Procedura Operativa

Security Assessment e Vulnerability Management

Poste Italiane

Redazione	Alessandra Toma	CA/TA/SI/SMI
Verifica	Nicola Sotira Enrico Di Benedetto Luca Luminoso Armando Salvatori Paolo Di Martino Fabio Sensidoni Giuliano Brignola Luigi Belcamino	CA/TA/CERT SI/CTO/CTOCO SI/CTO SI/TCCAT SI/ESITC SI/ESSD SI/ESITT SI/STLC
Approvazione	Rocco Mammoliti	CA/TA/SI

N. Versione	Data di Approvazione	Paragrafi modificati	Motivazioni dell'aggiornamento
1.0	20/01/2019		Prima stesura
1.1	11/04/2019	Tutti	Aggiornamento template e revisione complessiva dei contenuti.
1.2	15/05/2019	Cap. 4	Recepimento dei contributi da parte delle Funzioni aziendali interessate.

Sommario

Documento ad uso interno

Le informazioni contenute nel presente documento possono essere acquisite ed utilizzate dal personale aziendale con ordinaria diligenza per esclusive finalità lavorative, consapevole che queste costituiscono un bene da proteggere. È quindi vietato qualsiasi utilizzo delle stesse per finalità personali.

I documenti “ad uso interno” possono circolare liberamente nell’ambito di Poste Italiane ma non sono destinati alla diffusione.

L’eventuale divulgazione esterna può risultare inopportuna rispetto agli interessi aziendali. Pertanto, a tal fine è necessario richiedere un’autorizzazione al responsabile della classificazione.

Introduzione

Nel corso della vita di un'infrastruttura tecnologica o di un servizio, può sorgere la necessità di apportare modifiche sostanziali che possono introdurre nuovi scenari di rischio o diversamente, possono modificarsi i fattori esterni che introducendo nuove minacce possono incidere sulle infrastrutture/servizi in essere.

A fronte di nuove necessità, occorre adottare mezzi appropriati per mantenere le infrastrutture ed i servizi ad un livello di sicurezza adeguato al rischio al quale essi sono esposti. In tal senso è pertanto necessario dotarsi di strumenti che permettano di monitorare lo stato della sicurezza e di intervenire a fronte di situazioni di rischio. Inoltre, nel corso di realizzazione di nuovi servizi, e prima del rilascio produzione, è indispensabile effettuare le attività di verifica sulla sicurezza di quanto realizzato.

1 Obiettivi, ambito di applicazione e modalità di recepimento

L'obiettivo della presente procedura è di governare il processo relativo alle attività operative di Security Assessment e Vulnerability Management effettuate dalle diverse Funzioni aziendali di Poste Italiane, in funzione dei rispettivi ambiti di competenza, al fine di:

- realizzare una gestione integrata delle attività e consentire altresì di ottimizzare la pianificazione e le risorse coinvolte;
- estendere progressivamente il perimetro di analisi e verifica;
- facilitare la risposta di Poste Italiane nei confronti degli adempimenti obbligatori derivanti da normative, certificazioni di settore e accreditamenti per l'erogazione di servizi ai propri Clienti;
- garantire una visione e gestione integrata ed unitaria dei profili di rischio informatico dei sistemi ICT utilizzati nel contesto aziendale.

Tali attività vengono coordinate centralmente dalla Funzione *Responsabile del Governo della Sicurezza Informatica di Poste Italiane*[1] in termini di pianificazione, identificazione delle priorità e monitoraggio dei piani di rientro.

Esse vengono condotte periodicamente con particolare riferimento ai seguenti ambiti e partecipano alla determinazione dello stato della sicurezza dei sistemi ICT di Poste Italiane, rilevandone le eventuali vulnerabilità tecniche e fornendo le indicazioni necessarie alla stesura dei piani correttivi di intervento.

Le attività sono classificabili in:

- **Verifiche tecniche di sicurezza nel ciclo di vita dei progetti:** Penetration Test e Secure Code Review (statica e dinamica) e Vulnerability Assessment (VA) infrastutturali eseguiti in ambienti e fasi di pre-produzione, sia in relazione ai processi AI – Acquisizione e Implementazione (AI3 Lavorazione Iniziative prevalentemente applicative e AI6 – Delivery Management) che sulla base di campagne di verifica puntuali;
- **Goal-Oriented Penetration Test**, condotti sui sistemi in produzione esposti sulla rete interna (Intranet) ed esterna (Internet) relativi a servizi di particolare rilevanza o criticità, e sulle applicazioni mobili;
- **Penetration test a campione,** attivati a fronte di attività non pianificate derivanti da segnalazioni di nuove vulnerabilità (fonti interne ed esterne di varia natura), o sostanziali

[1] cfr. ALLEGATO 1: Transcodifica Ruoli-Strutture Aziendali-Sigle Organizzative.

mutamenti dello scenario delle minacce cui sistemi e servizi sono esposti, o a seguito di rilevazione di incidenti;

- **Assessment di Sicurezza sulle Terze Parti,** effettuati in conformità a quanto previsto dai contratti e dalle normative di riferimento;
- **Continuous Monitoring** costituito da:
  - Vulnerability Assessment (VA) infrastutturali sui sistemi in produzione condotti sulla rete interna (intranet) e su quella esterna (internet);
  - Assessment sul Mainframe.
- **Monitoraggio di tutti i Piani di Rientro** risultanti dalle suddette attività di Security Assessment e Vulnerability Management.

La procedura definisce infine le modalità operative e le responsabilità inerenti al processo di gestione delle attività di Security Assessment e Vulnerability Management necessarie per verificare il livello di adeguatezza del sistema di protezione mentre la risoluzione delle vulnerabilità rilevate è prevista nell'ambito dei processi di Change Management.

Il Documento si applica a Poste Italiane S.p.A. e costituisce una best practice di riferimento per le Società Controllate.

Le attività descritte nel presente documento e svolte dalle Funzioni aziendali interessate possono essere oggetto di distinte procedure e istruzioni operative puntuali, che devono essere in ogni caso strettamente conformi alla presente procedura.

L'insieme di tali documenti, ivi compresa la presente procedura, costituisce parte del sistema documentale centralizzato e specifico del modello di Information Security Governance di Poste Italiane, gestito dalla Funzione *Responsabile del Governo della Sicurezza Informatica di Poste Italiane*.

Tale sistema è puntualmente aggiornato in funzione delle evoluzioni organizzative e dei relativi impatti sulle attività operative di Security Assessment e Vulnerability Management, al fine di costituire e mantenere nel tempo un unico impianto documentale di riferimento ed una knowledge-base per le suddette attività.

2 Definizioni, abbreviazioni e acronimi

Si rimanda all'Allegato 1: Transcodifica Strutture Aziendali-Sigle Organizzative, per le definizioni e gli acronimi di carattere organizzativo; in particolare, obiettivo dell'allegato è quello di associare ogni ruolo (indicato in corsivo) alle funzioni aziendali di riferimento.

Di seguito sono invece riportate le tabelle che descrivono gli acronimi, le abbreviazioni e le definizioni usate nel documento.

Acronimi

Acronimo/abbreviazione	Descrizione
SdG	Società del Gruppo
CA	Corporate Affairs
CA/GRG/PSG	Corporate Affairs/Governo dei Rischi di Gruppo/Presidio Sistemi di Gestione
CA/TA	Corporate Affairs/Tutela Aziendale
CA/TA/SI	Corporate Affairs/Tutela Aziendale/Sicurezza Informatica
CA/TA/CERT	Corporate Affairs/Tutela Aziendale/Computer Emergency Response Team
SI	Sistemi Informativi
SI/CTO/CTOCO	Sistemi Informativi/Chief Technology Officer/CTO Continuity Operations
SI/ESITC	Sistemi Informativi/ Esercizio e Supporto IT Centrale
SI/ESSD	Sistemi Informativi/Esercizio e Supporto Servizi Digitali
SI/STLC	Sistemi Informativi/Servizi TLC
SI/ESITT	Sistemi Informativi/ Esercizio e Supporto IT Territoriale
PI	Poste Italiane S.p.A.
PT	Penetration Test
VA	Vulnerability Assessment
CCNL	Contratto Collettivo Nazionale di Lavoro

Definizioni

Termine	Definizione
Security Assessment	Attività mirate alla valutazione del rischio IT. Nell'ambito di tale attività e limitatamente al presente documento, sono comprese quelle mirate alla valutazione del rischio tecnologico rilevato, con particolare riferimento alle seguenti: • Vulnerability Assessment; • Penetration Test; • Secure Code Review; Assessment di Sicurezza sulle terze parti.
Vulnerability Assessment	Attività che consiste nell'identificare le vulnerabilità presenti sui sistemi prima che vengano messi in produzione oppure controllare con continuità quelle presenti su sistemi già rilasciati in produzione. I Vulnerability Assessment forniscono una fotografia dello stato di esposizione dei sistemi a vulnerabilità note. A questo scopo, vengono utilizzati tool automatici, attraverso i quali è possibile effettuare scansioni che permettono di conoscere dettagli riguardanti configurazioni ed eventuale presenza di vulnerabilità.
Secure Code Review	Analisi del codice sorgente (analisi statica) e del codice applicativo eseguibile (analisi dinamica) al fine di identificarne le vulnerabilità dovute ad una programmazione non corretta in termini di sicurezza o alla mancata aderenza a normative o best practice di settore. Tale attività è finalizzata a ridurre il rischio derivante dalla presenza di vulnerabilità di sicurezza nelle applicazioni prima che queste siano rilasciate in ambiente di Produzione.
Penetration Test	Processo di valutazione del livello di sicurezza di un sistema simulando l'attacco di un utente malintenzionato. I PT forniscono un dettaglio delle vulnerabilità sfruttabili e delle modalità di sfruttamento, andando a verificare la possibilità, per un attaccante attestato sulla intranet e/o su internet, di accedere alle componenti di un sistema, aggirando i meccanismi di protezione e/o le logiche applicative. Le verifiche vengono svolte in ragione dell'obiettivo e del contesto con il fine di rilevare vulnerabilità non note e, comunque, non verificabili attraverso gli strumenti di analisi e scansione automatica.
Assessment di Sicurezza sulle terze parti	Attività relative alle verifiche di seconda parte effettuate da PI nei confronti dei propri fornitori, finalizzate a riscontrare il livello di conformità e la corretta applicazione delle misure di sicurezza (tecniche e organizzative) adottate dagli stessi, rispetto alle normative applicabili, agli standard internazionali in ambito sicurezza informatica (es. ISO/IEC 27001, PCI-DSS, COBIT, NIST), alle best practices adottate dal fornitore in materia di sicurezza delle informazioni ed alle indicazioni fornite da Poste Italiane in conformità a quanto previsto negli accordi/contratti stipulati con le terze parti.
Valutazione del rischio tecnologico rilevato	Attività che consente di valutare il rischio tecnologico al quale sono esposte le piattaforme IT, attraverso le rilevazioni effettuate mediante attività di Security Assessment e Vulnerability Management.

3 Principi di riferimento

Le attività disciplinate dal presente documento devono essere svolte nel rispetto delle vigenti disposizioni di legge nonché dei principi e delle regole di comportamento contenuti nel Codice Etico del Gruppo Poste Italiane e negli altri strumenti normativi aziendali[2].

TRACCIABILITÀ – Le persone coinvolte nel processo devono garantire, ciascuna per la parte di propria competenza, la tracciabilità delle attività e dei documenti inerenti al processo, assicurandone l'individuazione e la ricostruzione delle fonti, degli elementi informativi e dei controlli effettuati che supportano le attività.

SEGREGAZIONE DI COMPITI E ATTIVITÀ – Il prevede la segregazione di compiti e responsabilità, tra unità organizzative distinte o all'interno delle stesse, al fine di evitare che attività incompatibili risultino concentrate sotto responsabilità comuni.

CONFORMITÀ ALLE LEGGI E COERENZA CON IL QUADRO NORMATIVO DI RIFERIMENTO GENERALE – Il processo è definito nel rispetto delle normative applicabili, in coerenza con il quadro di riferimento generale composto a titolo esemplificativo da: Statuto, Codice Etico, sistema organizzativo, sistema di poteri e deleghe, etc..

POTERI AUTORIZZATIVI – Gli strumenti normativi devono assicurare specifici livelli autorizzativi o di supervisione commisurati alle caratteristiche o alla tipologia delle transazioni.

RISERVATEZZA – Fermi restando la trasparenza delle attività poste in essere e gli obblighi di informazione imposti dalle disposizioni vigenti, le persone che operano nel processo assicurano la riservatezza richiesta dalle circostanze per ciascuna notizia / informazione appresa in ragione della propria funzione lavorativa".

CONFLITTO DI INTERESSI - Le persone coinvolte nel processo agiscono nei confronti delle controparti secondo rapporti improntati ai più alti livelli dell'etica di comportamento, nel rispetto del Codice Etico, evitando di assumere decisioni e di svolgere attività, in conflitto, anche solo potenziale con gli interessi dell'Azienda o comunque in contrasto con i propri doveri d'ufficio.

CONDOTTA ANTI-CORRUZIONE - La corruzione è proibita senza alcuna eccezione. Nel dettaglio, è vietato di (a) offrire, promettere, dare, pagare, autorizzare qualcuno a dare o pagare, direttamente o indirettamente, una qualunque cosa di valore o altra utilità ad un Pubblico Ufficiale o privato; (b) accettare o sollecitare, o autorizzare qualcuno ad accettare o sollecitare, direttamente o indirettamente, una qualunque cosa di valore o altra utilità da un Pubblico Ufficiale o un privato, quando, in entrambi i casi, l'intenzione sia di (i) indurre un Pubblico Ufficiale o un privato a esercitare, in maniera impropria, una funzione pubblica o svolgere, in maniera impropria, qualsiasi attività connessa a un business o ricompensarli per averle effettuate; (ii) influenzare un'azione od omissione da parte di un Pubblico Ufficiale o una sua qualsiasi decisione in violazione di un atto dovuto; (iii) ottenere, assicurarsi o mantenere un business o un vantaggio nella conduzione dell'attività d'impresa; o (iv) in ogni caso violare le leggi applicabili.

AUTONOMIA SOCIETARIA DELLE CONTROLLATE – È garantita l'autonomia societaria delle controllate per quanto attiene l'istituzione e il mantenimento di un processo adeguato e funzionante, nel rispetto degli indirizzi di direzione e coordinamento definiti da Poste Italiane".

AUTONOMIA ORGANIZZATIVA, GESTIONALE E DEL SISTEMA DEI CONTROLLI INTERNI DEL PATRIMONIO BANCOPOSTA – In conformità alle Disposizioni di Vigilanza, l'assetto organizzativo e di governo societario del Patrimonio BancoPosta si ispira al principio dell'autonomia organizzativa, gestionale e del sistema dei controlli interni.

[2] L'inosservanza dei principi contenuti nel presente documento normativo potrà comportare l'applicazione delle misure sanzionatorie contenute nel sistema disciplinare del CCNL.

APPROCCIO BASATO SUI RISCHI E SUI PROCESSI – Il Security Assessment e Vulnerability Management è ispirato a una logica per processi, si basa su un approccio preventivo ai rischi, contribuendo all'assunzione di decisioni consapevoli, e, ove possibile, alla traduzione dei principali rischi in opportunità.

RESPONSABILIZZAZIONE MANAGEMENT – Il management, nell'ambito delle funzioni ricoperte e nel conseguimento dei correlati obiettivi, garantisce l'applicazione del processo per le attività di competenza, partecipando attivamente al suo funzionamento.

COMUNICAZIONE E FLUSSI INFORMATIVI – A ogni organo e struttura aziendale sono rese disponibili le informazioni necessarie per adempiere alle proprie responsabilità, incluse quelle in materia di Sistema di Segnalazione delle Violazioni.

CULTURA DEL RISCHIO E DEL CONTROLLO – Il processo diffonde la cultura del rischio e del controllo, intesa come l'insieme delle norme di comportamento che determinano la capacità collettiva e dei singoli di identificare, misurare e mitigare i rischi attuali e futuri dell'organizzazione.

COERENZA CON OBIETTIVI AZIENDALI – Il processo contribuisce a una conduzione dell'impresa volta allo sviluppo sostenibile, alla massimizzazione del valore dell'azienda e coerente con gli obiettivi aziendali.

4 Oggetto del documento

4.1 Descrizione delle attività

Le attività di Security Assessment e Vulnerability Management hanno lo scopo di:

- verificare la conformità dei sistemi alle policy e procedure definite, ossia la loro effettiva e corretta applicazione;
- verificare l'adeguatezza delle misure implementate, ossia il loro effettivo grado di efficacia, efficienza e robustezza;
- valutare il livello di rischio tecnologico rilevato delle piattaforme ICT.
- fornire le indicazioni necessarie per l'implementazione delle azioni correttive atte a minimizzare il rischio (piani di rientro). Lo svolgimento di tali attività viene assicurato attraverso l'individuazione delle priorità di intervento in ambito Poste Italiane ed una pianificazione puntuale delle suddette attività.

Le attività di Security Assessment e Vulnerability Management dei sistemi e delle applicazioni di Poste Italiane sono svolte con strumenti diversi e da Funzioni aziendali differenti, in funzione della specifica competenza aziendale. La seguente figura sintetizza le attività operative di Security Assessment e Vulnerability Management realizzate, in relazione ai seguenti ambiti operativi individuati:

a. Continuous Monitoring;
b. Verifiche Tecniche di Sicurezza nel ciclo di vita dei progetti;
c. Goal-Oriented Penetration Test;
d. Assessment di Sicurezza sulle Terze parti;
e. Penetration Test a campione.

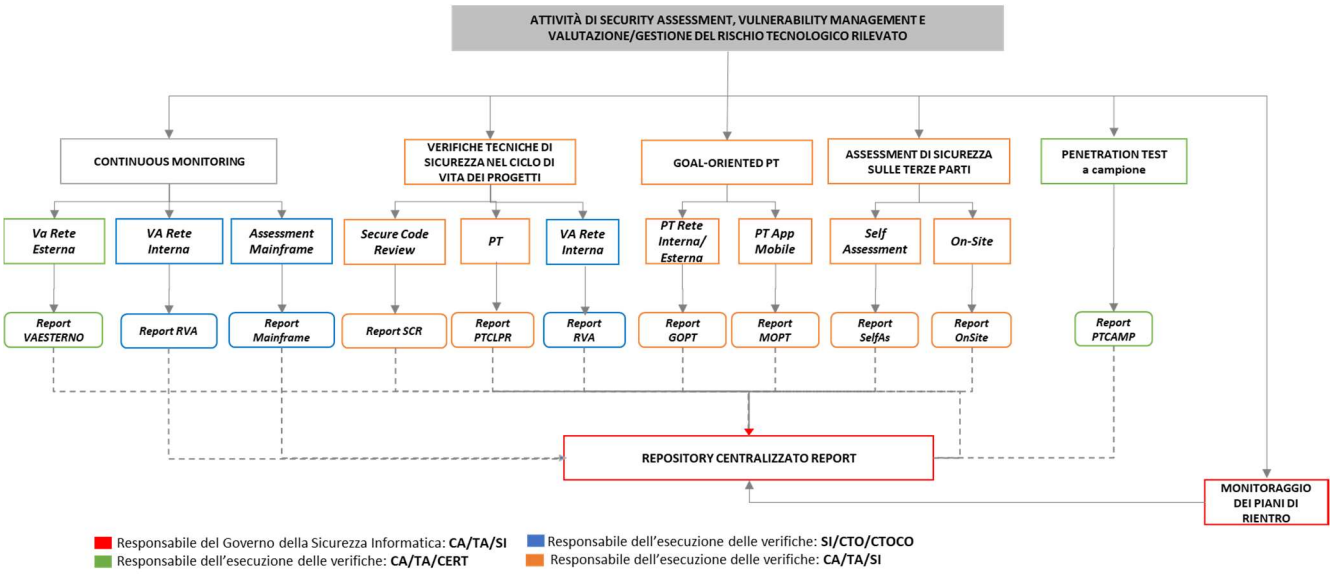

Figura 1 - Security Assessment e Vulnerability Management: ambiti operativi e attività

Le attività sono effettuate tramite l'ausilio di strumenti automatici e manuali e sono finalizzate a:

- il rilevamento delle vulnerabilità;
- la classificazione del grado di rischio associato allo sfruttamento della vulnerabilità;
- l'individuazione delle azioni correttive per minimizzare il rischio.

La descrizione puntuale di tali attività è riportata nei paragrafi successivi, in relazione agli ambiti operativi sopra individuati.

4.1.1 Continuous Monitoring

Tale ambito di verifica comprende le seguenti attività:

- Vulnerability Assessment (VA) infrastrutturali sui sistemi in produzione esposti sulla rete interna di Poste Italiane;
- Vulnerability Assessment (VA) infrastrutturali sui sistemi attestati sulla rete esterna;
- Assessment sui Mainframe.

La metodologia utilizzata da Poste Italiane per l'attività di VA infrastrutturale è conforme ai principali standard internazionali in materia [4][5][6][11].

Le fasi principali dell'attività relativa ai VA riguardano:

- Host Identification - analisi della rete al fine di determinare i sistemi attivi ed individuazione della versione del Sistema Operativo installato, inviando richieste ai sistemi stessi od ottenendo le informazioni dai server DNS esterni o interni;
- Enumerazione dei Servizi e Identificazione delle Vulnerabilità – analisi degli host attivi, al fine di determinare quali porte risultano essere aperte e quindi quali servizi risultano essere in ascolto. Per ogni servizio rilevato deve essere identificata la versione del software associato, al fine di effettuare test di verifica della presenza delle vulnerabilità che potrebbero essere sfruttate, per ottenere un accesso non autorizzato ai sistemi.

Le verifiche di VA avvengono secondo le seguenti fasi principali:

- configurazione dei tool software;
- esecuzione dei test automatici (scansione) - volti all'individuazione di porte e servizi accessibili, bug software errori di configurazione, etc.;
- analisi delle vulnerabilità rilevate al fine di eliminare i falsi positivi;
- documentazione delle risultanze della verifica.

4.1.1.1 VA Rete interna (Intranet)

Tali Vulnerability Assessment sono condotti in modalità continuativa con periodicità mensile dalla competente *Funzione Responsabile dell'esecuzione delle verifiche*, sulla componente infrastrutturale ed in

particolare sui server in produzione/disaster recovery e sui sistemi appartenenti al perimetro a supporto dei Servizi Digitali, esposti sulla rete interna. Le medesime attività vengono svolte sui server in sviluppo/collaudo e in certificazione, quando previste nell'ambito delle iniziative progettuali (OTE), ossia nei casi di OTE con una criticità media o elevata (MC, EC).

Tali attività prevedono la produzione di un Report ad hoc (c.d. Report RVA). Il report viene utilizzato e gestito per le attività di competenza da parte della Funzione che esegue l'attività e viene inviato alla *Funzione Responsabile del Governo della Sicurezza informatica*, che provvederà per le attività di propria pertinenza, ad effettuare la valutazione del rischio tecnologico rilevato delle piattaforme IT.

4.1.1.2 VA Rete esterna (Internet)

Tali attività vengono condotte periodicamente dalla *Funzione Responsabile dell'esecuzione delle verifiche*, sulla componente infrastrutturale dei sistemi attestati sulla rete esterna.

Tali attività prevedono la produzione di un Report ad hoc. Il report viene utilizzato e gestito per le attività di competenza da parte della Funzione che esegue l'attività e viene inviato *alla Funzione Responsabile del Governo della Sicurezza informatica*, che provvederà per le attività di propria pertinenza, ad effettuare la valutazione del rischio tecnologico rilevato delle piattaforme IT.

4.1.1.3 Assessment Mainframe

Gli Assessment in ambito Mainframe vengono effettuati trimestralmente. Tali Assessment tengono conto di una serie di requisiti di sicurezza individuati dalla *Funzione Responsabile del Governo della Sicurezza informatica* ed assicurati dalla *Funzione Responsabile dell'esecuzione delle verifiche*, in relazione allo specifico ambito.

I controlli prevedono normalmente le seguenti macrocategorie di verifica:

- Audit;
- Disponibilità;
- Integrità;
- Scambio dati sicuro;
- Oscuramento dei dati;
- Autorizzazione e controllo accessi;
- Identificazione ed autenticazione;
- Development.

4.1.2 Verifiche Tecniche di Sicurezza nel Ciclo di Vita dei Progetti

Le attività incluse in tale ambito sono effettuate negli ambienti di sviluppo/collaudo/certificazione preventivamente alla messa in produzione del servizio. La tipologia delle verifiche da effettuare è definita in funzione del tipo di applicazione, della criticità dei dati trattati e/o del valore di business. Le verifiche di

sicurezza sono effettuate sia per le applicazioni di tipo tradizionale (es applicazioni web, applicazioni legacy) che per le applicazioni di tipo Mobile.

Le verifiche in oggetto sono classificabili in:

- **Secure Code Review Statica**: analisi del codice sorgente (analisi statica) finalizzata ad individuarne le vulnerabilità dovute ad una programmazione non corretta in termini di sicurezza. L'analisi statica viene condotta sul codice sorgente di proprietà di Poste Italiane e sul codice sorgente di proprietà di terze parti, previa autorizzazione da parte di quest'ultime;
- **Secure Code Review Dinamica**: analisi condotta sul codice applicativo eseguibile (analisi dinamica) e/o sui servizi esposti verso altri sistemi. Tale analisi presuppone che tutte le componenti supportino il protocollo applicativo *http/https*;
- **Penetration Test**: insieme di attività basate sull'esecuzione controllata delle strategie e delle tecniche di attacco messe in atto da ipotetici criminali informatici, allo scopo di individuare eventuali vulnerabilità presenti nei sistemi in pre-produzione, rilevabili esclusivamente tramite tecniche di inferenza umana. Tale attività include l'esecuzione preliminare di Vulnerability Assessment (interno ed esterno) secondo le best practice internazionali e la regolamentazione specifica dei singoli servizi applicativi da testare.
- **VA Rete Interna** (cfr par. 4.1.1.1)

La metodologia utilizzata per l'esecuzione delle attività è conforme ai seguenti Standard:

- Open Web Application Security Project (di seguito OWASP) 2017, standard internazionale per lo sviluppo sicuro delle applicazioni;
- CWE-SANS Top 25 (Common Weakness Enumeration - SysAdmin, Audit, Networking, and Security) 2011: standard internazionale per aspetti di dead code e best practices;
- SQALE (Software Quality Assessment based on Lifecycle Expectations): metodologia internazionale per la valutazione del codice sorgente di un'applicazione;
- CVSS (Common Vulnerability Scoring System): per l'assegnazione delle severity e dello score delle vulnerabilità riscontrate.

4.1.3 Goal Oriented Pentest

Le attività comprese in tale ambito vengono condotte sui sistemi in produzione dalla *Funzione Responsabile dell'esecuzione delle verifiche*[3] e sono finalizzate ad individuare attacchi mirati e vulnerabilità[4], anche non note, che consentono di compromettere l'infrastruttura e i relativi dati gestiti e riguardano in particolare:

- la conduzione in modalità black-box di Penetration Test sui sistemi in produzione che erogano servizi di particolare criticità o rilevanza aziendale sulla rete interna e sulla rete esterna;

[3] cfr. ALLEGATO 1: Transcodifica Ruoli-Strutture Aziendali-Sigle Organizzative.

[4] Per vulnerabilità si intende qualunque caratteristica intrinseca dei sistemi, degli applicativi e delle infrastrutture trasversali sfruttabile da un agente di minaccia, al fine di concretizzare una minaccia alla Riservatezza, Integrità e Disponibilità (RID) del patrimonio tecnologico ed informativo aziendale.

- la conduzione di Penetration Test e Vulnerability Assessment sulle applicazioni mobili con strumenti manuali e automatici.

Le verifiche di PT avvengono secondo le seguenti fasi principali:

- information gathering - ha lo scopo di ottenere informazioni relative al sistema o alla rete ed alle vulnerabilità presenti, può essere svolto sia attraverso l'esecuzione dei test automatici (Vulnerability Assessment), sia con l'acquisizione di documenti ed altre informazioni fornite agli attaccanti (modalità di test white/grey box);
- analisi delle vulnerabilità rilevate al fine di individuare obiettivi da investigare in profondità;
- fase di attacco, avente lo scopo di ottenere, se possibile, pieni privilegi al sistema ed eventualmente ad altri sistemi che condividono la rete;
- documentazione delle risultanze della verifica. Ad ognuna delle vulnerabilità rilevate durante le attività di verifica è assegnato un livello di rischio stimato qualitativamente tramite una scala a 5 valori (Low, Medium, Medium-High, High, Critical) sulla base della probabilità di sfruttamento della vulnerabilità stessa e dai potenziali impatti.

Per svolgere le attività di Penetration Test sulle applicazioni, Poste Italiane utilizza una metodologia ormai consolidata nella comunità scientifica internazionale e riassunta all'interno dell'Open Web Application Security Project (OWASP) [9], organizzazione di riferimento per la sicurezza delle web application.

Per il Penetration Test delle applicazioni mobili di Poste Italiane il riferimento è normalmente costituito dall' Open Web Application Security Project Mobile Security Testing [12], a meno di esigenze specifiche delle Funzioni interessate, derivanti da indicazioni ricevute in merito da parte di Enti di accreditamento, Organismi di Vigilanza ed Enti certificatori, funzionali al mantenimento degli accreditamenti, delle autorizzazioni e delle certificazioni in possesso di Poste Italiane.
Particolare attenzione deve essere riservata, in fase di testing, alle classi di vulnerabilità rientranti tra le 10 vulnerabilità più importanti come diffusione e impatto sui sistemi, facenti parte della OWASP Top 10 [13].
L'esecuzione periodica dei VA/PT sulle applicazioni mobili (di seguito anche «App») di Poste Italiane e delle società del gruppo, si propone in particolare di:

- prevenire eventuali violazioni di sicurezza;
- prevenire esposti dei Clienti per illeciti riconducibili all'uso di App direttamente, indirettamente o in modo presunto collegate a Poste Italiane e/o alle Società del Gruppo;
- prevenire danni diretti e indiretti (es. incidenti di sicurezza, danno d'immagine) dovuti ad un utilizzo improprio delle App o dei marchi;
- tutelare la proprietà intellettuale (es. codice sorgente).

Tale servizio si rivolge a tutte le App che:

- espongono marchi riconducibili a Poste Italiane e/o alle società del Gruppo;
- sono sviluppate da e/o per conto del Gruppo Poste Italiane o da Terzi su iniziativa individuale non autorizzata;
- offrono funzionalità che prevedono il trattamento dei dati dei Clienti e sono fruibili non solo mediante market ufficiali, quali Google Play e Apple Store, ma anche attraverso market alternativi.

4.1.4 Assessment di Sicurezza sulle Terze Parti

Gli Assessment di sicurezza sulle terze parti, ove previsti dai contratti e dalle normative di riferimento, sono svolti dalla *Funzione Responsabile dell'esecuzione delle verifiche* che provvederà ad inserirli all'interno del piano programmatico annuale.
Tali verifiche sono effettuate in modalità self-assessment oppure on-site a campione.

4.1.5 Penetration Test a campione

Le attività effettuate in quest'ambito sono legate all'esecuzione di Penetration Test inseriti nella programmazione annuale (cfr. 4.2.1), oppure eseguiti estemporaneamente a fronte di eventi non programmabili, dovuti a mutamenti di scenari di minaccia, incidenti di sicurezza ed informazioni provenienti dalle attività di intelligence. Nel dettaglio le verifiche sono principalmente attivate a seguito di:

- reperimento dalle fonti OSINT/CLOSINT di informazioni di intelligence (Intelligence Driven Penetration Test);
- rilievo di eventi o di evidenze emerse durante le attività di monitoraggio del canale digitale che delineano una minaccia per il gruppo Poste Italiane (Threat Driven Penetration Test);
- approfondimenti necessari a valle di del rilievo di incidenti di sicurezza;
- specifiche richieste effettuate da altre funzioni aziendali o da aziende del Gruppo Poste italiane. (On Demand Penetration Test).

4.2 Il Processo

Tutte le attività di Security Assessment e Vulnerability Management descritte nel precedente capitolo sono caratterizzate dalle seguenti fasi progettuali:

1. Pianificazione;
2. Esecuzione;
3. Reporting;
4. Action Plan;
5. Conservazione;
6. Rilevazione dello stato della sicurezza.

4.2.1 Pianificazione

La fase di pianificazione prevede i seguenti step ed attività:

- pianificazione annuale delle verifiche, con la redazione ed aggiornamento del **Piano Generale di Verifica (PGV)**;
- pianificazione puntuale delle verifiche, con la redazione del **Piano Puntuale di Verifica (PPV).**

Le attività comprese nella fase di Pianificazione, descritte nei paragrafi successivi, sono illustrate nella figura seguente.

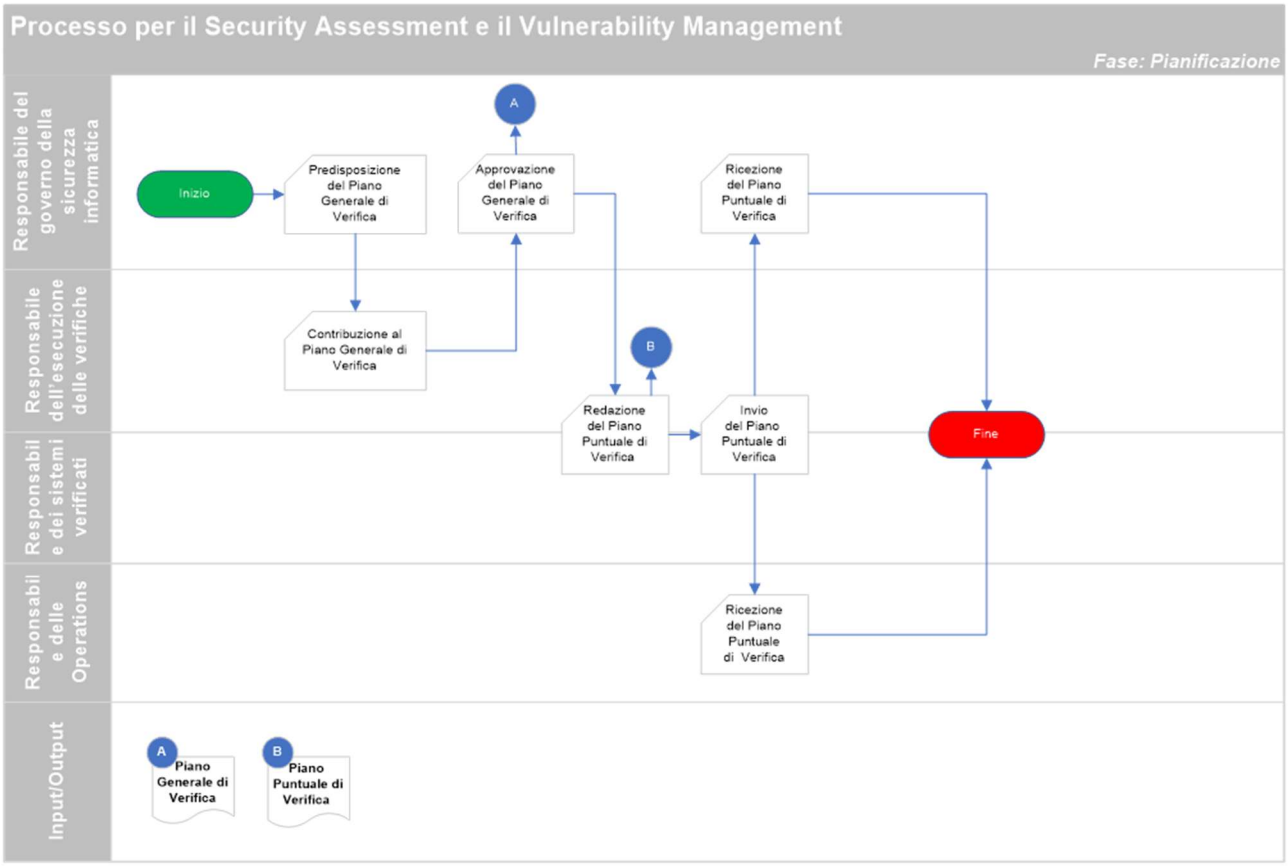

Figura 2 – Il processo di Security Assessment e Vulnerability Management – Pianificazione

4.2.1.1 Piano Generale di Verifica

Le verifiche effettuate da parte del *Responsabile dell'esecuzione delle verifiche* devono essere preventivamente programmate, al fine di assicurare nel corso dell'anno una pianificazione integrata che copra le esigenze di verifica dello stato della sicurezza dei sistemi, degli applicativi e delle infrastrutture.

La pianificazione annuale delle verifiche (PGV), deve essere redatta con i contributi di tutte le Funzioni *Responsabili dell'esecuzione delle verifiche* in relazione ai rispettivi ambiti di competenza, al fine ottimizzare gli interventi di verifica.

La funzione *Responsabile del Governo della Sicurezza Informatica* è responsabile della redazione e della validazione del PGV.

Il piano, finalizzato alla messa in sicurezza delle piattaforme IT di Poste Italiane, deve essere redatto tenendo conto di specifiche priorità.

L'assegnazione delle priorità di esecuzione delle attività di Security Assessment e Vulnerability Management, si basa su criteri oggettivi e risk-based, ed è finalizzata ad eseguire tali attività in maniera sistematica e secondo specifiche priorità, su tutte le applicazioni o i servizi rilevanti per Poste Italiane.

I criteri che regolano l'assegnazione della priorità di esecuzione si basano sulla disponibilità di una tabella contenente, per ogni ambito di appartenenza[5] individuato, la lista di tutti i sistemi e sull'applicazione di almeno uno o più dei seguenti razionali:

C0. applicativi che non sono stati oggetto di verifiche approfondite;
C1. adempimenti normativi obbligatori;
C2. la classe di rilevanza risultante dal CIRM:
C3. le risultanze dell'analisi del rischio già effettuate;
C4. il livello di rischio risultante dalle verifiche (si considerano prioritarie le piattaforme che hanno riportato un altissimo indice di rischio;
C5. le attività di verifica precedenti (ad esempio viene considerata prioritaria una piattaforma analizzata in tempi non ritenuti più consoni in quanto datati a prescindere dal livello rischio ottenuto).

In considerazione dei sistemi da sottoporre ad attività di Security Assessment e Vulnerability Management, potranno essere individuati di volta in volta ulteriori specifici razionali per l'assegnazione della priorità di intervento.

L'applicazione di tali razionali consente inoltre di mettere a fattor comune le informazioni raccolte con le varie attività operative di sicurezza (vulnerability assessment, penetration test, code review, ecc.) in modo da integrare la vista d'insieme delle piattaforme IT con relativo livello di rischio tecnologico rilevato.

Nel dettaglio, il PGV riporta:

- la lista dei sistemi, degli applicativi e delle infrastrutture trasversali;
- l'ambito normativo di riferimento (es. BankIT, EBA, 231, IMEL, ecc);
- tempi stimati di durata di ciascuna attività;
- traccia di eventuali aggiornamenti ed integrazioni alle liste definite, a seguito di mutamenti nel contesto interno o esterno ai sistemi e servizi in perimetro, ad esempio a seguito di incidenti interni di sicurezza o di nuove vulnerabilità di sicurezza la cui sfruttabilità viene resa pubblicamente nota;
- criteri di priorità applicati (es. C0, C1, ecc.).

4.2.1.2 Piano Puntuale di Verifica

Prima dell'inizio di una sessione di verifica, devono essere coinvolte le funzioni *Responsabili dell'Esecuzione delle verifiche* insieme alle funzioni *Responsabili dei sistemi verificati* e concordate le modalità e i tempi dell'attività. Successivamente viene redatto un Piano Puntuale di Verifica (PPV), contenente la finalità della verifica, l'elenco dei target di riferimento e le modalità di esecuzione della verifica.

Nello specifico il PPV deve riportare chiaramente:

- Il trigger che ha generato il piano di verifica puntuale (incidente, segnalazione puntuale, ecc.)
- la tipologia di verifica e l'obiettivo dell'analisi;
- le strutture organizzative coinvolte durante l'attività di verifica (le funzioni *Responsabili dei sistemi verificati* [6] e la funzione *Responsabile delle Operations*[7]);

[5] Gli ambiti di appartenenza consentono di realizzare delle classi di aggregazione, le piattaforme che appartengono a più ambiti sono indice di importanza e quindi considerate prioritarie (es. BP-Core).
[6] cfr. ALLEGATO 1: Transcodifica Ruoli-Strutture Aziendali-Sigle Organizzative.

- il target della verifica (applicativo) con l'indicazione dettagliata degli IP o delle sottoreti, nei casi applicabili;
- le modalità di esecuzione della verifica e la durata temporale;
- eventuali vincoli.

Il PPV deve essere notificato alla funzione *Responsabile del Governo della Sicurezza Informatica* e alla funzione *Responsabile delle Operations*.

4.2.2 Esecuzione

Le verifiche dovranno essere svolte dalle competenti funzioni *Responsabili dell'Esecuzione delle verifiche*, secondo le linee guida e standard internazionali di riferimento e nel rispetto delle policy e procedure aziendali applicabili, delle normative vigenti e delle indicazioni delle terze parti, quando funzionali al mantenimento delle certificazioni di settore o degli accreditamenti per l'erogazione dei servizi ai Clienti di Poste Italiane.

Le attività comprese nella fase di Esecuzione, descritte successivamente, sono illustrate nella figura seguente.

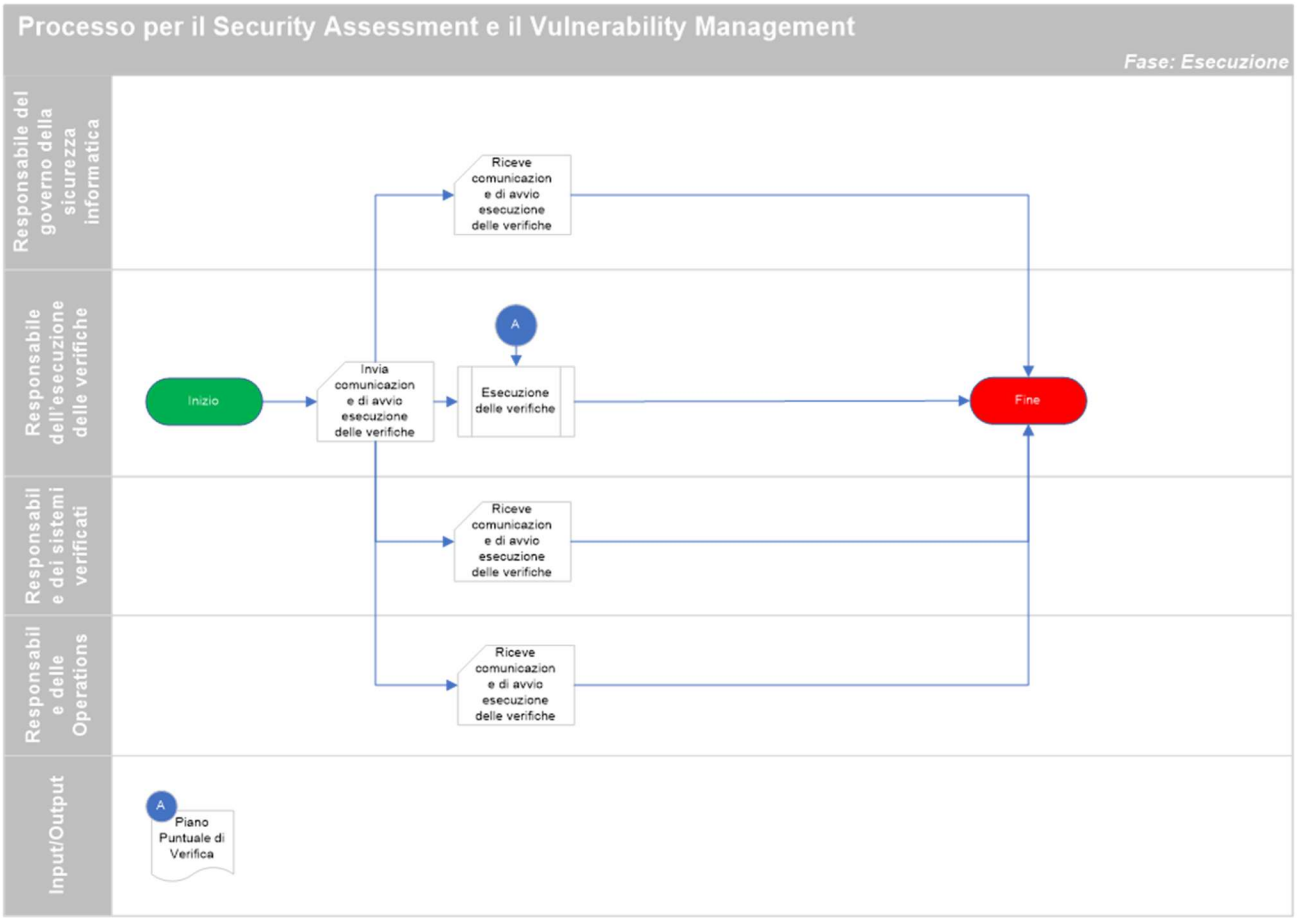

Figura 3 – Il processo di Security Assessment e Vulnerability Management – Esecuzione

[7] cfr. ALLEGATO 1: Transcodifica Ruoli-Strutture Aziendali-Sigle Organizzative.

L'avvio della fase di esecuzione operativa delle verifiche deve essere chiaramente comunicato alle funzioni *Responsabili dei sistemi verificati*, *Responsabili delle Operations* e alla *funzione Responsabile del Governo della Sicurezza Informatica*, già coinvolte nella fase di definizione del PPV. Tale comunicazione dovrà riportare, in particolar modo, il periodo temporale dei test ed il dettaglio dei sistemi interessati (es. IP sorgenti di attacco, IP target, ecc).

La fase esecutiva delle verifiche potrà essere oggetto di distinte procedure redatte in conformità alla presente, in funzione dell'ambito operativo e della specifica attività (cfr. par. 4.1) e comporterà la redazione di un Report delle Risultanze decritto nella successiva fase di Reporting (cfr. par. 4.2.3).

L'esecuzione delle attività di Security Assessment e Vulnerability Management deve essere effettuata attuando tutti gli accorgimenti necessari a minimizzare la possibilità di apportare danni ai sistemi di Poste Italiane derivanti da violazioni di sicurezza. In quest'ultimo caso, le attività devono essere immediatamente interrotte e dovrà essere attivato il processo di Gestione incidenti, secondo la specifica procedura aziendale.

4.2.2.1 Vincoli per la Conduzione delle Verifiche

Per l'esecuzione delle attività di verifica, ed in particolar modo per lo svolgimento dei Penetration Test, devono essere rispettati i seguenti vincoli di sicurezza:

- l'esecuzione dei test deve essere limitata al target oggetto di verifica, che dovrà pertanto essere puntualmente identificato all'interno del PPV;
- le tecniche di intrusione impiegate devono essere di tipo non invasivo o comunque tali da non provocare interruzione del servizio o arrecare danni permanenti ai sistemi agli applicativi ed alle infrastrutture trasversali;
- la raccolta di dati ed informazioni deve essere limitata allo stretto necessario, secondo i principi di correttezza, esaustività e non eccedenza;
- nel corso di tutte le attività di verifica dovrà essere garantita la stretta osservanza delle normative di riferimento e delle procedure di Poste Italiane in materia di sicurezza informatica e data protection;
- tutto il personale componente il gruppo di test, ed in special modo il personale esterno, è sottoposto alla stretta osservanza di una clausola di riservatezza, che vieta la comunicazione a terzi di qualsiasi informazione, anche a titolo di parere personale, relativo ai dati ed informazioni raccolte;
- i test possono essere svolti esclusivamente dal personale interno o esterno esplicitamente autorizzato e sotto il coordinamento di un Referente della Funzione di competenza con responsabilità di supervisione.

4.2.3 Reporting

Al termine dell'esecuzione delle attività di verifica viene redatto, da parte delle funzioni *Responsabili dell'esecuzione delle verifiche*, un Report delle Risultanze (RR) che costituisce la documentazione tecnica di ciascuna sessione di verifica puntuale e che contiene i dettagli atti alla riproducibilità dei test.

Le attività comprese nella fase di Reporting, descritte successivamente, sono illustrate nella figura seguente.

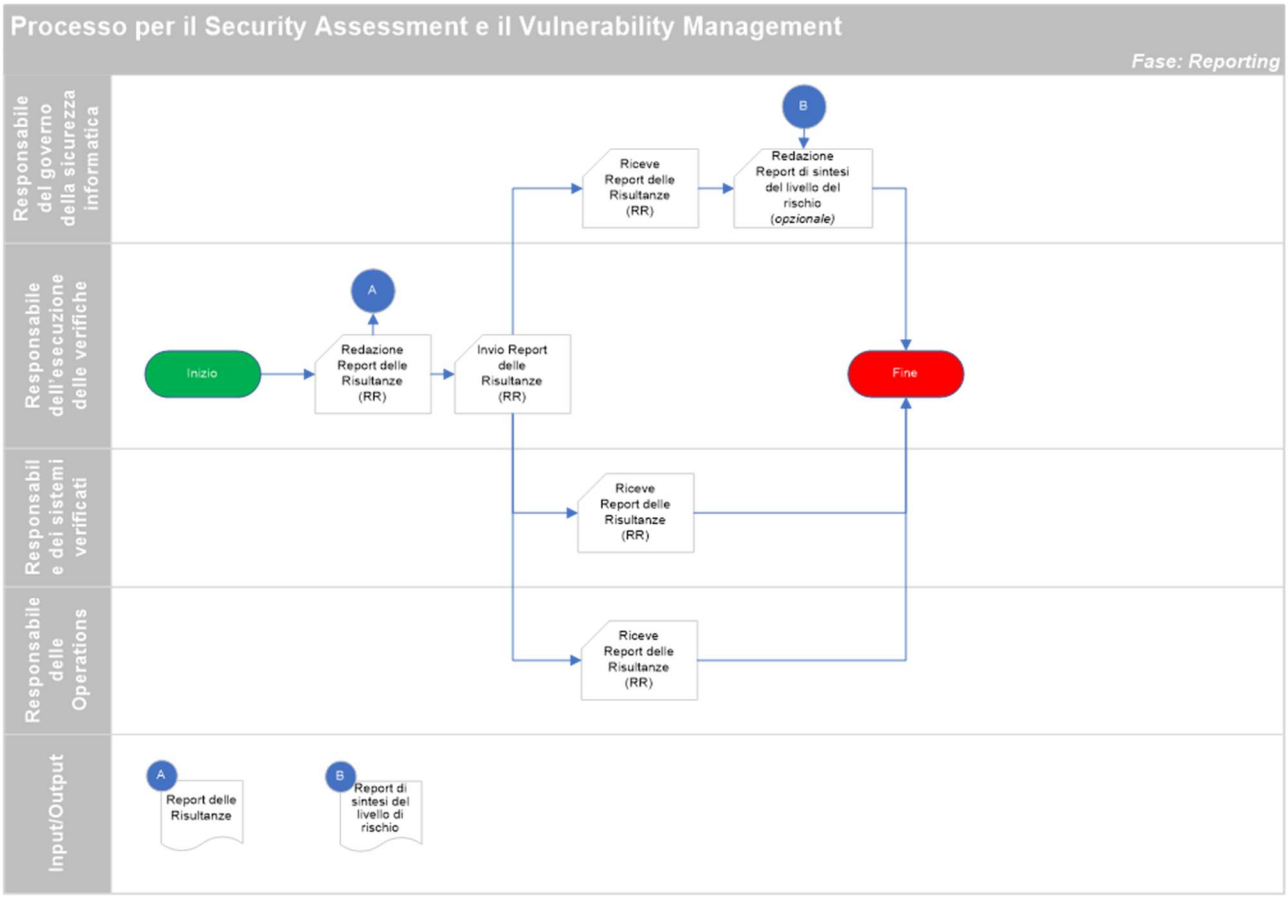

Figura 4 – Il processo di Security Assessment e Vulnerability Management - Reporting

Il Report con le risultanze delle verifiche condotte contiene almeno le seguenti informazioni:

- tipologie ed obiettivi della verifica;
- target (applicativo/sistema e, laddove previsto, IP) oggetto di verifica;
- strutture organizzative coinvolte nella verifica (funzioni *Responsabili per i sistemi verificati* e funzione *Responsabile del Governo della Sicurezza Informatica*);
- elenco delle vulnerabilità individuate/sfruttate categorizzate per livelli di rischio, utilizzando possibilmente la classificazione CVSS. La definizione della metodologia di classificazione è individuata nel contesto di distinte procedure, in funzione dell'ambito operativo e della specifica attività (cfr. cap. 4.1);
- per le vulnerabilità particolarmente critiche indicare, laddove applicabile e possibile, se è da ritenersi bloccante o meno ai fini del rilascio in produzione;
- raccomandazioni per la stesura del piano correttivo.

Laddove possibile, inserire nel report anche le seguenti informazioni:

- descrizione di dettaglio delle attività svolte;
- evidenze degli esiti delle prove effettuate (ad es. screenshot);
- descrizione sintetica dei possibili impatti a cui è esposto il sistema, l'applicativo o l'infrastruttura, rapportati all'agente di minaccia ed alla facilità di sfruttamento delle vulnerabilità stesse (nel caso dei PT).

Tale report viene comunicato inviato alle strutture organizzative competenti (*Responsabile del Governo della Sicurezza Informatica, Responsabili dei sistemi verificati, Responsabile delle Operations*).

Oltre a tale documento tecnico di dettaglio potrà essere redatto ove necessario, da parte del *Responsabile del Governo della Sicurezza Informatica*, anche un report di sintesi che descriva il livello di rischio tecnologico rilevato, il grado di conformità e adeguatezza, nonché le specifiche azioni di remediation necessarie ed i relativi Action Plan individuati.

4.2.4 Action Plan

Unitamente al Report delle risultanze sarà predisposto, da parte della funzione *Responsabile dell'esecuzione delle verifiche*, un Action Plan (AP) per la definizione dei rientri dalle vulnerabilità individuate per ciascun ambito.

In particolare, l'AP dovrà contenere almeno le seguenti informazioni:

- target (applicativo/sistema e, laddove previsto, IP) oggetto di verifica;
- risultanze (vulnerabilità riscontrate);
- rilevanza della vulnerabilità in termini di livelli di rischio, utilizzando possibilmente la classificazione CVSS (cfr. par. 4.2.3);
- suggerimento di azione correttiva.

Le attività comprese nella fase di Action Plan, descritte successivamente, sono illustrate nella figura seguente.

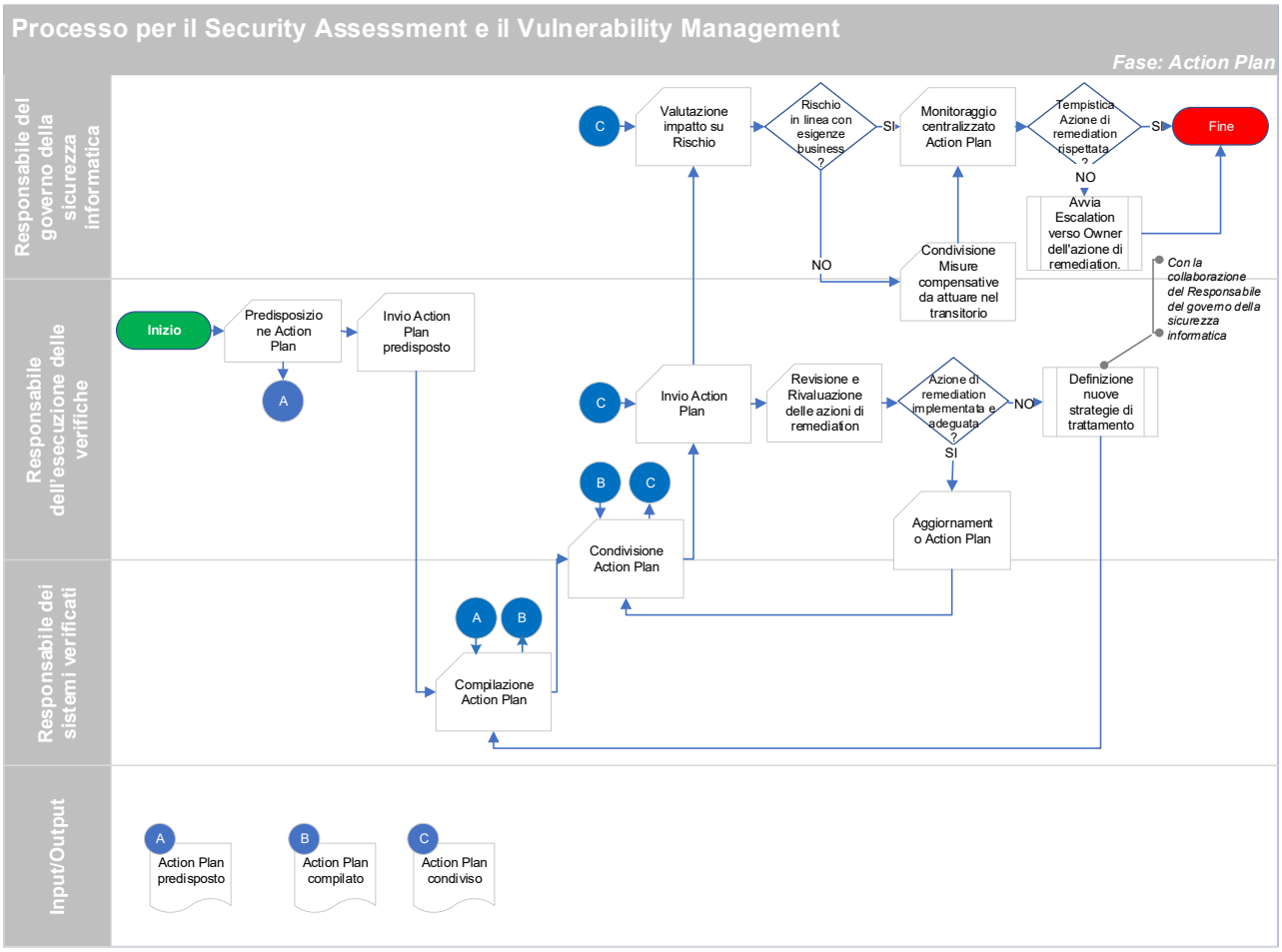

Figura 5 – Il processo di Security Assessment e Vulnerability Management – Action Plan

L'Action Plan dovrà essere compilato dalla *Funzione Responsabile dei sistemi verificati* entro 15 gg dalla ricezione e dovrà contenere almeno le seguenti informazioni, preventivamente condivise con *la Funzione Responsabile dell'esecuzione delle verifiche*:

- azioni per rientrare dalla vulnerabilità segnalata;
- scadenza del rientro (espressa in gg/mm/aaaa);
- responsabile dell'azione di rientro.

In ogni caso, le tempistiche associate alle azioni di rientro indicate nell'Action Plan dovranno essere direttamente proporzionali all'urgenza connessa al livello di rischio della vulnerabilità riscontrata.

L'Action Plan debitamente compilato da parte del *Responsabile dei sistemi verificati* deve essere condiviso con la *Funzione Responsabile dell'esecuzione delle verifiche* che ha in carico la gestione dell'Action Plan.

Tale piano deve essere inviato alla Funzione *Responsabile del Governo della Sicurezza Informatica* da parte del *Responsabile dell'esecuzione delle verifiche* che effettuerà centralmente le attività di monitoraggio delle relative azioni di rientro. Tale attività prevede:

- una valutazione dell'impatto di quanto previsto nell'Action Plan, sul livello di rischio associato all'asset interessato e ai servizi ad esso connessi. Qualora tale livello non risultasse in linea alle esigenze del Business aziendale, la Funzione *Responsabile del Governo della Sicurezza*

Informatica, contatta il *Responsabile dell'esecuzione delle verifiche* per condividere le necessarie azioni compensative da attuarsi nel transitorio.

- un controllo periodico sullo stato di attuazione delle azioni di rientro (remediation). Quando tali attività non dovessero risultare concluse entro i tempi previsti è attivato un processo di escalation verso le funzioni interessate.

4.2.4.1 Revisione e rivalutazione delle Azioni di Remediation

A fronte delle azioni individuate nell'Action Plan di cui al paragrafo precedente, sono effettuati da parte del *Responsabile dell'esecuzione delle verifiche*, dei controlli puntuali relativi a:

- verifica dell'effettiva implementazione dell'azione di remediation, in base al livello di criticità assegnata alle vulnerabilità (i.e. alta, media, bassa);
- adeguatezza (efficacia) dell'azione di remediation proposta.

La verifica di efficacia dell'intervento correttivo è svolta attraverso la ripetizione di Vulnerability Assessment oppure con attività manuali e puntuali, a seguito della comunicazione di chiusura dell'azione di remediation o quando i tempi previsti per il successivo VA risultino troppo distanti rispetto alle tempistiche definite nell'Action Plan. Quando l'intervento risulti non adeguato, si definiscono nuove strategie di trattamento anche con il supporto del *Responsabile del Governo della Sicurezza*, il piano di trattamento è aggiornato e inizia un nuovo ciclo. Se invece l'intervento risulta adeguato, il *Responsabile dell'esecuzione delle verifiche* aggiorna l'Action Plan condividendolo con il *Responsabile dei sistemi verificati* e lo invia per opportuna conoscenza al *Responsabile del Governo della Sicurezza Informatica.*

4.2.5 Conservazione

I risultati delle verifiche effettuate (Report delle risultanze-RR) e delle azioni di remediation attuate per il rientro delle vulnerabilità individuate (Action Plan) nonché i Piani Generali di Verifica (PGV) ed il Piano Puntuale di Verifica (PPV), dovranno essere:

- Archiviati nel dettaglio a cura del referente della Funzione *Responsabile dell'esecuzione delle verifiche*, sul sistema documentale centralizzato predisposto e gestito dalla *Funzione Responsabile del Governo della Sicurezza*;
- Conservati complessivamente in sintesi dalla Funzione *Responsabile del Governo della Sicurezza Informatica*, al fine costituire una Knowledge Base per indirizzare in maniera più efficace ed efficiente le iniziative di natura correttiva/evolutiva per il miglioramento della gestione della sicurezza (es. nuovi controlli correttivi e/o preventivi, ridefinizione processi e procedure, ridefinizione istruzioni operative), in un'ottica di Continuous Improvement.

La rappresentazione grafica delle attività comprese in questa fase è riportata nella figura seguente.

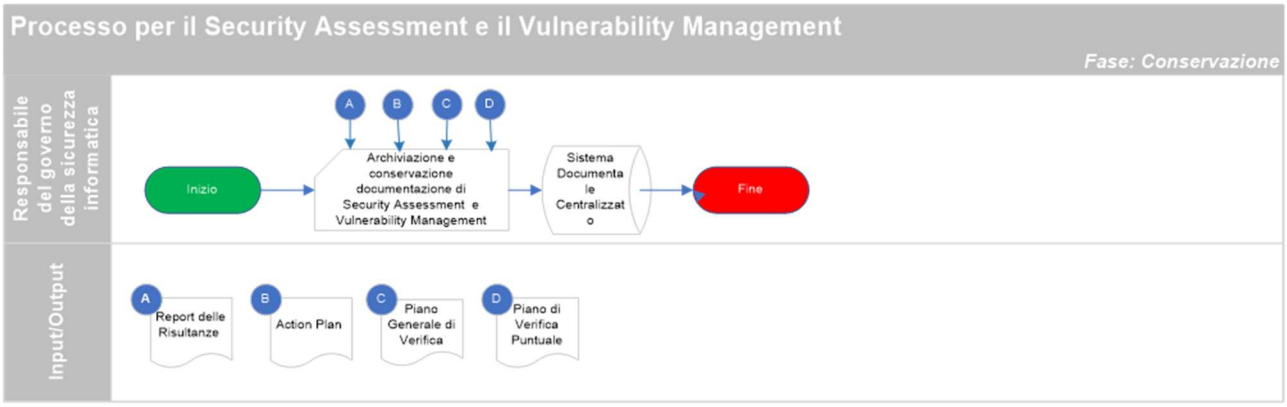

Figura 6 – Il processo di Security Assessment e Vulnerability Management – Conservazione

4.2.6 Rilevazione dello stato della Sicurezza

I risultati delle attività di Security Assessment e Vulnerability Management, sono recepiti ed analizzati da parte del *Responsabile del Governo della Sicurezza Informatica*, allo scopo di:

- fornire una vista sintetica e di dettaglio sull'andamento temporale delle vulnerabilità a cui sono esposte le singole applicazioni di Poste Italiane;
- realizzare una matrice di rischio che tenga conto dell'impatto valutato in base alla rilevanza dell'applicazione e delle vulnerabilità riscontrate.

Tali risultati contribuiscono alla gestione (valutazione, mitigazione, pianificazione, monitoraggio e reporting) del rischio informatico delle piattaforme tecnologiche e applicative di Poste Italiane, come previsto nell'ambito del Modello di Information Security Governance di PI.

La rappresentazione grafica delle attività comprese in questa fase sono illustrate nella figura seguente.

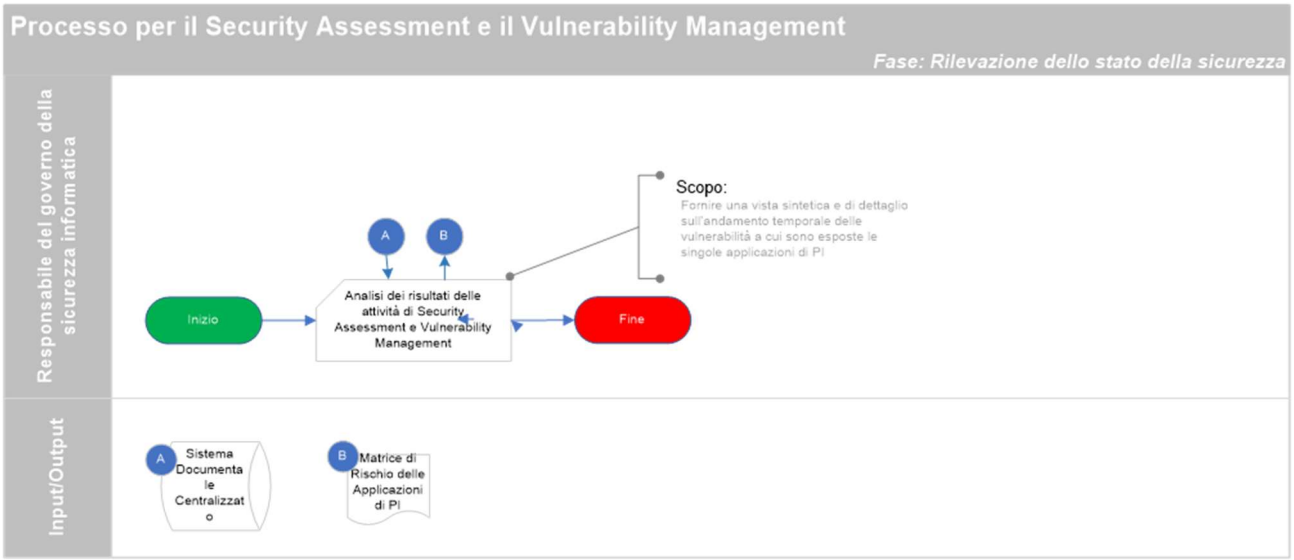

Figura 7 – Il processo di Security Assessment e Vulnerability Management – Rilevazione dello stato della sicurezza

4.3 Matrice delle Responsabilità

Di seguito viene riportata la matrice delle responsabilità (RACI) relativa al processo di Security Assessment e Vulnerability Management.

Nell'ambito delle responsabilità individuate nei capitoli precedenti, si definiscono i seguenti ruoli:

- **Responsabile del governo della sicurezza informatica**: la funzione aziendale designata per il governo della sicurezza Informatica;
- **Responsabile dell'esecuzione delle verifiche**: le funzioni deputate all'esecuzione delle verifiche;
- **Responsabile dei sistemi verificati**: le funzioni competenti che rappresentano gli owner dei sistemi oggetto di verifica e che attuano le opportune azioni di remediation;
- **Responsabile delle Operations**: le funzioni competenti di Operations.

Per quanto concerne l'associazione tra i suddetti ruoli e le funzioni aziendali di riferimento, si rimanda all'Allegato 1: Transcodifica Ruoli-Strutture Aziendali-Sigle Organizzative.

FASI DI PROCESSO	***Responsabile del Governo della Sicurezza Informatica***	***Responsabile dell'esecuzione delle verifiche***	***Responsabile dei sistemi verificati***	***Responsabile delle Operations***
Pianificazione				
Piano Generale di Verifica (PGV)	**RA**	**C**	**I**	
Piano Puntuale di Verifica (PPV)	**I**	**RA**	**I**	
Esecuzione				
Continuous Monitoring	**I**	**RA**	**IC**	**I**
Verifiche tecniche di sicurezza nel ciclo di vita dei progetti	**I**	**RA**	**IC**	
Goal Oriented PT	**I**	**RA**	**IC**	**I**
Assessment di sicurezza sulle terze parti	**I**	**RA**	**IC**	**I**
PT a campione	**I**	**RA**	**IC**	**I**
Reporting				
Report delle risultanze	**I**	**RA**	**I**	**I**
Report di sintesi del livello di rischio	**RA**			
Action Plan				
Predisposizione		**RA**		
Compilazione	**I**	**C**	**RA**	**I**

Revisione e rivalutazione delle azioni di rientro		**I**	**RA**	**I**	**I**
Monitoraggio del piano di rientro		**RA**	**I**	**C**	
Conservazione					
Archiviazione		**A**	**R**	**R**	
Conservazione		**RA**	**I**	**I**	

Tabella 1 - Il processo di Security Assessment e Vulnerability Management – Matrice RACI

Legenda:

R (Responsible): Il soggetto responsabile della realizzazione di un risultato/output di un'attività o fase

A (Accountable): Il responsabile che approva il risultato/output di un'attività o fase

C (Consulted): Il soggetto che collabora con il Responsible alla realizzazione di un risultato o output di un'attività/fase

I (Informed): Il soggetto informato della realizzazione di un risultato/output di un'attività/fase.

5 Responsabilità di aggiornamento

La Funzione responsabile del documento, che ne assicura la redazione, l'aggiornamento e la divulgazione è la funzione CA/TA/SI.

Le Funzioni coinvolte nelle attività disciplinate dal presente documento sono responsabili della rilevazione e della segnalazione alla Funzione CA/TA/SI degli accadimenti aziendali di carattere operativo che possono comportare la necessità di aggiornamento.

6 Riferimenti

Il presente documento è definito in coerenza con gli strumenti normativi interni e i riferimenti normativi esterni vigenti applicabili al Gruppo Poste Italiane. In particolare:

Esterni

[1] Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio 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 (regolamento generale sulla protezione dei dati)

[2] Direttiva (UE) 2016/1148 del Parlamento Europeo e del Consiglio del 6 luglio 2016 «recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione», nota anche come «Network and Information Security Directive»

[3] D.Lgs. n. 101/2018 – Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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

[4] NIST 800-115 – Technical Guide to Information Security Testing and Assessment

[5] NIST 800-37:2018 Risk Management Framework for Information Systems and Organizations A System Life Cycle Approach for Security and Privacy (Chapter 3)

[6] NIST SP 800-53:2015 Security and Privacy Controls for Federal Information Systems and Organizations (security controls: low/moderate/high-impact)

[7] International Standard ISO/IEC 27001:2013 Information Technology – Security techniques – Information Security Management System – Requirements

[8] ISO/IEC 27002:2013 Information Technology – Security techniques – Code of practice for information security controls

[9] The Open Web Application Security Project – OWASP

[10] Penetration Testing Framework 0.59 at vulnerabilityassessment.co.uk

[11] Open Source Security Testing Methodology – OSSTMM

[12] Open Web Application Security Project Mobile Security Testing

[13] OWASP Top 10 Most Critical Web Application Security Risks

[14] OWASP Risk Rating Methodology

[15] Common Vulnerability Scoring System (CVSS)

[16] CCNL per i Dirigenti di Aziende produttrici di Beni e Servizi

[17] CWE-SANS Top 25, 2011 - Common Weakness Enumeration - SysAdmin, Audit, Networking, and Security

[18] D.Lgs. 8 giugno 2001, n. 231 "Disciplina della responsabilità amministrativa delle persone giuridiche, delle Società e delle associazioni anche prive di personalità giuridica, a norma dell'art. 11 della legge 29 settembre 2000, n. 300"

Interni

[19] Modello di Information Security Governance di Poste Italiane

[20] Politica per la sicurezza delle Informazioni di Poste Italiane

[21] Politica Integrata del Gruppo Poste Italiane
[22] Linea Guida “Sistema di segnalazione delle violazioni (whistleblowing)”
[23] Linea Guida “Sistema Normativo Aziendale”
[24] Procedura Gestione Documenti
[25] Codice Etico del Gruppo Poste Italiane
[26] Compendio dei poteri di Poste Italiane
[27] CCNL per il personale non dirigente di Poste Italiane
[28] Relazione PIT-2917-01-REL-1.0: “Supporto per la definizione dei controlli di verifica del rispetto dei requisiti di sicurezza dell’ambiente mainframe di Poste Italiane”, Information Service Group del 20/09/2017
[29] Modello di Organizzazione, Gestione e Controllo di Poste Italiane S.p.A. ai sensi del Decreto Legislativo n. 231/2001 - “Responsabilità Amministrativa della Società”
[30] Linea Guida "Flussi informativi 231 all'Organismo di Vigilanza di Poste Italiane"

7 Sistemi di gestione e/o modelli organizzativi/normative di riferimento

Modello ai sensi del Decreto Legislativo n. 231/2001	☒
Modello 262	☐
Modello Privacy	☒
Sistema di Gestione per la Qualità	☒
Sistema di Gestione per la sicurezza delle informazioni	☒
Sistema di Gestione Ambientale	☐
Sistema di Gestione per la sicurezza e la tutela della salute sui luoghi di lavoro	☐
Sistema di Gestione Anticorruzione	☐
Sistema di Gestione dell'energia consumata per usi propri	☐
Gestione dei Servizi Informatici	☒
Normativa di Settore/Disposizioni da Organi di Vigilanza (es: normative bancarie, finanziarie, assicurative, postale…)	☒

8 Destinatari

I destinatari del documento, elencati di seguito, devono assicurare la diffusione della documentazione all'interno della propria Funzione, in coerenza con gli ambiti operativi ed applicativi di riferimento.

- CA
- SI
- CI

9 Allegato 1: Transcodifica Ruoli-Strutture Aziendali-Sigle Organizzative

L'allegato ha lo scopo di:

- associare ogni ruolo menzionato nella suddetta Procedura alle funzioni aziendali di riferimento, in base agli ambiti operativi/attività individuati nel documento (cfr. par. 4.1);
- associare alle funzioni coinvolte nel processo, gli acronimi organizzativi in uso.

9.1 Ruoli Aziendali e Sigle Organizzative correnti

Ruolo riportato nel documento	**Acronimo Funzione Aziendale/Organi**	**Ambito Operativo (cfr. par. 4Errore. L'origine riferimento non è stata trovata.) e Attività individuata nel documento**
Responsabile del Governo della Sicurezza Informatica	CA/TA/SI	Tutti gli ambiti/Tutte le attività.
Responsabile dell'esecuzione delle verifiche	CA/TA/SI	• Verifiche Tecniche di Sicurezza nel Ciclo di vita dei progetti/Tutte le attività; • Goal Oriented-Pentest/Tutte le attività; • Assessment di Sicurezza sulle Terze Parti/Tutte le attività.
	CA/TA/CERT	• Penetration Test a campione/Tutte le attività; • Continuous Monitoring/VA Rete Esterna.
	SI/CTO/CTOCO	• Continuous Monitoring/VA Rete Interna; • Assessment Mainframe.
Responsabile dei sistemi verificati	SI (in funzione dei rispettivi ambiti di operatività individuati nella procedura).	Tutti gli ambiti e le attività di competenza
Responsabile delle Operations	SI/CTO/CTOCO, SI/STLC, SI/ESSD, SI/ESITC SI/ESITT	Informazione in merito agli ambiti/attività di competenza.

Tabella 2 - Il processo di Security Assessment e Vulnerability Management – Ruoli aziendali e Acronimi Funzioni

9.2 Acronimi Sigle Organizzative

La definizione degli acronimi di tutte le Funzioni aziendali di Poste Italiane è disponibile sulla intranet aziendale al seguente link: https://noidiposte.poste/il-siglario-di-poste-italiane/

Per comodità sono riportati nella seguente tabella gli acronimi di maggior rilievo per il presente documento.

Acronimo Funzione Aziendale/Organi	Descrizione
CA/TA/SI	Corporate Affairs/Tutela Aziendale/Sicurezza Informatica
CA/TA/CERT	Corporate Affairs/Tutela Aziendale/Computer Emergency Response Team
SI	Sistemi Informativi
SI/CTO/CTOCO	Sistemi Informativi/Chief Technology Officer/CTO Continuity Operations
SI/ESITC	Sistemi Informativi/ Esercizio e Supporto IT Centrale
SI/ESSD	Sistemi Informativi/Esercizio e Supporto Servizi Digitali
SI/STLC	Sistemi Informativi/Servizi TLC
SI/ESITT	Sistemi Informativi/ Esercizio e Supporto IT Territoriale

Tabella 3 - Il processo di Security Assessment e Vulnerability Management – Acronimi sigle organizzative

**** QUESTA È L'ULTIMA PAGINA DEL DOCUMENTO ****