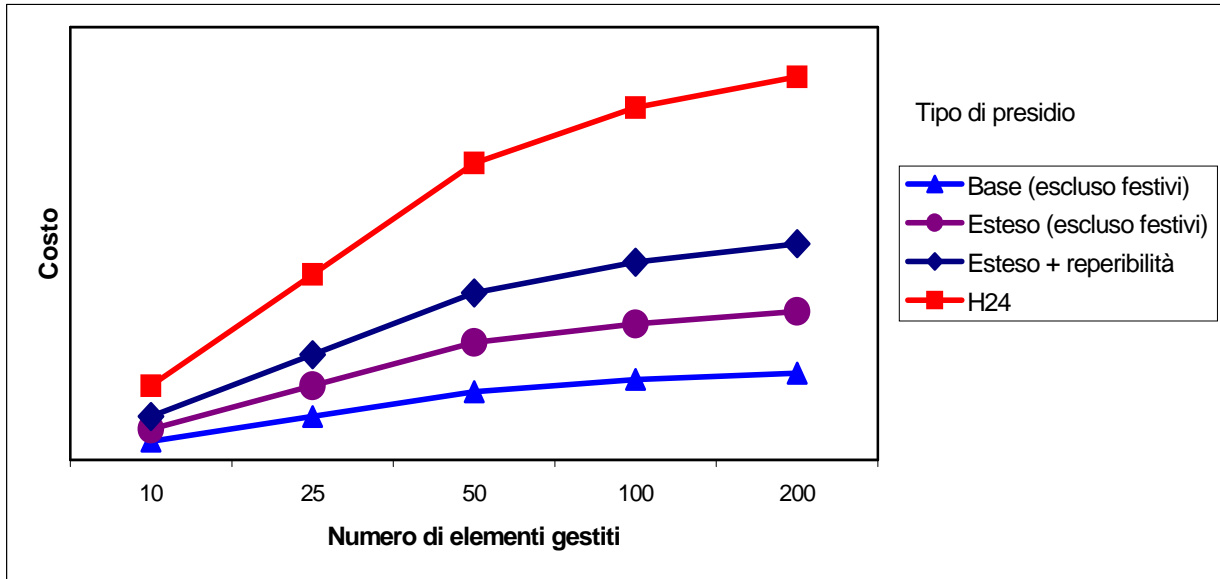


Figura 1 Relazione tra costo e tipo di presidio offerto

5. DESCRIZIONE DELLE ATTIVITÀ E DEI PRODOTTI

Le attività ed i prodotti relativi ai processi organizzativi e di supporto (processi trasversali), e cioè per esempio quelli relativi a gestione, documentazione, gestione della configurazione e assicurazione della qualità non sono descritti nella scheda e per la loro descrizione si rimanda alle schede specifiche.

Nel caso in cui attività o prodotti relativi a questi processi abbiano particolare rilevanza o criticità per la classe, essi sono comunque richiamati, evidenziando gli aspetti rilevanti o critici, rimandando per le caratteristiche generali alla scheda del processo.

I servizi svolti nell'ambito della classe di fornitura SIL si articolano su due diverse tipologie di attività. Le attività di progettazione e realizzazione, di natura transiente, finalizzate alla realizzazione del servizio e le attività di gestione, di natura continuativa, le cui interazioni sono illustrate in figura 2.

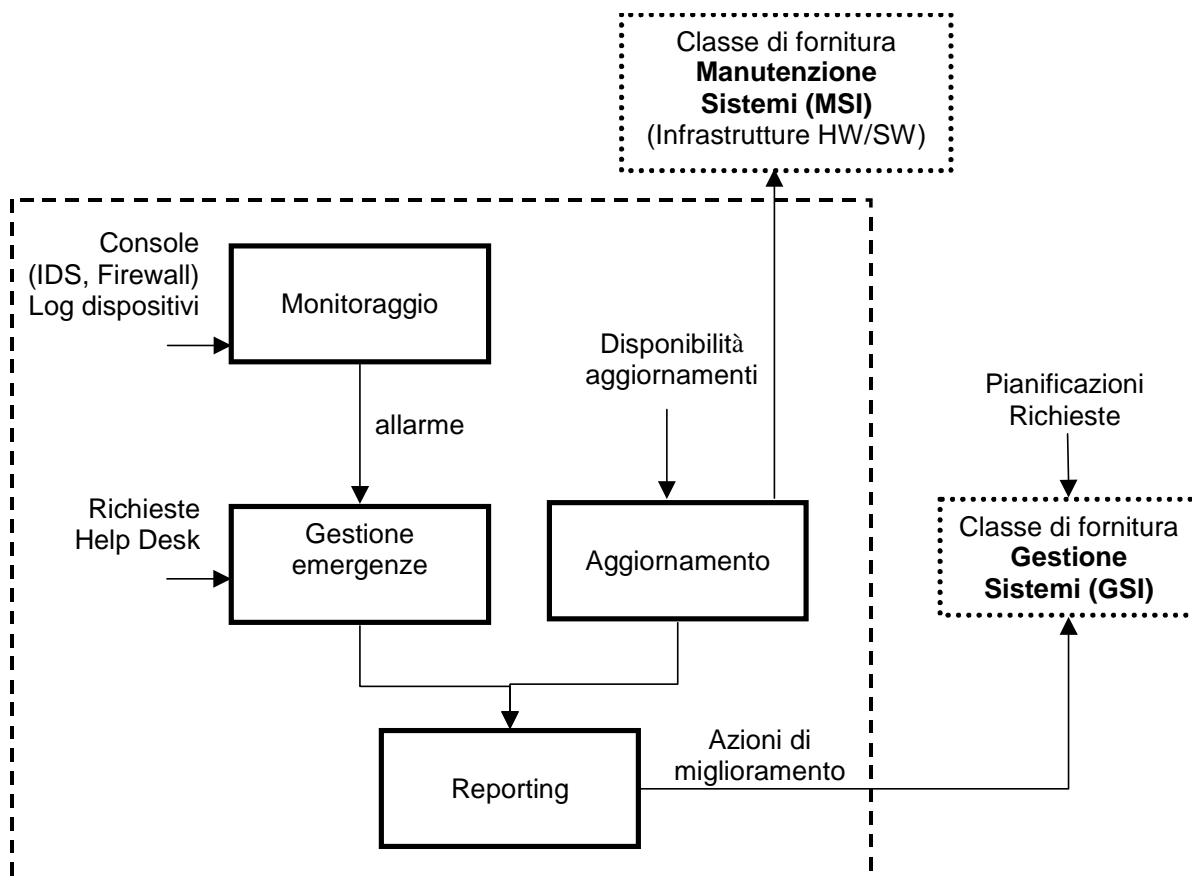


Figura 2: Attività di gestione della sicurezza logica

Il **monitoraggio** è l'attività di rilevazione di eventi ed allarmi critici per la sicurezza informatica. Ogni allarme o evento ed eventuali richieste da parte dell'Help Desk innescano il processo di **gestione delle emergenze**, che si prefigge la rapida ed efficace risoluzione delle anomalie riscontrate e il ripristino del corretto funzionamento dell'infrastruttura.

Altra attività importante è l'**aggiornamento** dei sistemi della sicurezza che avviene solitamente a seguito delle disponibilità di nuovi aggiornamenti da parte dei fornitori dei prodotti. Questa attività ha l'obiettivo di prevenire tempestivamente eventuali nuove minacce o di integrare i dati indispensabili al funzionamento del servizio. L'aggiornamento interagisce con i processi previsti nella classe di fornitura Manutenzione sistemi.

I dati raccolti durante lo svolgimento delle attività eseguite nell'ambito dell'erogazione del servizio sono aggregati ed elaborati durante l'attività di **reporting**. I risultati dell'attività sono utilizzati per individuare le aree di intervento nell'ottica di un miglioramento continuo del servizio. I miglioramenti individuati saranno attuati nell'ambito della classe Gestione Sistemi.

La seguente tabella riassume le principali attività del ciclo di vita della fornitura, che poi saranno descritte in maggior dettaglio nei paragrafi seguenti. Per ogni attività sono specificati:

- una stima indicativa del peso percentuale di effort richiesto, nell'ipotesi che la fornitura comprenda tutte le categorie di prodotto descritte al paragrafo 5.10 (firewall, IDS, content filtering, content security, security host hardening), che il servizio sia erogato con modalità dedicate per l'Amministrazione (non centralizzato presso un centro specializzato) e con presidio di tipo esteso e reperibilità telefonica. L'incidenza di ciascuna attività è rapportata al totale della tipologia di appartenenza ("progettazione e realizzazione" o "gestione");
- i prodotti di input e di output;
- i profili professionali EUCIP responsabili dell'esecuzione dell'attività.

ATTIVITA'	% EFFORT	INPUT	OUTPUT	PROFILI PROFESSIONALI RESPONSABILI
Analisi dei requisiti	15%	Capitolato tecnico della fornitura e ulteriori specifiche fornite dall'Amministrazione	Specifica dei requisiti	Consulente per la Sicurezza
Progettazione	30%	Specifiche dei requisiti	Progetto del sistema	Consulente per la Sicurezza
Progettazione collaudo	10 %	Progetto del sistema	Specifica di test Specifica di collaudo	Tecnico di Collaudo e Integrazione di Sistemi
Realizzazione del servizio	35%	Progetto del sistema	Progetto del servizio, Sistema di erogazione del servizio	Consulente per la Sicurezza
Avviamento del servizio	10 %	Sistema di erogazione del servizio	Rapporto di test Verbale di collaudo	Tecnico di Collaudo e Integrazione di Sistemi
Totale Attività di Progettazione e Realizzazione	100%			
Monitoraggio di sicurezza	40 %	Dati Eventi	Allarme	Consulente per la Sicurezza
Gestione operativa delle emergenze	20 %	allarme generato dal processo di monitoraggio di sicurezza; richiesta o segnalazione dell'help desk.	Risoluzione dell'emergenza Rapporto di incidente	Consulente per la Sicurezza
Aggiornamento	20 %	disponibilità di aggiornamenti	Verbale di intervento	Consulente per la Sicurezza

ATTIVITA'	% EFFORT	INPUT	OUTPUT	PROFILI PROFESSIONALI RESPONSABILI
Rendicontazione	20 %	log dei dispositivi Allarmi valori prestazionali	Rapporto sulla sicurezza logica	Consulente per la Sicurezza
Totale Attività di Gestione	100%			

5.1. ANALISI DEI REQUISITI

Questa attività si concretizza in un documento **Specifica dei requisiti** articolato nei seguenti punti:

- descrizione del servizio e dei relativi processi;
- requisiti contrattuali:
 - livello di copertura del servizio che il fornitore si impegna a garantire;
 - standard di servizio da assicurare attraverso indicatori di qualità;
 - efficacia del servizio;
- requisiti tecnologici, procedurali ed organizzativi emersi dai risultati dell'analisi del rischio;
- requisiti cogenti, in base alle norme in vigore;
- requisiti tecnici, definiti in base alle tecnologie disponibili;
- requisiti di gestione operativa e manutenzione;
- requisiti organizzativi per la gestione del servizio, in termini di struttura gerarchica e modalità operative.

Il documento Specifica dei requisiti tratta ciascuno degli elementi sopra indicati ed ha le seguenti caratteristiche:

- contiene il puntamento alla documentazione contrattuale di riferimento (capitolato, richiesta di offerta, ecc.) per ogni requisito trattato;
- fornisce, per ogni requisito, una descrizione dettagliata, orientata alla progettazione ed alla realizzazione.

5.2. PROGETTAZIONE

Questa attività produce il documento **Progetto del sistema**, con i seguenti contenuti:

- identificazione della architettura di alto livello del sistema riguardante gli elementi hardware, software e le operazioni manuali previste per la realizzazione di un SIL;
- elaborazione del prototipo del sistema ipotizzato, con la definizione dei flussi di attività;
- descrizione dei flussi di attività in una logica cliente-fornitore, per gestire la relazione come un ciclo o un insieme di cicli di servizio;

- definizione dei dati e dei requisiti degli strumenti necessari per la registrazione e la rendicontazione delle attività del SIL.

Il documento Progetto del sistema tratta ognuno degli elementi sopra indicati ed ha le seguenti caratteristiche:

- contiene, per ogni elemento, il puntamento alla documentazione contrattuale di riferimento (capitolato, richiesta di offerta, ecc.) per ogni requisito trattato;
- fornisce, per ogni elemento, una descrizione dettagliata orientata alla realizzazione.

5.3. PROGETTAZIONE COLLAUDO

A seguito della progettazione tecnica del sistema, sono svolte le attività di progettazione di test e collaudo, le cui caratteristiche sono le seguenti:

TEST

- è eseguito durante ed alla fine dello sviluppo;
- si articola in test di unità, di integrazione e stress test; ogni elemento del test è definito “prova”, quindi il test è composto di più prove;
- ha valore di verifica e di validazione;
- è eseguito in un ambiente di prova;
- è eseguito dal fornitore del servizio, generalmente da un gruppo dedicato (gruppo test e collaudo);
- necessita di una specifica di test.

COLLAUDO

- è eseguito dopo il completamento dei test ed è orientato all'accettazione formale del servizio;
- ha valore di validazione;
- può articolarsi in due fasi:
 - una prima fase (opzionale) in un ambiente che può essere il target finale, ma non è in esercizio;
 - una seconda fase (sempre necessaria) in condizioni di esercizio;
- è eseguito congiuntamente dal fornitore e dall'Amministrazione, che può delegare una terza parte, scelta per competenza, ove il cliente non possieda le necessarie capacità tecniche per seguire il collaudo;
- necessita di una specifica di collaudo, proposta dal gruppo di test e collaudo ed accettata dal cliente.

L'attività di test prevede la definizione delle prove per la verifica del corretto funzionamento del servizio realizzato e l'aderenza ai requisiti.

Per quanto concerne test e collaudo sono definiti

- la pianificazione temporale delle sessioni di prova;
- la definizione degli ambienti, strumenti e tecniche per l'esecuzione delle prove;
- le condizioni di accettabilità delle parti messe a disposizione dall'Amministrazione o derivanti dai processi di gestione rilasciati da un precedente gestore;

- le procedure di prova da eseguire (dati di input delle prove);
- i risultati attesi;
- i mezzi di prova, gli ambienti ed i metodi;
- i criteri di accettazione;
- i contenuti dei verbali di collaudo.

I prodotti di questa attività sono la **Specifica di test** e la **Specifica di collaudo**.

La Specifica di Test è utilizzata dal fornitore per l'esecuzione dei propri cicli di prove, mentre la Specifica di Collaudo è il riferimento per l'Amministrazione al fine di verificare ed accettare la fornitura.

Nel caso in cui, durante l'erogazione di durata pluriennale dei servizi di Gestione della sicurezza logica, si manifestino variazioni di tipo tecnologico, applicative od infrastrutturale, è possibile che una parte del servizio debba essere riprogettata (processi, attività, risorse impiegate, strumenti). Di conseguenza, in questi casi, sono previste nuove attività di test e collaudo, relativamente alle parti modificate.

5.4. REALIZZAZIONE DEL SERVIZIO

Questa attività è articolata nella acquisizione, realizzazione, integrazione e documentazione di

- strumenti tecnologici necessari alla gestione;
- software di gestione;
- procedure di prova (test).

Prodotto di questa attività è il documento **Progetto del servizio** che descrive l'organizzazione, le attività, le responsabilità, i processi necessari all'erogazione del servizio ed i relativi livelli di servizio. Il Piano è soggetto ad approvazione; essendo soggetto ad aggiornamento, sono quindi previste successive approvazioni.

La verifica sul documento è atta ad assicurare la non ambiguità dei requisiti trattati. La verifica è orientata ad accertare che:

- per ogni requisito trattato nel documento sia inserito il puntamento alla documentazione contrattuale di riferimento (capitolato/richiesta d'offerta);
- per ogni requisito sia fornita una descrizione orientata alla realizzazione del servizio.

Il servizio è installato sulla base del relativo Piano. Prodotto di questo passo è il **Sistema di erogazione del servizio** installato.

5.5. AVVIAMENTO DEL SERVIZIO

Questa attività prevede l'esecuzione delle prove della soluzione in accordo alla Specifica di Test, volte a verificare il corretto funzionamento e la rispondenza del sistema sviluppato alle specifiche ed ai requisiti.

Il prodotto di questa attività è il **Rapporto di test** contenente l'esito delle singole prove di test.

Al termine della realizzazione e dell'eventuale fase di pre-esercizio il servizio è rilasciato, previo collaudo effettuato da una Commissione di Collaudo nominata dall'Amministrazione.

La Commissione opera con autonoma responsabilità ed ha il compito di verificare che quanto realizzato dal Fornitore sia conforme ai requisiti indicati nel contratto. Sono oggetto di collaudo anche l'infrastruttura degli strumenti di supporto alla gestione e la documentazione.

Il Fornitore supporta la Commissione nell'esecuzione delle prove, nel rilevamento dei risultati, nella stesura del rapporto finale.

Per svolgere le prove di collaudo la Commissione utilizza, a titolo di guida, la Specifica di Collaudo concordata con il Fornitore.

La documentazione di esecuzione delle prove e delle non-conformità rilevate viene formalizzata nel **Verbale di collaudo** (emesso dalla Commissione di Collaudo) il quale costituisce riferimento per il riciclo delle attività di progettazione finalizzate alla rimozione delle non conformità rilevate.

5.6. MONITORAGGIO DI SICUREZZA

Il monitoraggio consiste nella rilevazione tempestiva di eventi ed allarmi critici per la sicurezza informatica.

L'attività si realizza per mezzo della continua e consapevole osservazione dell'infrastruttura gestita, all'interno della finestra temporale di erogazione prevista, al fine di

- prevenire i rischi;
- verificare la corretta attuazione delle politiche di sicurezza e la loro efficacia;
- individuare tempestivamente situazioni di allarme.

I tipi di informazioni ed i segmenti dell'infrastruttura da monitorare sono definiti dalla politica per la sicurezza dell'Amministrazione.

I dati e gli eventi da monitorare sono raccolti da

- le console di monitoraggio e gestione dei dispositivi forniti (per es. IDS, firewall);
- i log dei dispositivi forniti con il servizio ed eventuali log provenienti da altri dispositivi importanti dell'infrastruttura (per esempio, server di posta elettronica, router);
- le notifiche e gli allarmi provenienti dall'esterno dell'organizzazione, quali fornitori dei prodotti, istituti di ricerca.

Ciascun evento è valutato e verificato. Se la verifica ha esito positivo, è generato un **allarme** (prodotto dell'attività) che avvia l'attività di gestione delle emergenze (escalation).

5.7. GESTIONE OPERATIVA DELLE EMERGENZE

Ogni allarme o evento ed eventuali richieste da parte dell'Help Desk innescano la gestione delle emergenze, che si prefigge la rapida ed efficace risoluzione delle anomalie riscontrate e il ripristino del corretto funzionamento dell'infrastruttura.

L'attività di gestione delle emergenze ha l'obiettivo di fornire risposte concrete e rapide ad eventi critici in termini di sicurezza informatica.

Il processo è attivato a seguito di una segnalazione od evento potenzialmente critico. La segnalazione può essere notificata da

- un allarme generato dal processo di monitoraggio di sicurezza;
- una richiesta o una segnalazione dell'help desk di primo o secondo livello.

In funzione del tipo di segnalazione si procede con una rapida e tempestiva indagine per confermare o meno la presenza di una potenziale minaccia o per arginare una minaccia concretizzata.

Nel caso in cui la segnalazione sia altamente affidabile e non necessiti di ulteriori indagini, oppure quando l'indagine conferma la segnalazione (per esempio la compromissione di un sistema), si procede rapidamente con l'azione correttiva di pertinenza (come per esempio il blocco immediato del traffico pericoloso) in modo da risolvere l'emergenza (**Risoluzione dell'emergenza**). La messa in atto dell'azione correttiva può richiedere l'autorizzazione di un responsabile dell'Amministrazione gerarchicamente competente per la sicurezza. L'attività determina la registrazione dei dati sui risultati ottenuti, delle eventuali indagini e dei tempi di ciascuna fase.

Il risultato dell'attività è un dettagliato rapporto (**Rapporto di incidente**) sulle cause e sulle attività svolte per affrontare l'emergenza. Il rapporto sull'incidente riepiloga ed analizza gli eventi al fine di individuare le cause imputabili all'emergenza, documentando:

- il tipo di azione perpetrata,
- le cause all'origine dell'incidente,
- le conseguenze dell'accaduto,
- i tempi e le modalità di rilevazione dell'incidente,
- i tempi e le modalità di ripristino,
- altre anomalie riscontrate.

5.8. AGGIORNAMENTO

Altra importante attività è l'aggiornamento dei sistemi di sicurezza, che avviene solitamente a seguito della disponibilità di nuovi rilasci da parte dei fornitori dei prodotti. L'obiettivo è quello di prevenire tempestivamente nuove minacce e di integrare i dati indispensabili al funzionamento del servizio. Le attività di aggiornamento sono svolte nell'ambito della classe di fornitura Manutenzione sistemi (MSI).

L'attività è avviata a seguito della segnalazione della disponibilità di aggiornamenti da parte dei fornitori dei prodotti, per esempio:

- database delle *signature* degli antivirus;
- *aggiornamenti critici* per i sistemi operativi e le applicazioni di base;
- *black list* per sistemi di *content filtering*;
- database dei *pattern* di attacco degli IDS;

La rapidità nella distribuzione degli aggiornamenti varia in base al tipo di servizio ed in funzione dell'entità del rischio derivante dalla mancata od intempestiva esecuzione dell'attività. La criticità degli aggiornamenti è in generale definita in accordo con le politiche per la sicurezza stabilite ed in base ai requisiti strategici dell'Amministrazione. Per esempio, l'aggiornamento del database delle *signature* degli antivirus potrebbe richiedere tempi di esecuzione più ristretti rispetto ai tempi richiesti per l'aggiornamento di *black list* di un dispositivo di *content filtering*.

Risultato dell'attività è l'aggiornamento periodico delle componenti software dei prodotti oggetto del contratto. L'attività ed i relativi risultati sono registrati con un **Verbale di intervento**.

Qualora l'aggiornamento abbia un impatto significativo sul sistema, le attività saranno svolte nell'ambito della classe di Manutenzione sistemi (per esempio nel caso di Manutenzione preventiva).

5.9. RENDICONTAZIONE

Durante lo svolgimento delle attività di gestione operativa vengono raccolte ed analizzate le registrazioni degli eventi significativi per la sicurezza e quelli relativi ai guasti/malfunzioni. Per questo aspetto si può fare riferimento alla reportistica delle classi di fornitura Assistenza in locale e in remoto (ASS), Manutenzione sistemi (MSI) e Gestione e manutenzione reti (GMR).

Queste informazioni, aggregate ed elaborate, servono a monitorare il superamento/non superamento dei parametri di controllo del servizio e, soprattutto, ad individuare aree di intervento nell'ottica di un miglioramento continuo.

I dati di ingresso di questa attività comprendono i log dei dispositivi che realizzano l'infrastruttura di sicurezza (per esempio: firewall, IDS), gli allarmi che hanno attivato la gestione ordinaria o delle emergenze ed i valori prestazionali collezionati dai sistemi di monitoraggio.

L'elaborazione di questi dati consente la produzione di un **Rapporto sulla sicurezza logica** che

- permetta di analizzare l'andamento del servizio;
- evidenzi eventuali carenze nella sicurezza, per la definizione di azioni necessarie alla riduzione del rischio.

I contenuti del rapporto devono trattare, per ciascun servizio erogato:

- a) le anomalie riscontrate rispetto alle politiche di sicurezza definite, relativamente alle specificità del corrispondente servizio: deve essere prevista un’aggregazione delle anomalie (dove applicabile) in base alla tipologia, alla sorgente, alla destinazione ed alla fascia oraria degli eventi registrati come non conformi alle politiche di sicurezza.
- b) l’andamento nel tempo dei parametri prestazionali significativi per il servizio e per gli strumenti utilizzati. Ad esempio:
 - per gli strumenti adottati possono essere presi in considerazione: utilizzo della CPU, della memoria, delle interfacce di rete;
 - per i servizi specifici: lunghezza della coda dei messaggi di posta elettronica in attesa di controllo antivirus, il numero di connessioni contemporanee gestite da un dispositivo firewall.

5.10. DESCRIZIONE DEI PRODOTTI

Per agevolare la comprensione della classe di fornitura ed orientare alla scelta dei prodotti da impiegare per la gestione della sicurezza logica., è opportuno fornirne una breve descrizione.

Firewall

Un firewall può essere definito come un dispositivo od una architettura volti all’applicazione di una politica di gestione del traffico di rete lungo il perimetro del dominio di sicurezza. I firewall sono comunemente associati ad un determinato prodotto hardware o software e possono essere differenziati in base alla tecnologia utilizzata. Tra le principali tecnologie presenti sul mercato attuale si possono individuare:

- packet filtering (PF);
- stateful inspection (SI);
- application proxy (AP).

Queste tecnologie (o funzioni) sono spesso realizzate contemporaneamente sullo stesso prodotto. La tecnologia utilizzata è uno dei fattori determinanti per la valutazione del prodotto in termini di requisiti di sicurezza, insieme all’architettura scelta per la realizzazione della soluzione firewall.

Di seguito, a titolo indicativo, viene presentata una tabella riassuntiva, utilizzabile come supporto alla scelta della tecnologia di un firewall.

Parametri	Tecnologia		
	Packet filtering (PF)	Application proxy (AP)	Stateful inspection (SI)
Servizi / protocolli supportati	Tutti	Specifici	Tutti
Requisiti di sicurezza	Bassi	Alti	Medi
Prestazioni e scalabilità	Alte	Basse	Medio-alte

Il tipo di piattaforma (elaboratore di tipo “general purpose” oppure “piattaforma dedicata”) sulla quale è realizzato il firewall influenza parametri quali:

- prestazioni;
- flessibilità;
- costi;
- manutenibilità;
- stabilità.

Si può in genere considerare che una piattaforma dedicata offra maggiori prestazioni e garanzie di stabilità e manutenibilità, mentre una piattaforma “general purpose” assicuri una maggiore flessibilità.

Intrusion Detection System (IDS)

Un sistema IDS è un complesso di dispositivi (sia di tipo hardware sia di tipo software) di rilevazione e monitoraggio delle attività sospette od anomale rilevate all'interno del perimetro di monitoraggio. Tipicamente il sistema IDS implementa una sicurezza di tipo passivo. I dispositivi IDS (spesso indicati con il termine “sonde”) possono essere di tipo:

- network based;
- host based.

Nel primo caso il dispositivo analizza il traffico in transito nel segmento monitorato; esso può essere realizzato sia su piattaforme generiche (elaboratori general purpose) sia su piattaforme dedicate.

Nel caso host based sono oggetto del controllo i processi, i dati e le attività che sono attivi sull'elaboratore oggetto dell'IDS. I sistemi IDS host based, possono essere di tipo “real-time” o programmati ad intervalli prestabiliti. Generalmente gli IDS host based sono realizzati via software.

I diversi tipi di IDS non vanno considerati mutuamente esclusivi, sebbene il tipo network based sia quello più diffuso.

Un sistema IDS (sia di tipo network sia host based) è costituito da un insieme di sonde che analizzano il proprio target (traffico di rete, log, processi, ecc.) ed inviano eventi ad una o più console di gestione. Nelle sonde IDS network based il traffico di gestione è terminato su una scheda di rete dedicata.

Content filtering

I sistemi di content filtering applicano i principi di ammissibilità sui contenuti di determinati tipi di traffico, in base alla combinazione di criteri, quali ad esempio la classificazione dei contenuti o il profilo dell'utente. Le realizzazioni più diffuse sono quelle per il filtraggio ed il controllo di traffico di navigazione (HTTP) e della posta elettronica (SMTP). Nel primo caso, svolgono il compito di regolamentare la navigazione Internet, permettendo, negando e controllando l'accesso alle pagine Web in base al loro contenuto, in accordo alla politica stabilita. I sistemi di Content Filtering possono essere utilizzati come strumento per limitare i costi dovuti all'impegno della banda Internet. Il traffico di posta elettronica può essere regolato limitando l'ingresso di posta elettronica non desiderata (ad esempio con sistemi *anti-spam*).

I sistemi di content filtering sono generalmente componenti software che integrano le proprie funzionalità con dispositivi già presenti ed in modo particolare con proxy applicativi, quali i sistemi centralizzati usati per la navigazione Internet, e server di posta elettronica.

La classificazione dei contenuti può essere realizzata per mezzo di meccanismi statici e/o dinamici. I prodotti che utilizzano meccanismi di classificazione statici (ad esempio per mezzo di black list) sono generalmente caratterizzati dai seguenti aspetti:

- semplicità ed affidabilità del prodotto;

- necessità di frequenti aggiornamenti delle black list (con conseguente costo di sottoscrizione);
- bassissima percentuale di falsi positivi;
- percentuale di falsi negativi anche rilevante.

I prodotti di content filtering che utilizzano meccanismi dinamici sono caratterizzati dai seguenti aspetti:

- complessità del prodotto;
- frequenza di aggiornamenti molto contenuta;
- percentuale di falsi positivi bassa;
- percentuale di falsi negativi bassa.

Content security

I prodotti di content security realizzano contromisure per l'individuazione e la rimozione di contenuti malevoli, quali virus, worm, spyware.

I sistemi di content security possono essere realizzati in diverse modalità, le due più diffuse sono le seguenti:

- *sistema centralizzato*, provvede al controllo di specifici flussi di dati, integrando le proprie funzionalità con firewall, proxy, server di posta elettronica, ecc.;
- *sistema locale*, provvede alla protezione delle singole postazioni di lavoro o di singoli elaboratori di tipo server.

Le due modalità sono da considerarsi complementari. I prodotti di content security necessitano di continui e tempestivi aggiornamenti del proprio "database delle firme", per mezzo del quale possono rilevare e rimuovere con certezza i contenuti malevoli. A differenza dei prodotti di content filtering, nei prodotti/servizi di content security eventuali falsi positivi e/o falsi negativi possono non essere tollerabili.

In caso di emergenza, i prodotti di content security di tipo centralizzato devono offrire la possibilità di rimuovere contenuti potenzialmente malevoli, in base a criteri personalizzabili, quali il tipo di dati (per esempio immagini, eseguibili), parametri specifici del protocollo di comunicazione (per esempio il campo subject in una e-mail), ecc. La flessibilità di questo tipo di funzione può essere uno dei criteri per la valutazione del prodotto.

Le risposte dei diversi fornitori di soluzioni di content security alle nuove minacce, specialmente in casi di elevata pervasività, variano notevolmente in termini di rapidità ed efficacia. Per questa ragione è possibile (e consigliabile) utilizzare più prodotti di content security di fornitori diversi.

Security host hardening

Il servizio di security host hardening ha lo scopo di limitare il livello di vulnerabilità delle risorse ICT del sistema operativo e delle applicazioni di base. Il servizio generalmente copre i tipi di server critici per l'Amministrazione.

Il servizio si articola in tre fasi principali:

- definizioni della politica per l'eliminazione delle funzionalità non necessarie e per la personalizzazione dei sistemi operativi per i soli servizi che essi debbono offrire;

- monitoraggio della disponibilità degli aggiornamenti critici per i sistemi operativi e per il software di base, che si articola a sua volta in:
 - classificazione del livello di criticità in rapporto alle contromisure in essere sull'infrastruttura tecnologica;
 - tempestiva segnalazione alle unità organizzative competenti per la gestione dei sistemi coinvolti;
- verifica periodica, o su richiesta, della conformità delle configurazioni rispetto alle direttive definite.

La definizione delle direttive può avvenire seguendo direttamente le indicazioni dei produttori dei sistemi operativi o delle applicazioni stesse, o personalizzando le configurazioni in base alle specifiche dell'infrastruttura in cui i sistemi si trovano ad operare. Il servizio si integra con le attività della classe di fornitura "Gestione Sistemi".

Viene eseguita una verifica:

- su base periodica, per l'intero parco macchine al quale il servizio è rivolto;
- prima del rilascio in esercizio delle applicazioni;
- a seguito di modifiche importanti ai servizi erogati.

È necessaria inoltre una verifica periodica sia delle direttive definite per eventuali miglioramenti e adeguamenti a fronte di nuove vulnerabilità, sia della conformità delle configurazioni dei sistemi alle direttive approvate.

Il servizio produce:

- direttive di configurazione per il componente richiesto, quali sistemi operativi o software di base;
- segnalazione di disponibilità di aggiornamenti, con relativo livello di criticità ed indicazione del tempo massimo di applicazione;
- rapporto sulla conformità delle configurazioni analizzate, su base periodica o su richiesta.

6. DESCRIZIONE DEI PROFILI PROFESSIONALI COINVOLTI

Nella tabella seguente (Matrice di Responsabilità Attività – Profilo Professionale) sono riportati per ciascuna attività i profili professionali EUCIP tipicamente coinvolti nello svolgimento dell'attività stessa e nel rilascio dei relativi prodotti, qualificati in termini di:

- responsabile (**R**), è il profilo professionale che esegue l'attività, coordina gli eventuali contributi di altri profili professionali ed è responsabile primario della qualità dei prodotti dell'attività;
- contributore (**C**), è il profilo professionale che contribuisce con competenze specialistiche allo svolgimento di elementi dell'attività e può gestire in autonomia, in accordo con il responsabile, specifiche sotto-attività; i contributori sono suddivisi in due categorie:

- contributore tipico (Ct), il suo contributo all'attività è richiesto nella quasi totalità delle istanze di fornitura, una sua eventuale assenza dovrebbe essere considerata un'eccezione e le relative motivazioni dovrebbero essere esplicitate (peculiarità tecniche od organizzative dell'istanza di fornitura).
- contributore specifico (Cs), il suo contributo all'attività è legato alle specificità dell'istanza di fornitura, la sua presenza, anche se frequente, non può essere considerata tipica.

Il profilo professionale responsabile di tutte le attività di questa classe di fornitura, eccetto quelle relative a test e collaudo, è il Consulente per la Sicurezza.

Per profilo professionale responsabile (o contributore) si deve intendere non una singola persona fisica, ma una famiglia professionale, caratterizzata da competenze comuni, ove coesistono livelli di esperienza, aree di specializzazione e ruoli organizzativi differenziati.

Ad esempio, è possibile, anzi probabile, che lo specialista coinvolto nelle attività di natura progettuale di SIL, dall'analisi dei requisiti sino all'avviamento del servizio, sia distinto da quello responsabile delle successive attività di gestione, pur appartenendo entrambi al medesimo profilo professionale di Consulente per la Sicurezza.

Le competenze del Consulente per la Sicurezza abbracciano sia le attività di progettazione e realizzazione delle procedure e delle tecnologie di sicurezza sia le attività di gestione operativa ed il profilo può contribuire, in altre classi di fornitura, alla definizione ed implementazione dei requisiti di sicurezza nell'ambito di progetti di sviluppo.

Il Consulente per la Vendita e l'Applicazione di Tecnologie Informatiche contribuisce esclusivamente nella fase di analisi requisiti, come elemento di raccordo tra le fasi di stesura dell'offerta e di avvio del progetto dopo l'aggiudicazione della fornitura.

Il profilo Tecnico di Collaudo e Integrazione di Sistemi, con il contributo del Consulente per la Sicurezza, è responsabile delle attività di progettazione ed esecuzione dei test e del collaudo del servizio (supporto all'Amministrazione per il collaudo).

Gli altri profili che contribuiscono alle attività sono:

- il Progettista di Sistemi informatici, per la definizione dell'architettura del sistema;
- il Responsabile di Rete, per le attività di progettazione e realizzazione dei servizi di sicurezza che più impattano la rete;
- il Sistemista Multiplatforma, per le attività di progettazione, realizzazione del servizio ed aggiornamento, in particolare per quanto attiene alla componente di security host hardening.

Nel caso vi fossero esigenze di rendicontazione che richiedano sviluppi o personalizzazioni complesse per la gestione dei dati del servizio potrebbe essere necessario il coinvolgimento del profilo di Responsabile di Base di Dati nelle attività di progettazione e realizzazione del servizio.

Nella tabella "Matrice di Responsabilità Attività – Profilo Professionale" è anche indicata per ciascun profilo professionale, responsabile (R) o contributore tipico (Ct), un'ipotesi di massima del suo impegno (quantità di lavoro, "effort") nell'attività. Tale impegno è espresso come percentuale, fatto 100 l'impegno totale richiesto dall'attività, ed è quindi una stima del "peso" relativo del profilo professionale nell'esecuzione dell'attività.

Si tratta ovviamente di stime di larga massima ipotizzate a partire da un'astratta istanza di fornitura tipica e che non tengono conto della presenza di eventuali contributori specifici.

Per la stima si è ipotizzato che la fornitura comprenda tutte le categorie di prodotto descritte al paragrafo 5.10 (firewall, IDS, content filtering, content security, security host hardening) e che il servizio sia erogato con modalità dedicate per l'Amministrazione (non centralizzato presso un centro specializzato).

TABELLA MATRICE DI RESPONSABILITA' ATTIVITA' – PROFILO PROFESSIONALE

Profilo professionale	Attività								
	Analisi dei requisiti	Progettazione	Progettazione collaudo	Realizzazione del servizio	Avviamento del servizio	Monitoraggio di sicurezza	Gestione operativa delle emergenze	Aggiornamento	Rendicontazione
4 – Consulente per la Vendita e l'Applicazione di Tecnologie Informatiche	Ct 10%								
11- Tecnico di Collaudo e Integrazione di Sistemi			R 80%		R 80%				
13- Progettista di Sistemi Informatici		Ct 10%							
15 – Consulente per la Sicurezza	R 90%	R 70%	Ct 20%	R 70%	Ct 20%	R 100%	R 100%	R 90%	R 100%
16 -Responsabile di Basi di Dati		Cs		Cs					
17 – Responsabile di Rete		Ct 10%		Ct 15%					
19 – Sistemista Multiplatforma		Ct 10%		Ct 15%				Ct 10%	
% di effort - totale	100%	100%	100%	100%	100%	100%	100%	100%	100%

I profili professionali di riferimento sono quelli definiti dallo schema EUCIP (European Certification of Informatics Professionals) sviluppato dal CEPIS (Council of European Professional Informatics Societies) che, per ciascun profilo, indica le attività tipiche ed il dettaglio delle competenze possedute.

Le sintesi delle competenze dei profili professionali coinvolti nelle attività di questa classe di fornitura sono le seguenti (tra parentesi l' identificativo del profilo):

(4) Consulente per la Vendita e l'Applicazione di Tecnologie Informatiche (Sales and Application Consultant). Un consulente per la vendita e l'applicazione di tecnologie informatiche secondo lo standard EUCIP deve abbinare alla competenza in una specifica tecnologia (legata al contesto, es. CAD) anche la conoscenza di concetti avanzati di marketing e delle esigenze tipiche dei clienti. E' indispensabile l'efficacia persuasiva nel presentare soluzioni, dimostrazioni pratiche e proposte commerciali.

(11) Tecnico di Collaudo e Integrazione di Sistemi (Systems Integration & Testing Engineer). Un tecnico di collaudo e integrazione di sistemi secondo lo standard EUCIP deve essere molto efficace in varie aree dello sviluppo di sistemi: preparazione della documentazione per l'utente finale, allestimento di sistemi IT, test delle loro funzioni, sia nel complesso che per singoli moduli componenti, identificazione delle anomalie e diagnosi delle possibili cause. E' richiesta anche una conoscenza specifica su come vengono costruite le interfacce tra moduli software.

(13) Progettista di Sistemi Informatici (IT Systems Architect). Un progettista di sistemi informatici secondo lo standard EUCIP assume un ruolo centrale nella progettazione, integrazione e miglioramento di sistemi IT – con particolare riguardo alle architetture software – curandone anche la sicurezza e le prestazioni; oltre ad una vasta competenza dell'ICT (in tutti i campi: software, hardware e reti) e di tecniche di progettazione specifiche, è richiesta la capacità di descrivere un sistema in termini di componenti e flussi logici.

(15) Consulente per la Sicurezza (Security Adviser). Un consulente per la sicurezza secondo lo standard EUCIP deve essere molto efficace nell'identificare i requisiti di sicurezza dei sistemi ICT e nel definire soluzioni affidabili e agevoli da gestire. Ad una competenza dell'ICT ampia e approfondita deve essere abbinata la capacità di interagire con altre funzioni ICT per favorire l'integrazione di tecnologie per la sicurezza all'interno dell'infrastruttura ICT.

(16) Responsabile di Basi di Dati (Database Manager). Un responsabile di basi di dati secondo lo standard EUCIP assume un ruolo centrale tanto nella progettazione di strutture di dati quanto nella gestione ordinaria dei DB; tra i requisiti figurano dunque una profonda competenza in tutti gli aspetti delle tecnologie dei DB, un approccio collaborativo ai contesti di progetto, esperienza nelle tecniche di modellazione dei dati, ma anche l'efficacia nel definire e applicare le procedure e nell'organizzare le operazioni ordinarie.

(17) Responsabile di Rete (Network Manager). Un responsabile di rete secondo lo standard EUCIP deve essere molto efficace nel gestire un sistema informativo di rete di media complessità e nel migliorarne le prestazioni. Deve inoltre saper interagire con i progettisti di reti e con eventuali fornitori esterni in merito a tutte le fasi del ciclo di vita di una rete.

(19) Sistemista Multipiattaforma (X-Systems Engineer). Un sistemista multipiattaforma secondo lo standard EUCIP deve avere una particolare competenza su vari sistemi operativi e sui rispettivi metodi per affrontare i problemi, sull'ottimizzazione delle prestazioni, sulla programmazione a livello di sistema e sull'integrazione tra piattaforme diverse; l'attitudine alla diagnosi e alla risoluzione dei problemi è richiesta per dare supporto su sistemi proprietari o aperti e su configurazioni ibride.

7. INDICATORI/MISURE DI QUALITÀ

La tabella Attività/Prodotti/Indicatori associa ad ogni attività e/o prodotto della fornitura gli indicatori di pertinenza descritti nelle schede successive.

NOTA – Per i documenti vanno considerati anche tutti gli indicatori presenti nel Processo di Documentazione.

Tabella 1 - Attività/Prodotti/Indicatori

Attività	Prodotto	Indicatore di qualità				Processo trasversale		
		Caratteristica	Sottocaratt.	acro IQ	Denominazione IQ	cod PT	acro PT	Denominazione PT
Analisi dei requisiti	Specifica dei requisiti	Funzionalità	Accuratezza	RSD	Rispetto degli standard documentali	6.1.1	PGD	Documentazione
Progettazione	Progetto del sistema	Funzionalità	Accuratezza	RSD	Rispetto degli standard documentali	6.1.1	PGD	Documentazione
Realizzazione del servizio	Progetto del servizio	Funzionalità	Accuratezza	RSD	Rispetto degli standard documentali	6.1.1	PGD	Documentazione
Realizzazione del servizio	Sistema di erogazione del servizio	Efficienza	Efficienza temporale	RSC	Rispetto della scadenza contrattuale	6.2.1	PGE	Gestione
Monitoraggio di sicurezza		Efficienza	Efficienza temporale	TES	Tempestività di escalation			
Gestione operativa delle emergenze		Efficienza	Efficienza temporale	TRE	Tempestività di risoluzione dell'emergenza			

Attività	Prodotto	Indicatore di qualità				Processo trasversale		
		Caratteristica	Sottocaratt.	acro IQ	Denominazione IQ	cod PT	acro PT	Denominazione PT
Gestione operativa delle emergenze	Rapporto di incidente	Funzionalità	Accuratezza	RSD	Rispetto degli standard documentali	6.1.1	PGD	Documentazione
Gestione operativa delle emergenze	Rapporto di incidente	Efficienza	Efficienza temporale	RSC	Rispetto della scadenza contrattuale	6.2.1	PGE	Gestione
Aggiornamento		Efficienza	Efficienza temporale	TAP	Tempestività aggiornamento periodico			
Aggiornamento		Funzionalità	Accuratezza	AAP	Accuratezza dell'aggiornamento periodico			
Aggiornamento		Funzionalità	Adeguatezza	EAG	Efficienza degli aggiornamenti			
Aggiornamento	Verbale di intervento	Funzionalità	Accuratezza	RSD	Rispetto degli standard documentali	6.1.1	PGD	Documentazione
Rendicontazione	Rapporto sulla sicurezza logica	Funzionalità	Accuratezza	RSD	Rispetto degli standard documentali	6.1.1	PGD	Documentazione
Rendicontazione	Rapporto sulla sicurezza logica	Efficienza	Efficienza temporale	RSC	Rispetto della scadenza contrattuale	6.2.1	PGE	Gestione

Classe di fornitura	GESTIONE DELLA SICUREZZA LOGICA
Caratteristica /Sottocaratteristica	Efficienza/Efficienza temporale
Indicatore/Misura	Tempestività di escalation – TES
Sistema di gestione delle misure	<p>Viene utilizzato uno strumenti di supporto al <u>monitoraggio</u>, in grado di raccogliere ed elaborare i dati elementari per fornire la misura degli indicatori, quali i sistemi di gestione di trouble ticketing e le console di monitoraggio della sicurezza.</p> <p>Mentre tutti gli eventi generati dal sistema di trouble ticketing vengono considerati ed analizzati, per quelli originati dalla console di monitoraggio, a livello contrattuale l'Amministrazione definirà i criteri per selezionare quelli da considerare rilevanti per questo indicatore.</p> <p>Per tutti gli eventi considerati nel periodo di osservazione, si misura il ritardo tra il tempo di presa in carico dell'evento ed il tempo di attivazione dell'<u>escalation</u> (avvio dell'attività di gestione delle emergenze).</p> <p>La criticità del monitoraggio è definita sulla base delle indicazioni contenute nella Tabella 1 e nella relativa nota.</p>
Unità di misura	Frequenza
Dati elementari da rilevare	<ul style="list-style-type: none"> • data e ora di presa in carico dell'evento • data e ora di avvio dell'escalation
Periodo di riferimento	3 mesi
Frequenza esecuzione misure	4 volte l'anno
Regole di campionamento	Si considerano tutti gli eventi relativi al periodo di osservazione, all'interno della finestra temporale definita per l'erogazione del servizio.
Formula di calcolo	<p>Dati necessari:</p> <ul style="list-style-type: none"> • data e ora di presa in carico dell'evento (T_i), al minuto • data e ora di avvio dell'escalation (T_e), al minuto <p>Il ritardo di avvio dell'escalation viene così calcolato:</p> $TES = T_e - T_i$ <p>Si calcola la frequenza dei ritardi inferiori al valore normale</p> $FN_{TES} = \frac{N_{\text{ritardi}}(\text{durata} \leq \text{valore normale})}{N_{\text{eventi}}} \times 100$ <p>e la frequenza dei ritardi inferiori al valore limite</p> $FL_{TES} = \frac{N_{\text{ritardi}}(\text{durata} \leq \text{valore limite})}{N_{\text{eventi}}} \times 100$
Regole di arrotondamento	<ul style="list-style-type: none"> • La durata dei ritardi va arrotondata al minuto • La frequenza va arrotondata al punto percentuale sulla base del primo decimale <ul style="list-style-type: none"> – al punto % per difetto se la parte decimale è $\leq 0,5$ – al punto % per eccesso se la parte decimale è $> 0,5$

<p>Obiettivi (valori soglia)</p>	<p>Obiettivi</p> <ul style="list-style-type: none"> • TES ≤ valore normale con $FN_{TES} \geq$ frequenza normale • TES ≤ valore limite con $FL_{TES} =$ frequenza limite <p>Valori soglia</p> <ul style="list-style-type: none"> • valore normale = 20 minuti per attività critiche • valore normale = 45 minuti per attività non critiche • valore limite = 4 ore per attività critiche • valore limite = 8 ore per attività non critiche <ul style="list-style-type: none"> • frequenza normale = 90% per attività di monitoraggio critiche • frequenza limite = 100% per attività di monitoraggio critiche <p>NOTA: La criticità del monitoraggio è definita sulla base delle indicazioni contenute nella Tabella 1 e nella relativa nota.</p>
<p>Azioni contrattuali</p>	<p>Per ogni riduzione dell'1% rispetto all'obiettivo si applica una penale dello 0,4% (per attività non critiche) e dello 0,8% (per attività critiche) dell'importo contrattuale del servizio relativo al periodo di riferimento.</p> <p>Per ogni evento per il quale si supera il valore limite si applica una penale di importo pari allo 0,2% dell'importo del servizio relativo al periodo di riferimento.</p>
<p>Eccezioni</p>	<p>L'applicazione delle regole contrattuali inizia dopo un periodo di osservazione dall'avvio del servizio della durata di 3 mesi</p>

Classe di fornitura	GESTIONE DELLA SICUREZZA LOGICA
Caratteristica /Sottocaratteristica	Efficienza/Efficienza temporale
Indicatore/Misura	Tempestività di risoluzione dell'emergenza – TRE
Sistema di gestione delle misure	Strumenti di supporto in grado di raccogliere ed elaborare i dati elementari per fornire la misura degli indicatori, quali i sistemi di gestione di trouble ticketing. Per tutti gli eventi considerati nel periodo di osservazione, si misura l'ampiezza del ritardo di risoluzione, ossia la differenza tra il tempo di presa in carico dell'emergenza (evento critico che necessita di una azione di tipo reattivo) ed il tempo di chiusura dell'intervento al netto dell'intervallo di tempo dell'eventuale autorizzazione a procedere che è data dall'interfaccia definita dall'Amministrazione tramite l'interfaccia delegata per i problemi di sicurezza.
Unità di misura	Percentuale
Dati elementari da rilevare	<ul style="list-style-type: none"> • data e ora di presa in carico dell'emergenza • data e ora di richiesta eventuale autorizzazione • data e ora di arrivo dell'eventuale autorizzazione • data e ora di chiusura intervento (risoluzione dell'emergenza)
Periodo di riferimento	3 mesi
Frequenza esecuzione misure	4 volte l'anno
Regole di campionamento	Si considerano tutti gli eventi relativi al periodo di osservazione, all'interno della finestra temporale definita per l'erogazione del servizio.
Formula di calcolo	<p>Dati necessari:</p> <ul style="list-style-type: none"> • data e ora di presa in carico dell'emergenza (<i>Tie</i>) • data e ora di richiesta eventuale autorizzazione (<i>Tra</i>) • data e ora di arrivo dell'eventuale autorizzazione (<i>Taa</i>) • data e ora di chiusura intervento (risoluzione dell'emergenza) (<i>Tee</i>) <p>Il tempo di risoluzione dell'emergenza viene così calcolato:</p> $TRE = (Tee - Tie) - (Taa - Trs)$ <p>Si calcola quindi la frequenza dei tempi inferiori al valore normale</p> $FN_{TRE} = \frac{N_{tempi(durata \leq \text{valore normale})}}{N_{eventi}} \times 100$ <p>e la frequenza dei tempi inferiori al valore limite</p> $FL_{TRE} = \frac{N_{ritardi(durata \leq \text{valore limite})}}{N_{eventi}} \times 100$
Regole di arrotondamento	<ul style="list-style-type: none"> • La durata dei ritardi va arrotondata al minuto • La frequenza va arrotondata al punto percentuale sulla base del primo decimale - al punto % per difetto se la parte decimale è $\leq 0,5$ - al punto % per eccesso se la parte decimale è $> 0,5$

<p>Obiettivi (valori soglia)</p>	<p>Obiettivi</p> <ul style="list-style-type: none"> • TRE ≤ valore normale con $FN_{TRE} \geq$ frequenza normale • TRE ≤ valore limite con $FL_{TRE} =$ frequenza limite <p>Valori soglia</p> <ul style="list-style-type: none"> • valore normale = 8 ore • valore limite = 48 ore • frequenza normale = 90% • frequenza limite = 100%
<p>Azioni contrattuali</p>	<ul style="list-style-type: none"> • per ogni riduzione dell'1% rispetto all'obiettivo si applica una penale dello 0,5% dell'importo contrattuale del servizio relativo al periodo di riferimento • per ogni evento per il quale si supera il valore limite si applica una penale di importo pari allo 0,2% dell'importo del servizio relativo al periodo di riferimento
<p>Eccezioni</p>	<p>L'applicazione delle regole contrattuali inizia dopo un periodo di osservazione dall'avvio del servizio della durata di 3 mesi</p>

Classe di fornitura	GESTIONE DELLA SICUREZZA LOGICA
Caratteristica /Sottocaratteristica	Efficienza/Efficienza temporale
Indicatore/Misura	Tempestività aggiornamento periodico – TAP
Sistema di gestione delle misure	Documenti che permettono il confronto dei tempi pianificati con i tempi effettivamente impiegati (Piano del servizio nella versione più aggiornata e Verbale di intervento). Il metodo di misura prevede il confronto tra i tempi pianificati per l'intervento di manutenzione ed i tempi risultanti dai verbali di intervento. Vanno considerati <ul style="list-style-type: none"> • gli interventi iniziati e terminati nel <u>periodo di osservazione corrente</u> • gli interventi iniziati nel <u>periodo di osservazione precedente</u> e terminati in quello <u>corrente</u>
Unità di misura	Percentuale
Dati elementari da rilevare	<ul style="list-style-type: none"> • Tempi pianificati per l'intervento • Tempi effettivi impiegati
Periodo di riferimento	6 mesi
Frequenza esecuzione misure	2 volte l'anno
Regole di campionamento	Tutti gli interventi eseguiti vengono verificati e confrontati con il piano
Formola di calcolo	Dati necessari <ul style="list-style-type: none"> • numero degli interventi eseguiti nel tempo pianificato, nel periodo di osservazione • numero degli interventi eseguiti, nel periodo di osservazione $TAP = \frac{N_{int_eseguiti_nel_tempo_pianificato}}{N_{int_eseguiti}} \times 100$
Regole di arrotondamento	La percentuale va arrotondata al mezzo punto percentuale sulla base del primo decimale <ul style="list-style-type: none"> - al mezzo punto % per difetto se la parte decimale è $\leq 0,25$ o compresa tra 0,5 e 0,75 - al mezzo punto % per eccesso se la parte decimale è compresa tra 0,25 e 0,5 o tra 0,75 ed il punto superiore
Obiettivi (valori soglia)	TAP ≥ 96
Azioni contrattuali	Per ogni 0,5% di TAP in meno rispetto all'obiettivo si applica una penale di importo compreso tra lo 0,1% e l'1% del corrispettivo del servizio relativo al periodo di riferimento
Eccezioni	L'applicazione delle regole contrattuali inizia dopo un periodo di avviamento stabilito contrattualmente

Classe di fornitura	GESTIONE DELLA SICUREZZA LOGICA
Caratteristica /Sottocaratteristica	Funzionalità/Accuratezza
Indicatore/Misura	Accuratezza dell'aggiornamento periodico – AAP
Sistema di gestione delle misure	<p>Verifica degli esiti dell'aggiornamento attraverso i verbali di intervento. Si registra il numero di apparecchiature aggiornate correttamente rispetto al totale delle apparecchiature su cui sono stati eseguiti gli interventi di manutenzione Vanno considerati</p> <ul style="list-style-type: none"> • gli interventi iniziati e terminati nel <u>periodo di osservazione corrente</u> • gli interventi iniziati nel <u>periodo di osservazione precedente</u> e terminati in quello <u>corrente</u>
Unità di misura	Percentuale
Dati elementari da rilevare	<ul style="list-style-type: none"> • Numero totale di apparecchiature oggetto di intervento • Numero di apparecchiature aggiornate correttamente
Periodo di riferimento	6 mesi
Frequenza esecuzione misure	2 volte l'anno
Regole di campionamento	Verifica su tutti gli interventi del periodo di osservazione
Formula di calcolo	<p>Dati necessari</p> <ul style="list-style-type: none"> • numero degli interventi pianificati eseguiti nel periodo di osservazione • numero delle apparecchiature correttamente aggiornate nel periodo di osservazione $AAP = \frac{N_{\text{apparecchiature_aggiornate_correttamente}}}{N_{\text{int}}} \times 100$
Regole di arrotondamento	<p>La percentuale va arrotondata al mezzo punto percentuale sulla base del primo decimale</p> <ul style="list-style-type: none"> - al mezzo punto % per difetto se la parte decimale è $\leq 0,25$ o compresa tra 0,5 e 0,75 - al mezzo punto % per eccesso se la parte decimale è compresa tra 0,25 e 0,5 o tra 0,75 ed il punto superiore
Obiettivi (valori soglia)	AAP ≥ 96
Azioni contrattuali	Per ogni 0,5% di AAP in meno rispetto all'obiettivo si applica una penale di importo compreso tra lo 0,1% e l'1% del corrispettivo del servizio relativo al periodo di riferimento
Eccezioni	L'applicazione delle regole contrattuali inizia dopo un periodo di avviamento stabilito contrattualmente

Classe di fornitura	GESTIONE DELLA SICUREZZA LOGICA
Caratteristica /Sottocaratteristica	Funzionalità/Adeguatezza
Indicatore/Misura	Efficienza degli aggiornamenti – EAG
Sistema di gestione delle misure	<p>Strumenti automatici in grado di raccogliere ed elaborare i dati elementari per fornire la misura degli indicatori. Per il periodo di osservazione previsto, si misura il rapporto tra il numero di aggiornamenti con esito positivo ed il numero di aggiornamenti totali effettuati. L'esito dell'aggiornamento può essere determinato, in maniera automatica o in maniera manuale, a seconda delle modalità definite per lo strumento utilizzato. Per esempio, l'esito dell'aggiornamento di un sistema di antivirus può essere verificato attraverso l'uso del virus di test standard EICAR. I log del sistema antivirus evidenzieranno o meno il corretto riconoscimento del virus di test, nonché la data e l'orario di aggiornamento.</p> <p>La data e l'ora di disponibilità dell'aggiornamento è quello ufficialmente indicato dal produttore dell'applicazione. Qualora il produttore non comunichi l'ora della distribuzione dell'aggiornamento, si utilizza la data e l'ora di ricezione della notifica di disponibilità dell'aggiornamento (per esempio notifica via posta elettronica).</p> <p>La criticità degli aggiornamenti è definita sulla base delle indicazioni contenute nella Tabella 1 e nella relativa nota.</p>
Unità di misura	Tempo
Dati elementari da rilevare	<ul style="list-style-type: none"> • numero di aggiornamenti disponibili (per esempio disponibilità di nuovo aggiornamento dell'antivirus) • data e ora della disponibilità dell'aggiornamento • data e ora di conclusione delle operazioni di aggiornamento • esito dell'aggiornamento
Periodo di riferimento	3 mesi
Frequenza esecuzione misure	4 volte l'anno
Regole di campionamento	<p>Si considerano tutti gli aggiornamenti relativi al periodo di osservazione. Nel caso di due aggiornamenti disponibili a distanza di tempo inferiore al valore soglia, si considera solo l'ultimo aggiornamento.</p> <p>Per esempio, nel caso si rendano disponibili due diversi aggiornamenti di tipo non critico, il primo alle 10:00 ed il secondo alle 17:30, sarà considerato per il calcolo della misura solo l'aggiornamento delle 17:30.</p>

<p>Formula di calcolo</p>	<p>Dati necessari:</p> <ul style="list-style-type: none"> • numero di aggiornamenti disponibili • data e ora della disponibilità dell'aggiornamento (<i>Tda</i>) • data e ora di conclusione delle operazioni di aggiornamento (<i>Tca</i>) • esito dell'aggiornamento <p>Il ritardo di aggiornamento viene così calcolato:</p> $EAG = Tca - Tda$ <p>Si calcola quindi la frequenza degli aggiornamenti con ritardi inferiori al valore normale</p> $FN_{EAG} = \frac{N_{agg}(\text{ritardo} \leq \text{valore normale})}{N_{totale \text{ aggiornamenti}}} \times 100$ <p>e la frequenza di quelli inferiori al valore limite</p> $FL_{EAG} = \frac{N_{agg}(\text{ritardo} \leq \text{valore limite})}{N_{totale \text{ aggiornamenti}}} \times 100$
<p>Regole di arrotondamento</p>	<ul style="list-style-type: none"> • Il ritardo va arrotondato al minuto • La frequenza va arrotondata alla frazione di punto percentuale sulla base del primo decimale <ul style="list-style-type: none"> - al punto % per difetto se la parte decimale è $\leq 0,5$ - al punto % per eccesso se la parte decimale è $> 0,5$
<p>Obiettivi, valori soglia</p>	<p>Obiettivi</p> <ul style="list-style-type: none"> • EAG \leq valore normale con $FN_{EAG} \geq$ frequenza normale • EAG \geq valore limite con $FL_{EAG} \geq$ frequenza limite <p>Valori soglia</p> <ul style="list-style-type: none"> • valore normale = 30 minuti per gli aggiornamenti critici • valore normale = 3 giorni per gli aggiornamenti non critici • valore limite = 90 minuti per gli aggiornamenti critici • valore limite = 7 giorni per gli aggiornamenti non critici • frequenza normale = 95% • frequenza limite = 100% <p>NOTA: La criticità degli aggiornamenti è definita sulla base delle indicazioni contenute nella Tabella 1 e nella relativa nota.</p>
<p>Azioni contrattuali</p>	<ul style="list-style-type: none"> • per ogni riduzione dello 0,5% rispetto alla frequenza normale, si applica una penale dello 0,1% dell'importo contrattuale. • per ogni evento per il quale si supera il valore limite si applica una penale di importo pari allo 0,2% dell'importo del servizio relativo al periodo di riferimento nel caso di aggiornamenti critici e dello 0,1% per gli aggiornamenti non critici.
<p>Eccezioni</p>	<p>L'applicazione delle regole contrattuali inizia dopo un periodo di osservazione dall'avvio del servizio della durata di 3 mesi.</p> <p>L'indicatore è applicabile solo ai sistemi che erogano il servizio in maniera centralizzata, ovvero sono esclusi i servizi rivolti alle postazioni lavoro.</p>

8. GLOSSARIO

Proxy

I sistemi proxy (dall'inglese mandato, procura) sono dispositivi che realizzano una separazione della comunicazione tra un'applicazione client (per esempio un browser web) ed un server remoto (per esempio un server web). Le tipologie di proxy più diffuse separano il traffico al livello applicativo, consentendo un alto livello di sicurezza; in questo caso si usa anche il termine "Application Proxy" o "Application Gateway". I sistemi proxy sono tipicamente posizionati tra la rete interna ed Internet, proteggendo gli utenti durante la navigazione web e limitando l'esposizione alle minacce esterne al solo sistema proxy. Mediante opportuni meccanismi di conservazione in locale dei contenuti maggiormente acceduti, i sistemi proxy possono accelerare la navigazione web.

Virus

È correntemente utilizzato come termine generico per classificare software malevoli in grado di replicarsi in maniera autonoma. Generalmente, al verificarsi di determinati eventi, un virus può arrecare danni di varia entità sui sistemi infettati.

Worm

Simili ai virus, se ne differenziano per le modalità e le tecniche utilizzate per diffondersi.

Spyware

Correntemente si definisce spyware una tecnologia, tipicamente software, volta alla raccolta e trasmissione di informazioni private. Di solito gli spyware agiscono in modo invisibile e trasmettono le informazioni a soggetti ostili. A causa della diversa sensibilità dei vari Paesi in materia di tutela della privacy, queste tecnologie non sono sempre adeguatamente e legalmente perseguite.

Falso negativo

Classificazione erronea di un'unità che possiede un dato attributo alla categoria che esprime il non possesso dell'attributo. In questo contesto, un falso negativo è un evento significativo non segnalato dallo strumento di rilevazione.

Falso positivo

Classificazione di unità statistiche in base ad un determinato attributo; si dice falso positivo l'attribuzione erronea al gruppo delle unità che possiedono l'attributo di un'unità che non lo possiede. In questo contesto, un falso positivo è un evento non significativo segnalato con un allarme dallo strumento di rilevazione.