FONDAZIONE
BRUNO KESSLER

ORGANIZZAZIONE PER LA SICUREZZA INFORMATICA NELLA FONDAZIONE BRUNO KESSLER

CONTESTO NORMATIVO

In ottemperanza al complesso e dinamico quadro normativo vigente, finalizzato all'innalzamento dei livelli di cybersicurezza e resilienza a livello dell'Unione Europea e nazionale, si delinea una disciplina di riferimento articolata e interconnessa. Tale disciplina impone obblighi, attribuisce responsabilità e definisce misure tecniche e organizzative a carico dei soggetti erogatori di servizi essenziali o importanti. Il fondamento di tale architettura normativa è costituito dalla Direttiva (UE) 2022/2555, nota come Direttiva NIS2, la quale persegue la finalità principale di assicurare un livello comune ed elevato di cybersicurezza in tutta l'Unione. Detta Direttiva introduce un'evoluzione sostanziale rispetto alla precedente normativa, estendendone l'ambito di applicazione a nuovi settori e introducendo requisiti più stringenti in materia di gestione del rischio, obblighi di notifica degli incidenti informatici e poteri di supervisione in capo alle autorità competenti.

L'ordinamento giuridico italiano ha provveduto al recepimento della Direttiva NIS2 con il Decreto Legislativo 4 settembre 2024, n. 138 (di seguito, "Decreto NIS"). Tale decreto traspone i principi e gli obblighi sanciti a livello europeo, individuando nell'Agenzia per la Cybersicurezza Nazionale (ACN) l'autorità nazionale competente e definendo il perimetro soggettivo di applicazione, che comprende le entità qualificate come "soggetti essenziali" e "soggetti importanti", i quali sono tenuti all'adempimento delle prescrizioni ivi contenute.

Al fine di fornire direttive operative per l'adempimento degli obblighi normativi, l'Agenzia per la Cybersicurezza Nazionale ha emanato la Determinazione n. 164179 in data 14 aprile 2025. Tale atto amministrativo, recante le "Specifiche di base per l'adempimento agli obblighi di cui agli articoli 23, 24, 25, 29 e 32 del decreto NIS", costituisce un allegato tecnico che, sulla base del Framework Nazionale di Cybersecurity, disciplina in modo analitico le misure di sicurezza che i soggetti destinatari della normativa devono implementare. Le aree di intervento spaziano dalla governance alla protezione delle infrastrutture tecnologiche, dalla gestione degli incidenti alla sicurezza della catena di approvvigionamento.

In via complementare, lo standard internazionale ISO/IEC 27001 costituisce un paradigma di riferimento e una prassi operativa consolidata per la gestione della sicurezza delle informazioni. Esso fornisce un modello per l'istituzione, l'attuazione, il mantenimento e il miglioramento continuo di un Sistema di Gestione della Sicurezza delle Informazioni (SGSI). Benché l'adesione a tale standard rivesta carattere volontario, i principi e i controlli in esso codificati sono universalmente riconosciuti quale strumento efficace per il conseguimento e la dimostrazione della conformità ai requisiti normativi, inclusi quelli derivanti dalla Direttiva NIS2 e dal relativo decreto di recepimento.

FONDAZIONE
BRUNO KESSLER

ORGANIZZAZIONE PER LA SICUREZZA INFORMATICA

Per chiarire la situazione attuale, si ritiene opportuno delineare brevemente il ruolo del JointLab per la Cybersecurity e la sua funzione nella salvaguardia dell'infrastruttura IT della Fondazione, antecedentemente all'entrata in vigore della Direttiva NIS2. Tale premessa faciliterà la comprensione del ruolo di supporto che il JointLab assume con l'entrata in vigore della NIS2 a supporto dell'implementazione delle misure previste dalla stessa e dalla normativa di recepimento, con particolare riferimento all'ausilio operativo dei ruoli di Chief Information Security Officer e di Cyber Risk Manager descritti in seguito.

Da gennaio 2025 è stato costituito il **JointLab per la Cybersecurity,** laboratorio interno ad FBK composto da un gruppo di ricercatori afferenti al Centro per la Cyber Security insieme ad alcuni membri del Servizio Soluzioni Digitali e Infrastrutture IT. Esso costituisce pertanto un polo di aggregazione di competenze specialistiche, la cui capitalizzazione abilita lo sviluppo di servizi di consulenza avanzata e la traslazione delle problematiche operative in filoni di ricerca scientifica di alto impatto. Il Laboratorio risponde infatti al duplice mandato di elevare la postura di sicurezza dell'ente e, contestualmente, di agire quale motore di innovazione per lo sviluppo di servizi e applicazioni secondo un paradigma di security-by-design. Tale approccio strategico e operativo trascende i meri obiettivi di efficacia ed efficienza, per integrare nativamente i requisiti di protezione e affidabilità dell'infrastruttura tecnologica.

Il JointLab per la Cybersecurity fornisce inoltre **consulenza e supporto specialistico,** in particolare nell'analisi e valutazione delle minacce e delle vulnerabilità, nel controllo dei rischi e nell'analisi delle minacce informatiche, quali ad esempio le comunicazioni elettroniche sospette, anche come servizio a terzi.

La funzione del JointLab è pertanto strumentale al conseguimento e al mantenimento della conformità rispetto al quadro normativo cogente, anche con riferimento alla Direttiva (UE) 2022/2555 (NIS2) e alla normativa italiana di recepimento.

La Fondazione Bruno Kessler rientra nei "soggetti importanti" per la Direttiva NIS2, con tipologia "1. Ricerca", "1.1. Organizzazioni di ricerca", come confermato a seguito della registrazione della Fondazione sul Portale dei Servizi ACN con autodichiarazione di tipologia e settore di riferimento, e da successiva comunicazione ACN (ai sensi dell'articolo 7, comma 3, lettera a) del decreto legislativo n 138 del 2024), di "inserimento nell'elenco dei soggetti NIS" (DNISA00008719) del 13 aprile 2025.

La normativa NIS2 prevede per i "soggetti importanti" che sia definita, approvata e resa nota da parte degli organi di amministrazione l'organizzazione per la sicurezza informatica, con definizione dei ruoli e responsabilità.

L'art. 20 della Direttiva NIS2 e l'art. 23 del D.Lgs. 138/2024 prevedono che le responsabilità siano in capo "all'organo amministrativo e all'organo direttivo". In Fondazione, sono stati individuati quali destinatari dell'obbligo:

- il **Consiglio di Amministrazione**, quale "organo amministrativo", che definisce il rischio ed esercita la propria funzione di indirizzo e governo approvando le procedure, le policies e gli standard generali proposti dai punti

di contatto per la cybersecurity. A tale organo compete inoltre sulla base della normativa anche l'approvazione del piano di formazione per il personale, riconoscendone il valore quale misura di mitigazione del rischio essenziale. La vigilanza strategica sul corretto adempimento del quadro normativo e delle politiche interne resta una sua prerogativa fondamentale.

- Il **Segretario generale**, quale "organo direttivo" che, assumendo la visione unitaria degli indirizzi e degli obiettivi varati dal Consiglio di Amministrazione e che è chiamato a risponderne anche sulla base dei principi previsti dalla regolamentazione organizzativa e gestionale della Fondazione, che sovrintende all'implementazione degli obblighi e dell'implementazione delle misure approvate dal Consiglio di Amministrazione.

Al fine di assicurare la piena conformità alle prime prescrizioni normative previste per i soggetti importanti, la Fondazione ha designato nella seduta del Consiglio di Amministrazione del 7 febbraio 2025 il Punto di contatto e relativo Sostituto, nelle persone di Mirco Vivaldi e di Matteo Rizzi. Tramite Portale dei Servizi, sono state aggiornate e trasmesse le informazioni di cui all'articolo 7 (Adozione degli obblighi di base in materia di misure di sicurezza informatica e notifica di incidenti), commi 4 e 5:

- lo spazio di indirizzamento IP pubblico e i nomi di dominio in uso;
- gli accordi di condivisione delle informazioni sulla sicurezza informatica (in essere con la Polizia Postale);
- gli organi di amministrazione e direttivi preposti al ruolo di Responsabili per le violazioni, tramite inserimento nel Portale di CF e PEC personali e conseguente accettazione dell'assegnazione di responsabilità degli stessi tramite SPID.

Inoltre, sono state attribuite specifiche responsabilità operative alle seguenti persone che presidiano la sicurezza informatica, con riferimento alle competenze relative al monitoraggio, alla vigilanza, alla esecuzione e al coordinamento in materia di sicurezza delle informazioni, oltre a coadiuvare la stesura di regolamenti, procedure e policy. Essi agiscono come fulcro del sistema di gestione, assicurando l'attuazione della Direttiva NIS2 e delle altre normative pertinenti.

- **Mirco Vivaldi**
  - **Chief Information Security Officer (CISO)** per gli aspetti che riguardano i sistemi informatici ed infrastrutturali interni, con particolare riferimento alla **definizione**, **attuazione**, **mantenimento** e **miglioramento della Sicurezza delle Informazioni**. È incaricato di sovrintendere all'applicazione delle procedure operative per la **gestione degli incidenti di sicurezza**, garantendo che le comunicazioni agli stakeholder interni ed esterni avvengano secondo le modalità e le tempistiche prescritte dalla normativa. Sovrintende il **monitoraggio continuo dei rischi per la sicurezza dei sistemi informativi e di rete**. È altresì delegato alla supervisione ed al **controllo della sicurezza informatica per l'intera catena di approvvigionamento**, assicurando che i fornitori di beni e servizi ICT rispettino i requisiti di sicurezza stabiliti. Rientrano nelle sue competenze la **gestione degli inventari degli asset hardware e software, la gestione delle identità digitali, dei privilegi di accesso e delle modalità di autenticazione** secondo i principi del minimo privilegio. Si occupa di

definire, **attuare e testare i piani di continuità operativa, di ripristino in caso di disastro e di gestione delle crisi informatiche**, nonché di sviluppare e implementare il piano di gestione e notifica degli incidenti di sicurezza. La sua funzione include la responsabilità sui processi di gestione delle vulnerabilità, sul monitoraggio degli eventi di sicurezza e sul **coordinamento dei programmi di formazione e sensibilizzazione del personale** in materia di cybersecurity, fatta salva ogni competenza relativa alla sicurezza fisica e alla protezione dei dati personali che esuli dalla sicurezza logica e infrastrutturale.

  - E' inoltre Coordinatore del JointLab per la Cybersecurity di FBK e Punto di Contatto per la Direttiva NIS2.

- **Dott. Matteo Rizzi**
  - **Cybersecurity Risk Manager -** per gli aspetti che riguardano i processi di valutazione e trattamento del rischio informatico, con particolare riferimento alla **supervisione** e **esecuzione operativa delle attività di gestione del rischio cyber**. In tale veste, attua il piano di **gestione dei rischi per la sicurezza informatica**, curando **l'identificazione**, **l'analisi**, la **valutazione**, il **trattamento** e il **monitoraggio continuo dei rischi per la sicurezza dei sistemi informativi e di rete**, in conformità con le politiche definite e approvate. Tale delega comprende la **definizione e documentazione delle politiche di sicurezza informatica**, e di sovrintendere ai processi di gestione del rischio cyber. La sua delega si estende inoltre alla **valutazione e alla gestione del rischio associato alla catena di approvvigionamento**, assicurando che i rischi introdotti da fornitori terzi, dai loro prodotti e servizi siano compresi, documentati e mitigati. Effettua inoltre la supervisione dei **processi di gestione delle vulnerabilità**, inclusa la ricezione, l'analisi e la risposta alle informative concernenti nuove debolezze dei sistemi, nonché del monitoraggio della tempestiva applicazione delle necessarie contromisure. La sua funzione comprende infine il **coordinamento delle attività di formazione e sensibilizzazione del personale in materia di rischio informatico**, la verifica dell'adeguatezza delle misure di sicurezza implementate e la **produzione di reportistica periodica sullo stato di conformità** e sul profilo di rischio della Fondazione, agendo **in stretto coordinamento con il Chief Information Security Officer** per garantire un approccio integrato e coerente alla sicurezza delle informazioni.
  - È inoltre parte integrante del JointLab per la Cybersecurity di FBK e Sostituto Punto di Contatto per la Direttiva NIS2.

Tali figure sono paritarie, agiscono in modo sinergico e collaborativo per garantire un approccio integrato e olistico alla gestione della cybersicurezza per la Fondazione. Le due figure operano sul medesimo piano funzionale e rispondono in maniera coordinata e allineata alle richieste, alle necessità e alle sfide che si presenteranno nel perseguimento degli obiettivi di adempimento normativo e di governo della sicurezza informatica.

L'approccio metodologico adottato nell'espletamento delle attività è orientato agli obiettivi strategici della Fondazione declinati poi in quelli delle relative Articolazioni organizzative. Si applicheranno uno o più framework e buone pratiche di Governance, Risk and Compliance (GRC), al fine di pervenire a un ponderato equilibrio tra le esigenze di sicurezza informatica e gli obiettivi di business.

FONDAZIONE
BRUNO KESSLER

ULTERIORI RESPONSABILI COINVOLTI

L'attuazione delle procedure di sicurezza, promossa, coordinata e monitorata dall'approccio sinergico delle figure di riferimento precedentemente esposte, è una responsabilità diffusa che richiede una stretta collaborazione tra i Responsabili delle varie Articolazioni, Unità e Uffici, in particolare con:

- I **Direttori delle Articolazioni organizzative di ricerca e studio** che sono responsabili dell'implementazione delle misure di sicurezza all'interno delle proprie aree di competenza, con un'attenzione specifica ai dispositivi **non** gestiti centralmente.
- I **Responsabili del Servizio Appalti e Contratti** e del **Servizio Patrimonio** che forniscono il loro supporto specialistico per l'analisi dei rischi inerenti, rispettivamente, alla catena di approvvigionamento ed alla componente tecnologica dell'Internet of Things (IoT).
- **Il Responsabile del Servizio Soluzioni Digitali e Infrastrutture IT** che garantisce il supporto operativo per la messa in sicurezza degli accessi e per la risposta tecnica agli incidenti, anche mediante la propria Unità **FBK Digital** che collabora per la sicurezza delle applicazioni sviluppate internamente.
- Il rafforzamento dell'interoperabilità operativa è un obiettivo chiave, perseguito attraverso la collaborazione strutturata con ulteriori presidi coinvolti, in particolare con l'**Unità Prevenzione della Corruzione, Trasparenza e Privacy** e **con la DPO,** che assicurano la coerenza con le normative in materia di protezione dei dati personali, e con il **Team Certificazioni** per mantenere l'allineamento cruciale con lo standard ISO/IEC 27001.

Il sistema di vigilanza si articola su due livelli:

- la **vigilanza interna** è esercitata dal Consiglio di Amministrazione, dal Chief Information Security Officer e dal Cybersecurity Risk Manager, secondo le rispettive competenze strategiche e operative;
- la **vigilanza esterna** è invece di competenza delle autorità designate, ovvero l'**Agenzia per la Cybersicurezza Nazionale (ACN)** e il **CSIRT Italia**, ai quali la Fondazione è tenuta a rispondere ed a notificare gli incidenti secondo le disposizioni di legge.