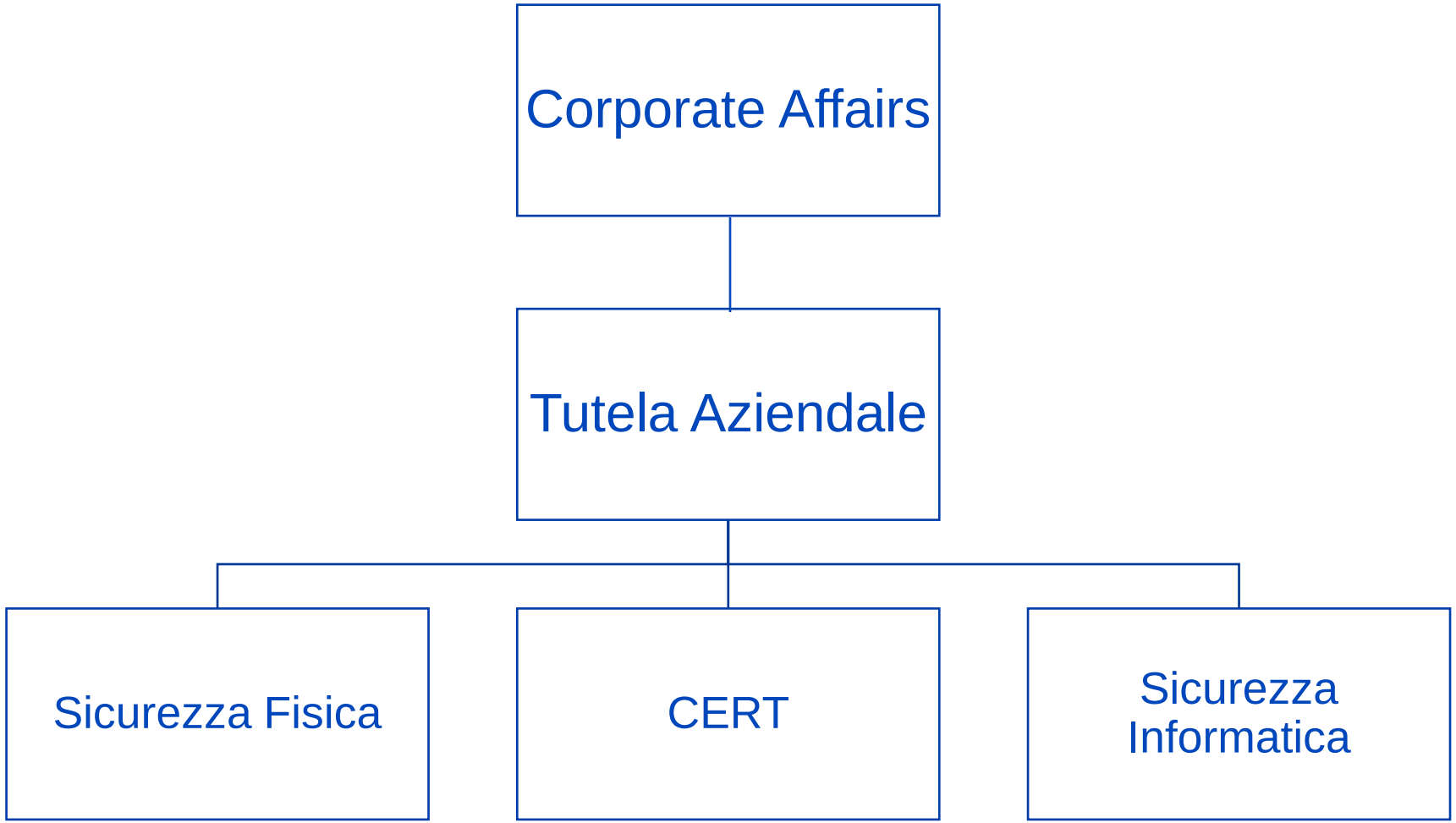
NOTE PER AUDIZIONE POSTE ITALIANE PER DECRETO LEGGE N°105/2019

POSTE ITALIANE

Roma, 3 Ottobre 2019

CORPORATE AFFAIRS – TUTELA AZIENDALE

ORGANIGRAMMA



ORGANIZZAZIONE CYBER SECURITY DEL GRUPPO POSTE ITALIANE

IN RIGUARDO ALL'ART.1, COMMA 3, LETTERA B DEL DECRETO LEGGE N°105/2019

Il Gruppo Poste Italiane:

- è dotato di un **sistema di politiche di sicurezza informatica** e di una struttura organizzativa pensata e realizzata ad hoc per la gestione della sicurezza informatica per garantire la migliore protezione del patrimonio informativo aziendale, secondo un approccio risk-based;
- è dotato di un **sistema di gestione degli eventi e incidenti di sicurezza informatica** per prevenire e mitigare l'effetto di un attacco informatico, individuando, sulla base dell'esperienza pregressa, apparati o prodotti che possono rappresentare un punto di "debolezza";
- attraverso un approccio olistico che tiene conto degli aspetti di sicurezza fisica e logica e sfrutta le migliori e più innovative tecnologie hardware e software, è in grado di garantire **un'adeguata protezione dei dati;**
- dispone di un **sistema di gestione della continuità operativa** per i servizi finanziari di BancoPosta; in relazione alla costituzione di nuovi soggetti giuridici come Postepay S.p.A., il Gruppo ha ritenuto strategico avviare un programma per costituire un nuovo modello di Crisis Management e far evolvere il modello di Business Continuity Management a livello di Gruppo, il tutto in linea con le normative e gli standard di riferimento BS 11200:2014, ISO 22301:2012;
- dispone di presidi di sicurezza operativi al fine di effettuare con continuità il **monitoraggio dello stato di sicurezza e delle prestazioni delle reti e delle applicazioni**;
- è continuamente interessato da **programmi di formazione** e informazioni in materia di sicurezza informatica; è stato realizzato un portale utile per sensibilizzare **sui temi della cybersecurity** tutti dipendenti del Gruppo, con contenuti e linguaggi pensati per soddisfare le esigenze di ogni utente;
- si avvale per l'affidamento di forniture di beni, sistemi e servizi ICT di **imprese e professionisti opportunamente identificati e qualificati in albo**.

ACCORDI

- Ad aprile 2018 è stata rinnovata l'intesa fra Poste Italiane e Polizia Postale, uno storico rapporto collaborativo che ha richiesto l'adeguamento, un accordo che richiede anche un adeguamento alla rapida evoluzione delle attività e dei servizi offerti da Poste Italiane

- Poste Italiane e Polizia Postale hanno il comune obiettivo di ridurre rischi e reati, quali l'indebito utilizzo di carte di credito, phishing, acquisizione di dati personali sensibili, frodi informatiche e truffe

- EECTF European Electronic Crime Task Force

- Fondazione Global Cyber Security Center

CONTRIBUTI

- **Tempistiche per l'applicazione del decreto**: l'elenco delle reti dei sistemi informativi, comprensivo della relativa architettura e componentistica potrebbe essere insufficiente per produrre la documentazione completa, data l'ampiezza del perimetro del Gruppo Poste Italiane. Ciò premesso, si propone di prevedere un tempo superiore pari ad almeno 12 mesi
- **Sistema di notifiche:** attualmente il sistema prevede notifiche verso più attori istituzionali (CSIRT Italiano, Autorità competenti NIS, AgiD, Banca d'Italia/CODISE, Garante Privacy) con diverse metodologie di comunicazione e trasmissione. Si ritiene che l'armonizzazione delle varie esigenze di notifica potrebbe rendere più efficienti le differenti procedure
- **Laboratorio CVCN:** verifica lo stato di sicurezza di prodotti, apparati e sistemi utilizzati per il funzionamento di reti, servizi e infrastrutture. Al riguardo, risulterà fondamentale per le imprese comprendere le tempistiche per l'ottenimento della certificazione. Potrebbe inoltre essere opportuno chiarire i criteri per la certificazione dei servizi considerando le integrazioni che le imprese hanno con le tecnologie dei grandi partner extra-UE.
- **Revisione della contrattualistica per forniture in essere (modi e tempi) e adeguamento tecnologico:** occorre tener conto degli effetti della contrattualistica già in essere che potrebbe necessitare di interventi di revisione non quantificabile sia in termini economici sia in relazione ai tempi di realizzazione
- **Approvvigionamento – il rapporto della nuova disciplina con il codice degli appalti:** Il vincolo all'utilizzo di tecnologie e servizi certificati potrebbe porre delle criticità in fase di approvvigionamento.
- **Whitelist di certificazione**: è auspicabile che sia previsto un meccanismo che privilegi la certezza e la trasparenza attraverso whitelist, di quali siano le reti, i sistemi informativi e di servizi informatici che abbiano, in un dato periodo, i requisiti prescritti ai fini della certificazione
- **Gestione dei costi:** quanto già sostenuto dall'azienda pone Poste Italiane in una condizione di avanzata tutela che, tuttavia, non l'esime dal compiere ulteriori investimenti e sostenere maggiori oneri per l'effetto dell'entrata in vigore del decreto-legge. Questo potrebbe creare anche delle distorsioni competitive che vanno a favore di soggetti non inclusi nel provvedimento. Sarebbe opportuno prevedere dei meccanismi di agevolazione fiscale in modo da incentivare maggiormente la presa in carico delle attività e degli investimenti a far data dall'entrata in vigore del provvedimento

Posteitaliane

poste.it