Polizia di Stato

Direzione Centrale per la Polizia Scientifica e la Sicurezza Cibernetica

La Direzione centrale ha al suo interno quattro Servizi:

- Servizio Affari generali
- Servizio Polizia scientifica
- Servizio Polizia postale e per la sicurezza cibernetica
- Servizio per la Sicurezza cibernetica del Ministero dell'Interno

Il **Servizio Affari generali** ha al suo interno due divisioni che svolgono i seguenti compiti

La I Divisione

- segreteria del Direttore Centrale;
- affari generali della Direzione Centrale;
- supporto al Direttore Centrale per la pianificazione, definizione ed attuazione dei programmi e degli obiettivi nell'ambito del sistema del controllo strategico e di gestione;
- funzione di coordinamento delle attività dei Servizi;
- affari connessi al raccordo delle attività per quanto concerne la gestione delle risorse umane e dei rapporti sindacali;
- gestione della corrispondenza ordinaria e classificata e dell'archivio generale della Direzione Centrale;
- comunicazione interna ed esterna;
- questioni di natura tecnico-giuridica;
- collazione di contributi in materia di provvedimenti normativi e per la risposta ad atti di sindacato parlamentare;
- adempimenti previsti dalla normativa in materia di trasparenza e prevenzione della corruzione;
- rapporti con l'Ufficio IV – Comunicazione istituzionale della Segreteria del Dipartimento.

La II Divisione

- raccordo delle procedure informatiche ed il relativo supporto tecnico per la Direzione Centrale;
- adempimenti previsti dalla normativa in materia di salute e sicurezza nei luoghi di lavoro per la Direzione;
- funzioni connesse alle attività inerenti al sistema di gestione della qualità e *audìt*;
- supporto al Direttore ai fini della definizione del piano di fabbisogno della Direzione Centrale funzionale all'acquisto di beni, servizi e materiale di facile consumo occorrenti alla stessa, a cura delle altre articolazioni del Dipartimento, secondo le quote-parti delle risorse finanziarie ordinarie assegnate per le esigenze della Direzione centrale e di quelle connesse ai finanziamenti europei.

Il **Servizio Polizia scientifica** è strutturato in cinque divisioni che svolgono le seguenti attività

La I Divisione cura gli affari generali del Servizio e la gestione della corrispondenza; provvede al coordinamento delle attività delle altre Divisioni del Servizio e predispone i contributi unitari del Servizio; cura la gestione delle risorse umane e delle dotazioni tecnologiche per il supporto delle attività di settore; provvede alla formazione professionale e all'aggiornamento del personale operante nel settore della Polizia Scientifica; cura la gestione del flusso dei reperti; cura le relazioni esterne e internazionali nel settore della Polizia Scientifica; cura l'indirizzo e il coordinamento delle attività degli uffici periferici della Polizia Scientifica della Polizia di Stato; svolge analisi investigative sulla scena del crimine e sui delitti insoluti, cura il supporto all'attività video – fotografica; cura la gestione del parco veicolare assegnato al Servizio Polizia Scientifica; provvede all'elaborazione delle statistiche relative ai carichi di lavoro e alle risorse impegnate a supporto dei processi decisionali nonché svolge attività funzionali alla realizzazione di infrastrutture fisiche e tecnologiche a livello centrale e periferico nelle

materie di competenza; cura la pianificazione del fabbisogno funzionale di beni, servizi e materiale di facile consumo del Servizio Polizia Scientifica e delle articolazioni territoriali nonché lo svolgimento delle attività propedeutiche ai medesimi acquisti e alle manutenzioni delle strumentazioni ed apparecchiature;

La II Divisione ha competenza in materia di: identità preventiva e connessa gestione dell'archivio del Casellario centrale d'identità; identità giudiziaria; evidenziazione delle impronte latenti; gestione operativa del Sistema automatizzato per il riconoscimento delle impronte digitali (AFIS), monitoraggio e supervizione dell'infrastruttura nonché la protezione e la sicurezza dei relativi dati; configurazione delle applicazioni e cura dei relativi servizi di interoperabilità con gli altri sistemi informatici nazionali, europei ed internazionali finalizzati all'interscambio delle impronte digitali e di altre informazioni identificative previste dai rispettivi accordi; assicura i servizi di cooperazione nell'ambito delle Decisioni di Prum, espletando le funzioni di punto di accesso nazionale al sistema EURODAC, individuato ai sensi del Regolamento (UE) n. 603/2013 del Parlamento e del Consiglio del 26 giugno 2013; cura la gestione centralizzata degli utenti dei sistemi collegati ad AFIS e assicura il coordinamento delle attività di competenza svolte dagli uffici territorialmente dipendenti.

La III Divisione ha competenza in materia di analisi chimiche, indagini sulle droghe ed espleta attività di studio e di analisi dei precursori delle sostanze stupefacenti ed esplodenti, curando anche lo sviluppo e la validazione di nuovi protocolli analitici; garantisce il monitoraggio e la geolocalizzazione delle sostanze stupefacenti a livello nazionale, assolvendo anche alla funzione di *focal point* per la segnalazione di nuove droghe per il Sistema Nazionale Allerta Precoce; svolge indagini su esplosivi e materiali infiammabili, indagini merceologiche; espleta attività in materia di identità grafica e falso documentale, provvedendo anche alla gestione del Sistema Informatico Documenti Autentici e Falsi (SIDAF); espleta le attività di coordinamento delle attività di laboratorio svolte dagli Uffici territorialmente competenti.

La IV Divisione cura, per finalità forensi, le attività in materia di analisi e comparazioni foniche nonché in materia di analisi e miglioramento di immagini e video; svolge, per finalità forensi, attività in materia analisi di dispositivi elettronici e telematici; cura la gestione e lo sviluppo del Sistema Automatico di Riconoscimento Immagini (SARI) e svolge attività di digital forensics e di accertamenti tecnici di analisi telematica; cura le attività in materia di sistemi di intelligenza artificiale per applicazioni multimediali e analisi biometriche; svolge compiti in tema di impiego delle tecnologie per la stampa 3D per scopi forensi e di georadar; cura le attività in materia di rilevamento di segnali e di trasmissioni elettromagnetiche; svolge indagini balistiche e gestisce il balipedio e la collezione d'armi della Polizia Scientifica; sviluppa l'analisi delle tracce ematiche (BPA) e svolge indagini sui residui dello sparo; svolge attività in materia di rilievo planivolumetrico, di ricostruzione tridimensionale della dinamica della scenda del crimine e realtà virtuale; cura la ricerca, lo sviluppo e la definizione di protocolli tecnici sulle tematiche di settore e assicura il coordinamento delle attività di laboratorio svolte dagli uffici territorialmente dipendenti.

La V Divisione ha competenza in materia di genetica forense, biologia generale e analisi del DNA; assicura il monitoraggio, l'analisi e lo studio degli inserimenti nel Sistema Ricerca Scomparsi (RI.SC); assicura il coordinamento delle attività di laboratorio svolte dagli Uffici territorialmente dipendenti; provvede alla formulazione e allo sviluppo di acquisti nonché all'ideazione di nuovi progetti di cooperazione; svolge attività di studio e di collaborazione in materia C.B.R.N. nonché di medicina legale.

Il **Servizio Polizia postale e per la sicurezza cibernetica** è altresì strutturato in cinque divisioni, che hanno i seguenti compiti

La I Divisione

- assicura la formazione e l'aggiornamento professionale negli ambiti di specifica competenza del Servizio;
- cura i rapporti con l'Ufficio IV - Comunicazione istituzionale della Segreteria del Dipartimento;
- sviluppa campagne di prevenzione e di educazione alla legalità online;
- svolge analisi statistiche relativamente ai fenomeni delittuosi nelle materie di competenza, provvedendo anche alla conseguente pianificazione strategica di prevenzione e contrasto;
- cura la valutazione dei fabbisogni e la pianificazione strategica delle risorse umane assegnate al Servizio e ai Centri Operativi per la Sicurezza Cibernetica (C.O.S.C.) e alle Sezioni Operative per la Sicurezza Cibernetica (S.O.S.C.);

- cura le relazioni sindacali nonché i rapporti con gli Uffici del Dipartimento ed i COSC nelle materie di competenza;
- assicura la gestione del Commissariato di P.S. Online e la gestione informatizzata dell'archivio del Servizio;
- predispone i contributi unitari per gli atti normativi e di amministrazione generale, per gli atti di sindacato ispettivo parlamentare e per le questioni di natura tecnico-giuridica, nelle materie di specifica competenza;
- assicura il coordinamento delle attività di gestione della logistica e delle dotazioni strumentali assegnate ai C.O.S.C. e alle S.O.S.C., comprese le risorse messe a disposizione da Poste Italiane S.p.a nell'ambito delle convenzioni stipulate;
- cura le relazioni internazionali negli ambiti di competenza del Servizio.

La II Divisione

- svolge attività di prevenzione e di contrasto degli illeciti online, con segnato riguardo ai reati contro la persona;
- svolge funzioni in tema di protezione dei minori online, assicurando le attività di prevenzione e di contrasto dei fenomeni di cyberbullismo, di istigazione alle condotte autolesioniste, delle dipendenze on line dei minori, nonché di ogni altra forma di aggressione online nei confronti dei minori stessi;
- garantisce il coordinamento e la pianificazione strategica delle attività informative ed investigative per la prevenzione ed il contrasto delle condotte illecite in materia di comunicazioni, ivi comprese quelle commesse con l'uso dei social network;
- anche in relazione a quanto previsto dagli articoli 14, l4-bis, l4-ter, l4-quater e l4-quinquies della legge 3 agosto 1998, n. 269, nonché dalla legge 29 maggio 2017, n. 71, assicura la gestione del Centro Nazionale di Contrasto alla Pedopornografia Online (C.N.C.P.O.) di cui al predetto articolo l4-bis della legge n. 269 del 1998;
- attraverso il C.N.C.P.O. e le altre strutture interne, provvede alla raccolta in via continuativa e alla gestione delle segnalazioni inerenti alle materie di competenza, ivi comprese quelle provenienti da fonti qualificate pubbliche e private, anche di carattere internazionale, ai fini del coordinamento investigativo sul piano nazionale, nonché internazionale su base bilaterale e multilaterale con gli Organi di Polizia di altri Paesi, nonché con le Organizzazioni di cooperazione internazionale di polizia e di cooperazione internazionale giudiziaria per le materie di specifica competenza;
- assicura il coordinamento delle attività condotte nelle materie di competenza, svolte dagli Uffici periferici della Specialità, garantendo anche lo svolgimento di attività di carattere informativo e investigativo in materia; collabora alle campagne e alle iniziative di informazione e di sensibilizzazione concernenti l'utilizzo corretto e consapevole del web;
- attraverso l'Unità di Analisi del Crimine Informatico (U.A.C.I.), cura l' analisi di tutti i reati e fenomeni di competenza, anche emergenti, attraverso la raccolta e l'elaborazione dei relativi dati, finalizzata alla tutela delle vittime, al profiling criminologico, alla valutazione dei rischi e all'eventuale progettazione di iniziative di ricerca scientifica, eventualmente avvalendosi di collaborazioni con istituzioni universitarie.

La III Divisione

- attraverso il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (C.N.A.I.P.I.C.), svolge le attività per la prevenzione e il contrasto degli attacchi informatici di cui all'articolo 7-bis del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni dalla legge 31 luglio 2005, n. 155;
- svolge, attraverso le proprie strutture, il monitoraggio, l'analisi, le attività di prima risposta ed incident response, in relazione agli attacchi informatici ai danni delle Infrastrutture Critiche;
- assicura il raccordo operativo con i referenti tecnici delle medesime Infrastrutture e con gli Enti pubblici e privati operanti nel settore della cybersicurezza;
- cura l'attività investigativa relativa agli attacchi informatici;
- coordina, nella specifica materia, le attività delle competenti articolazioni periferiche della Specialità della Polizia postale e delle comunicazioni;
- garantisce, nello specifico settore di competenza, il supporto alle attività di gestione dell'ordine e sicurezza pubblica;
- assicura il coordinamento e l'espletamento delle attività informative ed investigative per la prevenzione ed il contrasto alle minacce eversivo-terroristiche in rete, secondo quanto previsto dall'articolo 7-bis del predetto decreto-legge n. 144 del 2005, nonché dall'articolo 2 del decreto legge 18 febbraio 2015, n. 7, convertito, con modificazioni, dalla legge 17 aprile 2015, n. 43, garantendo, su base bilaterale e multilaterale, con gli Organi di Polizia di altri Paesi, nonché con le Organizzazioni di cooperazione internazionale di polizia e di cooperazione internazionale giudiziaria, per le materie di specifica competenza;

- provvede, inoltre, alla gestione dell'Ufficio del punto di contatto HTC Emergency 24/7, previsto dalla Convenzione sul cyber crime, stipulata a Budapest il 23 novembre 2001 e ratificata dalla legge 18 marzo 2008, n. 48, mantenendo, a tal fine, i rapporti con i collaterali organi esteri di polizia e con gli Enti della cooperazione internazionale, assolvendo altresì alle funzioni del Punto di contatto nazionale, ai sensi dell'art. 35 della medesima Convenzione;
- svolge, infine, nelle materie di specifica competenza, attraverso le proprie strutture laboratoriali, attività di ricerca e di sviluppo di soluzioni tecnologiche avanzate per il supporto tecnico-operativo alle attività istituzionali, con particolare riferimento alle attività di analisi forense, coordina e supporta, per i profili di competenza, le attività dei Nuclei Operativi per la Sicurezza Cibernetica istituiti nell'ambito dei C.O.S.C..

La IV Divisione

- assicura il coordinamento delle attività informative e investigative per la prevenzione e il contrasto dei fenomeni di criminalità informatica, caratterizzati dall'utilizzo di particolari tecniche di hacking, tecnologie software e hardware per acquisire, riprodurre e utilizzare fraudolentemente "identità digitali", codici di utilizzo di servizi bancari online o di carte di pagamento nelle transazioni elettroniche o che implichino la contraffazione o l'illecito utilizzo dei mezzi di pagamento elettronici;
- mantiene i rapporti con i referenti della società Poste Italiane S.p.a. al fine di garantire un efficace monitoraggio dei fenomeni delittuosi, in funzione della pianificazione strategica tesa a prevenire i reati e a mitigare i rischi di frode;
- cura, altresì, il coordinamento e la pianificazione strategica dell'attività informativa e investigativa per la prevenzione e il contrasto delle attività illecite in materia di reati postali, di truffe commesse attraverso la rete internet, di illeciti commessi attraverso i social network e di reati connessi alla telefonia;
- mantiene i rapporti, per gli aspetti di competenza, con il Ministero dello Sviluppo Economico;
- mantiene altresì i rapporti con l'Autorità per le Garanzie nelle Comunicazioni, attraverso l'apposita sezione operativa allocata presso la medesima Autorità; la predetta sezione operativa assicura il collegamento e il supporto operativo con la stessa Autorità, in relazione alle specifiche funzioni di quest'ultima in tema di regolamentazione e vigilanza nei settori delle telecomunicazioni, dell'audiovisivo, dell'editoria e delle poste.

La V Divisione:

- cura la gestione dell'infrastruttura tecnologica del Servizio, nonché la custodia del materiale informatico assegnato;
- garantisce il supporto tecnico-operativo alle attività d'istituto della Specialità in materia di sicurezza cibernetica, ivi compresi il supporto alle attività di digital forensics nei settori di specifica competenza;
- assicura, inoltre, il supporto in materia di sistemi di intelligenza artificiale per la sicurezza cibernetica;
- svolge attività di analisi di immagini a supporto delle attività di contrasto della pedo-pornografia;
- cura i rapporti con gli interlocutori di riferimento, pubblici e privati, attivi nel campo della ricerca e dell'innovazione scientifica, per il costante aggiornamento di metodologie e soluzioni tecnologiche, necessarie alle esigenze della Specialità, nell'ambito della digital forensics e più in generale nel settore della ricerca e dell'innovazione scientifica;
- concorre alla definizione di piani di formazione specialistica per profili di information technology (IT);
- assicura la raccolta delle esigenze volte alla realizzazione di nuovi sistemi IT d'interesse del Servizio, la pianificazione delle acquisizioni IT e la gestione dei relativi contratti;
- garantisce le funzioni di focal point per la gestione degli accessi alle banche dati istituzionali ed investigative in uso al Servizio;
- assicura, nei settori tecnici di rispettiva competenza, il coordinamento delle articolazioni periferiche della Specialità;
- cura l'implementazione, secondo gli standard e la normativa di settore, delle misure di sicurezza IT relative all'infrastruttura informatica gestita attuando gli indirizzi e le politiche delineate dai competenti uffici della Polizia di Stato.

Il **Servizio per la Sicurezza cibernetica del Ministero dell'Interno**, infine, ha due divisioni cosi suddivise

La I Divisione cura la gestione del Computer Emergency Response Team (indicata nel documento

con acronimo C.E.R.T.) del Ministero dell'Interno, svolgendo le necessarie attività di carattere tecnico e amministrativo; provvede, attraverso il predetto C.E.R.T., alla raccolta e all'analisi dei dati e delle informazioni relativi alla minacce e agli incidenti informatici concernenti la sicurezza delle reti, dei sistemi informativi e delle infrastrutture informatiche del Ministero; cura, inoltre, attraverso il C.E.R.T. del Ministero, il monitoraggio e l'analisi precoce delle vulnerabilità di protezione rese note, lo scambio di informazioni con le istituzioni e gli altri enti competenti, secondo le modalità e i termini stabiliti dalle vigenti disposizioni, per la prevenzione e il trattamento delle minacce e degli incidenti informatici; assicura, per mezzo del C.E.R.T. del Ministero, la gestione degli eventuali incidenti informatici e le attività di risposta agli stessi, al fine di preservare l'integrità e la continuità dei servizi; garantisce il coordinamento delle iniziative di pertinenza delle strutture competenti volte ad assicurare le funzioni di sicurezza informatica, operanti nell'ambito del Gabinetto, degli altri Uffici di diretta collaborazione, dei Dipartimenti, degli altri Uffici di livello equiparato del Ministero dell'interno, alle articolazioni periferiche comunque denominate del medesimo Dicastero, nonché dell'Agenzia nazionale per l'amministrazione e la destinazione dei beni sequestrati e confiscati alla criminalità organizzata.

La I Divisione espleta, negli ambiti di competenza, attività di analisi della sicurezza informatica, svolgendo in favore del Comitato di analisi per la sicurezza cibernetica del Ministero dell'interno di cui all'art. 109-septies attività di ricerca, studio e consulenza nelle materie di competenza, operando, a tal fine, in collaborazione con il C.E.R.T. del Ministero; cura l'attività di impulso al fine di verificare l'osservanza degli adempimenti normativi e degli standard di sicurezza cibernetica; fornisce ausilio al C.E.R.T. del Ministero per la predisposizione della relazione annuale al Ministro dell'interno in materia di sicurezza cibernetica; cura la gestione delle risorse umane, della formazione e dell'addestramento, unitamente alla gestione delle risorse economiche e delle infrastrutture.

La I Divisione, infine, cura le attività di segreteria e di supporto al Comitato di analisi per la sicurezza cibernetica del Ministero dell'interno di cui all'art. 109-septies.

La II Divisione cura la gestione del Centro di Valutazione assicurando le attività di valutazione, controllo e certificazione inerenti alle forniture di beni, sistemi e servizi ICT da impiegare sulle reti, sui sistemi informativi e sulle infrastrutture informatiche del Ministero dell'Interno inclusi nel perimetro di sicurezza nazionale cibernetica ; esercita le funzioni di ispezione e di verifica di cui all'articolo 1, comma 6, lettera c) del decreto-legge n.105 del 2019; svolge le attività finalizzate all'identificazione e alla valutazione della vulnerabilità delle reti, dei sistemi informativi e delle infrastrutture informatiche del Ministero, anche attraverso l'organizzazione di esercitazioni e simulazioni; cura la predisposizione di direttive tecniche e di policy di sicurezza nelle materie di rispettiva competenza; promuove le campagne informative e le iniziative di formazione e sensibilizzazione in favore del personale delle diverse carriere e qualifiche del Ministero.

21/06/2024