Pirola
Pennuto
Zei

GDPR e Cybersecurity

UNINDUSTRIA
25 novembre 2025

Avv. Mario Valentini

Pirola Pennuto Zei

GDPR e NIS2

Si tratta di **normative complementari**, che mirano a rafforzare la sicurezza e la protezione di informazioni. Il **GDPR** è principalmente volto a tutelare i dati personali e i diritti e le libertà fondamentali degli individui. La **NIS2** si concentra sulla sicurezza e la resilienza delle reti e dei sistemi informativi che sono cruciali per la fornitura di servizi per la collettività.

- Entrambe le normative hanno un approccio basato sul rischio e prevedono obblighi di notifica di incidenti di sicurezza.
- Valutazione della gravità dell'incidente.
- Cooperazione tra Autorità di Vigilanza.

Sicurezza del trattamento – Art. 32 GDPR

L'art. 32 GDPR impone al Titolare ed al Responsabile del trattamento di garantire un livello di sicurezza dei dati personali adeguato al rischio.

Il Titolare del trattamento è, inoltre, tenuto a notificare eventuali violazioni dei dati personali all'Autorità di Controllo competente e comunicare la violazione dei dati personali all'interessato del trattamento («Data Breach»).

OBIETTIVO

⇩

Proteggere i dati personali da distruzione, perdita, modifica accidentale o illecita, accesso o divulgazione non autorizzata.

Data breach

VIOLAZIONE DEI DATI PERSONALI «DATA BREACH»

Art. 33 e art. 34 GDPR

Notificare tutte le violazioni dei dati personali all'Autorità Garante per la protezione dei dati personali, **a meno che sia improbabile che la violazione possa effettivamente rappresentare un rischio per i diritti e per le libertà degli assistiti e degli interessati**

comunicare le violazioni alle persone interessate in caso di **elevato rischio per i loro diritti e la libertà personali**

Data breach

CHE COSA SIGNIFICA «VIOLAZIONE DEI DATI PERSONALI»

Art. 4 n. 12 GDPR

"la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati".

Data breach

Un incidente di sicurezza costituisce una violazione dei dati personali ove questo comporti una:

- "**violazione della riservatezza**", in caso di divulgazione dei dati personali o accesso agli stessi non autorizzata o accidentale, in quanto ai dati devono accedere solo le persone autorizzate

- "**violazione dell'integrità**", in caso di modifica non autorizzata o accidentale dei dati personali, in quanto i dati non devono subire modifiche o cancellazioni non autorizzate

- "**violazione della disponibilità**", in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali, in quanto ai dati si deve accedere tutte le volte in cui se ne ha bisogno

Se si verifica almeno uno di questi tre casi, si ha una violazione di dati personali

Data breach

Notifica della violazione all'Autorità Garante

Nel caso in cui la valutazione, effettuata dal Titolare del trattamento circa la probabilità o meno che il ***data breach*** avvenuto possa effettivamente rappresentare un rischio per i diritti e per le libertà degli interessati, abbia esito affermativo, lo stesso tempestivamente e comunque **non oltre le 72 ore** dalla conoscenza della violazione, **dovrà notificare la violazione all'Autorità Garante della protezione dei dati personali**.

Data breach

L'art. 33 del GDPR prevede che in caso di violazione dei dati il Titolare del trattamento, dovrà notificare l'evento al Garante, tranne nel caso in cui "***sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche***"

ad esempio… nel caso di perdita di una chiavetta USB con dati cifrati. Se la chiave di cifratura rimane in possesso del Titolare del trattamento e non si tratta dell'unica copia dei dati personali, questi ultimi sarebbero inaccessibili a qualsiasi pirata informatico. Ciò significa che è improbabile che la violazione presenti un rischio per i diritti e le libertà degli interessati in questione. Se in seguito diventa evidente che la chiave di cifratura è stata compromessa o che il software o l'algoritmo di cifratura è vulnerabile, il rischio per i diritti e le libertà delle persone fisiche cambia e potrebbe quindi essere necessaria la notifica.

Data breach

Alla luce di quanto disposto nel Provvedimento dell'Autorità Garante per la protezione dei dati personali del 27 maggio 2021 a **partire dal 1° luglio 2021,** la notifica di una violazione di dati personali deve essere inviata al Garante tramite un'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità, e raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/

Nella stessa pagina è disponibile un modello facsimile, da NON utilizzare per la notifica al Garante ma utile per vedere in anteprima i contenuti che andranno comunicati al Garante.

Per semplificare gli adempimenti previsti per i Titolari del trattamento, il Garante ha messo disposizione un **apposito strumento di autovalutazione (*self assessment*),** che consente di individuare le azioni da intraprendere a seguito di una violazione dei dati personali derivante da un incidente di sicurezza.

Data breach

Quando si deve comunicare la violazione anche agli interessati

L'**art. 34 del GDPR, paragrafo 1**, afferma che: "*Quando la violazione dei dati personali è suscettibile di presentare un* ***rischio elevato per i diritti e le libertà delle persone fisiche,*** *il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo*".

La comunicazione della violazione dei dati agli interessati è prevista solo se è suscettibile di presentare un **rischio elevato per i diritti e le libertà delle persone fisiche** ed in tal caso il Titolare del trattamento deve **comunicare la violazione** dei dati all'interessato **senza ingiustificato ritardo** come indicato all'art. 34 del GDPR, in quanto l'obiettivo principale della comunicazione agli interessati consiste nel fornire loro informazioni specifiche sulle misure che questi possono prendere per proteggersi.

Data breach

Ai sensi dell'**art. 34 del GDPR, paragrafo 3**, non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:

a) il titolare del trattamento ha messo in atto le **misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione**, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

b) il titolare del trattamento ha **successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato** per i diritti e le libertà degli interessati;

c) detta comunicazione richiederebbe **sforzi sproporzionati**. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Data breach

Il Titolare del trattamento deve comunque **documentare ogni violazione** avvenuta, unitamente alle circostanze che l'hanno causata, alle sue conseguenze e ai provvedimenti adottati per porvi rimedio.

Tale procedimento deve essere supportato dalla tenuta, da parte del Titolare del trattamento, del cosiddetto "**registro delle violazioni**", che consiste in un documento che ha la duplice funzione di consentire, al Titolare, un **agevole monitoraggio e controllo di tutte le violazioni di dati personali**, avvenute nel corso delle proprie attività di trattamento e, al Garante, in caso di ispezione, di verificare la valutazione svolta, ai fini del rispetto dell'obbligo di notifica.

Infatti, indipendentemente dal fatto che una violazione debba o meno essere notificata al Garante, il Titolare del trattamento **deve conservare la documentazione di tutte le violazioni.**

Data breach

Tale aspetto è contenuto nell'articolo 33 comma 5 del GDPR in base al quale: "***Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo***".

Tale obbligo è collegato al principio di **responsabilizzazione (*accountability*)**, di cui all'articolo 5 comma 2 del GDPR, principio che abbiamo menzionato sopra.

Come richiesto dall'articolo 33, comma 5 del GDPR il Titolare del trattamento è tenuto a registrare i dettagli relativi alla violazione, comprese le cause, i fatti e le categorie dei dati personali interessati, ed indicare gli effetti e le conseguenze della violazione e i provvedimenti adottati per porvi rimedio.

Introduzione alla NIS2

FRAMEWORK NORMATIVO SULLA CYBERSICUREZZA : IL RECEPIMENTO DELLA DIRETTIVA NIS2

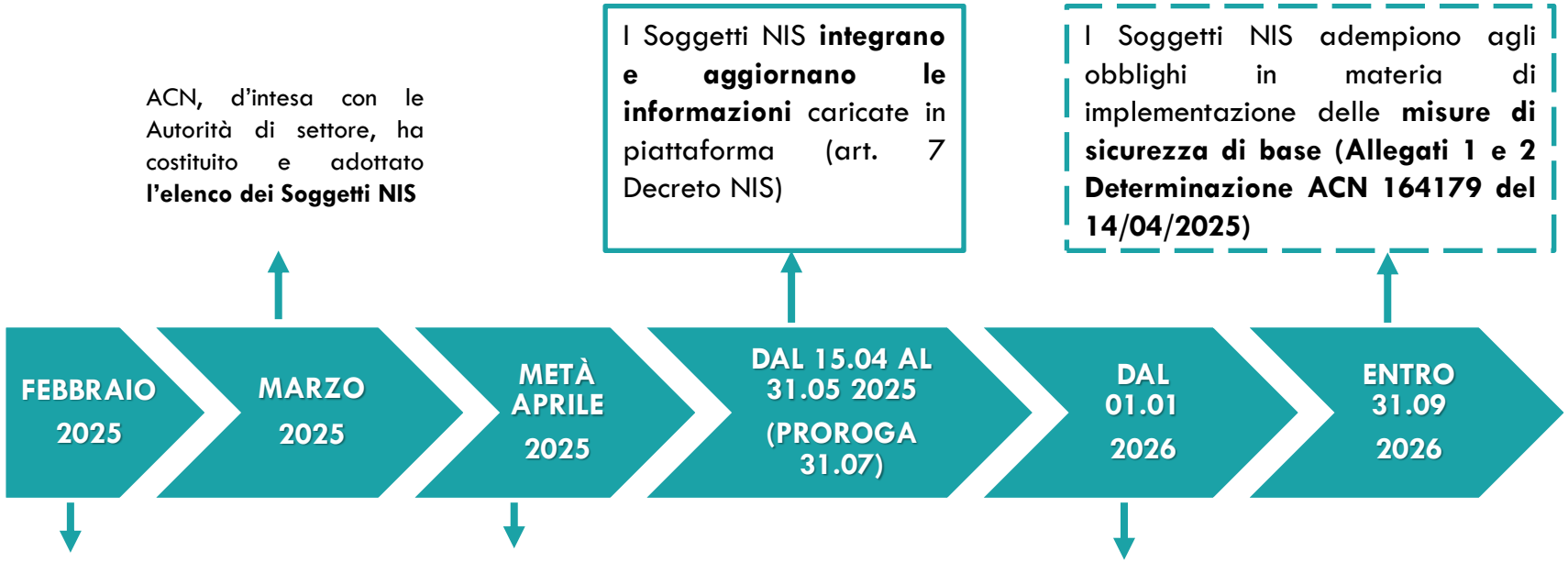
Direttiva (UE) n. 2022/2555 (« Direttiva NIS2»)

- **Aggiorna le norme dell'Unione Europea in materia di cybersicurezza** introdotte nel 2016, modernizzando e uniformando il quadro giuridico esistente
- Fa **parte di un ampio pacchetto di strumenti giuridici e di iniziative a livello dell'Unione,** mirato ad **aumentare la resilienza di soggetti pubblici e privati** alle minacce nell'ambito cibernetico
- Mira a **garantire un aumento del livello di sicurezza cibernetica comune** grazie all'armonizzazione delle norme applicabili ai diversi operatori nei diversi Stati membri e al rafforzamento dei livelli *standard* di sicurezza rispetto a quelli previsti dalla disciplina vigente

D.Lgs. n. 138/2024 («Decreto NIS»)

- Il Decreto NIS impone l'**adozione di misure di sicurezza proporzionate e basate su un approccio multi-rischio**
- Rafforza i meccanismi di **notifica degli incidenti** e i **poteri ispettivi e sanzionatori delle autorità competenti**

FRAMEWORK NORMATIVO SULLA CYBERSICUREZZA: LE TEMPISTICHE



AGGIORNAMENTO DELLE INFORMAZIONI SUL PORTALE ACN

- **Entro il 31 maggio di ogni anno:** aggiornamento delle informazioni di cui all'articolo 7, commi 4 e 5 del Decreto NIS tramite il Servizio NIS/aggiornamento annuale

- **Tempestivamente e, in ogni caso, entro 14 giorni dalla data di modifica:** notifica – sempre tramite i servizi NIS - di qualsiasi modifica/integrazione/variazione delle informazioni trasmesse

AGGIORNAMENTO ANNUALE INFORMAZIONI – TO DO LIST

- Invitare il **sostituto punto di contatto**
- Verificare la **correttezza e l'aggiornamento dei dati** anagrafici e di contatto
- Elencare i **componenti degli organi di amministrazione e direttivi**
- Invitare (se ritenuto opportuno) la **segreteria**
- Elencare **i servizi che rientrano nell'ambito di applicazione della direttiva NIS** (+stati membri in cui vengono offerti)
- Elencare gli **indirizzi IP statici (pubblici) e i nomi di dominio** in uso o nella disponibilità del soggetto NIS
- Elencare gli **accordi di condivisione** delle informazioni

AGGIORNAMENTO ANNUALE DELLE INFORMAZIONI SUL PORTALE ACN

La Determinazione 136177/2025 richiede ai Soggetti NIS di comunicare, oltre al Punto di contatto, anche **altre figure coinvolte nella gestione degli adempimenti NIS quali**:

- **Sostituto punto di contatto:** persona fisica designata (medesime modalità previste per la designazione del PdC) - supporta il Punto di contatto nelle proprie funzioni, potendo interloquire direttamente con l'ACN nonché effettuare variazioni/aggiornamento annuale sul Portale NIS

- **Segreteria (facoltativa):** persona fisica che supporta il Punto di contatto ed il Sostituto per promuovere l'efficace interlocuzione con l'ACN. Può visualizzare ed aggiornare le informazioni richieste sui Servizi NIS ma non effettuare la trasmissione di comunicazioni inerenti al perfezionamento degli adempimenti NIS

- **Operatori (facoltativi):** una o più persone fisiche che supportano il Punto di contatto (e il Sostituto) operando sui Servizi NIS. Gli operatori agiscono sul Portale dei Servizi NIS limitatamente alle attività di visualizzazione ed aggiornamento delle informazioni richieste

AGGIORNAMENTO ANNUALE DELLE INFORMAZIONI SUL PORTALE ACN

ELENCO DEI SERVIZI NIS

Tutti i servizi che rientrano nell'ambito di applicazione del Decreto NIS (ossia tutti i servizi di cui agli allegati I,II, III e IV) **e in quali Stati membri (inclusa l'Italia) sono erogati dal Soggetto NIS.** (Nei gruppi di imprese, l'obbligo di aggiornamento annuale deve essere assolto da ogni persona giuridica distintamente)

INDIRIZZI IP E NOMI DI DOMINIO

Tutti gli indirizzi IP statici e pubblici che il Soggetto NIS utilizza o ha a propria disposizione (anche ove acquisiti tramite contratti o accordi con fornitori di servizi di registrazione di nomi di dominio o altre organizzazioni responsabili della fornitura di nomi di dominio)

Tutti gli indirizzi IP e i nomi di dominio gestiti per conto di terzi (i.e., clienti) **o da terzi** (i.e., fornitori di servizi). (Se gli indirizzi IP e nomi di domino sono in uso o nella disponibilità di più organizzazioni, ogni organizzazione dovrà elencare gli indirizzi IP e i nomi di dominio presenti - devono essere elencati, se del caso, anche gli indirizzi IP di filiali dell'organizzazione localizzate al di fuori del territorio nazionale o UE. Al contrario, non è necessario indicare anche gli indirizzi IP e i nomi di dominio riferiti a società estere che fanno parte del medesimo gruppo di imprese.)

ACCORDI DI CONDIVISIONE

Accordi di condivisione delle informazioni sulla sicurezza informatica, al fine di prevenire o rilevare gli incidenti e aumentare il livello di sicurezza informatica dei quali il Soggetto NIS sia parte. (Il termine per l'adeguamento a tale prescrizione è fissato ad ottobre 2026. Nel corso dell'aggiornamento annuale 2025 è prevista la sola notifica degli accordi di condivisione vigenti e sottoscritti successivamente all'entrata in vigore del Decreto NIS. La notifica degli accordi previgenti l'entrata in vigore del Decreto NIS è rimandata all'aggiornamento annuale 2026.)

AGGIORNAMENTO ANNUALE DELLE INFORMAZIONI SUL PORTALE ACN

ORGANI DI AMMINISTRAZIONE E DIRETTIVI

- Sono gli organi che detengono il **potere di direzione dell'organizzazione**, incluso, ove presente, il Consiglio di Amministrazione (cfr. articolo 1, comma 1, lettera e) Determinazione ACN 136117/2025)
- Le «**persone fisiche responsabili ai sensi dell'articolo 38, comma 5, del Decreto NIS**» sono le **persone fisiche che compongono gli organi di amministrazione e gli organi direttivi dei soggetti essenziali e dei soggetti importanti.** (Nelle organizzazioni in cui non è previsto un CDA, è necessario individuare l'organo che svolge le analoghe funzioni ed elencarne i membri.) In ogni caso, il rappresentante legale è considerato tra i componenti degli organi di amministrazione e direttivi
- I dirigenti aziendali, le persone fisiche che svolgono le funzioni di punto di contatto (e sostituto), di CISO o di responsabile della sicurezza aziendale e che non hanno anche la carica di consigliere di amministrazione della Società, NON sono considerate membri degli organi di amministrazione e direttivi

E' preferibile, ma non obbligatoria, l'indicazione dell'indirizzo PEC individuale e/o nominativo dei componenti degli organi di amministrazione e direttivi che vengono elencati, essendo sufficiente indicare un indirizzo PEC funzionale dell'organizzazione (come il domicilio digitale) o, qualora non disponibile, un indirizzo PEO aziendale.

ADEMPIMENTI SUCCESSIVI: LE MISURE DI SICUREZZA DI BASE

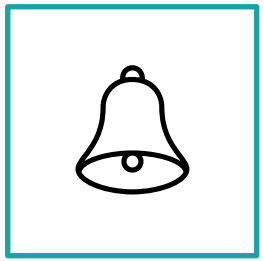
Termine per l'adozione delle misure di sicurezza di base che si applicano a **tutti i sistemi informativi e di rete del Soggetto NIS: diciotto mesi dalla ricezione, da parte del Soggetto NIS della comunicazione di inserimento nell'elenco dei Soggetti NIS (entro settembre 2026).**

I requisiti delle misure di sicurezza indicano cosa deve fare un Soggetto NIS per essere conforme alle misure di sicurezza in termini di specifiche da realizzare. Tali specifiche possono essere generalmente distinte in due tipologie:

- **Tecniche**, implicano l'adozione e l'utilizzo di strumenti tecnologici – e.g., la cifratura, modalità di autenticazione multifattore
- **Amministrative**, riguardano la gestione, l'organizzazione, la documentazione e il controllo di processi e attività, e.g., il Soggetto NIS deve essere in possesso o provvedere all'elaborazione di una serie di documenti, ivi incluse **politiche per la gestione del rischio di cybersicurezza**

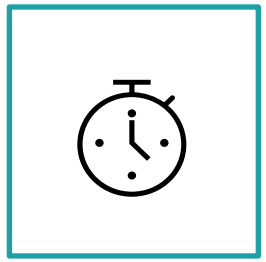
Mantenere un elenco aggiornato dei sistemi critici	Definire e approvare l'organizzazione cyber	Mantenere inventari aggiornati degli asset IT, IoT e OT	Identificare e gestire le vulnerabilità nei sistemi informativi
Adottare procedure documentate per l'accesso ai sistemi	Adottare una politica di cybersecurity approvata	Gestire l'accesso con credenziali robuste e l'autenticazione multi-fattore per i sistemi rilevanti	Proteggere i dati a riposo e in transito con cifratura sicura
Integrare la cybersicurezza nei processi di approvvigionamento	Definire e documentare piani per la continuità operativa e ripristino	Assicurarsi che gli aggiornamenti di sicurezza siano tempestivi e che i registri di access log siano sicuri	Proteggere le reti da accessi non autorizzati
Proteggere l'accesso fisico agli asset critici con misure di controllo adeguate e documentate	Attuare un piano di formazione sulla sicurezza informatica per tutti i dipendenti	Monitorare continuamente gli asset per individuare anomalie	Adottare un piano di risposta agli incidenti

L'ADEMPIMENTO DELLE MISURE DI SICUREZZA DI BASE: LA NOTIFICA DEGLI INCIDENTI CYBER



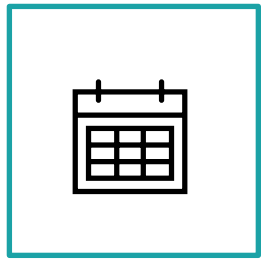
NOTIFICA → **OBBLIGATORIA**

NOTIFICA → **VOLONTARIA**



24h PRE-NOTIFICA
72h NOTIFICA INTEGRATIVA
1 mese RELAZIONE FINALE

https://www.acn.gov.it/portale/w/guida-alla-notifica-degli-incidenti-informatici



Decorrenza OBBLIGO di notifica di base: **GENNAIO 2026**

L'ADEMPIMENTO DELLE MISURE DI SICUREZZA DI BASE: LA NOTIFICA DEGLI INCIDENTI CYBER

Notifica OBBLIGATORIA

INCIDENTE (ART. 2 LETT. T D.LGS. 138/2024)

evento che **compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati** conservati, trasmessi o elaborati dai servizi offerti dai sistemi informativi e di rete o accessibili attraverso di essi

+

COMUNICAZIONE senza indebito ritardo alle terze parti coinvolte previa consultazione di CSIRT

SIGNIFICATIVO (ART. 25, CO. 4 D.LGS. 138/2024)

- **Grave perturbazione operativa dei servizi del soggetto interessato**
- **Perdite finanziarie** rilevanti per il soggetto segnalante (anche in conseguenza dell'irrogazione di una sanzione, ad es. dell'Autorità Garante o alla condanna al risarcimento del danno subito da terzi)
- **Impatto su terze parti** (persone fisiche / giuridiche) che possano subire o abbiano subito un danno materiale o immateriale

Notifica VOLONTARIA

Quasi-incidenti e incidenti relativi a reti, sistemi informativi e servizi informatici di propria pertinenza

L'ADEMPIMENTO DELLE MISURE DI SICUREZZA DI BASE: LA NOTIFICA DEGLI INCIDENTI CYBER

I. VALUTAZIONE INIZIALE DELL'INCIDENTE verificatosi rispetto, almeno, ai seguenti aspetti essenziali:

- **Sistemi informatici e di rete interessati** (impatto potenziale sulla continuità operativa)
- **Gravità e caratteristiche tecniche della minaccia informatica** (analisi delle vulnerabilità delle infrastrutture e sistemi aziendali – pericolosità della minaccia)
- **Durata dell'incidente**
- **Numero di utenti o sistemi coinvolti**
- **Esperienza pregressa in incidenti analoghi**

II. ATTIVAZIONE DEI CANALI DI COMUNICAZIONE INTERNI ED ESTERNI AUTORIZZATI

- Individuazione dei soggetti che all'interno dell'organizzazione aziendale sono **autorizzati a comunicare con CSIRT e Autorità competenti** in merito all'incidente verificatosi
- Definizione di **protocolli di comunicazione interna** (rivolta al personale) **ed esterna** (clienti, fornitori, partner, media)

LA SICUREZZA DELLA SUPPLY CHAIN

La NIS 2 pone una particolare attenzione alla **protezione della supply chain** (catena di approvvigionamento), riconoscendola come la vera vulnerabilità sistemica (Art. 24, comma 2, lettera d) Decreto NIS).

L'interruzione di un servizio critico da parte di un fornitore, anche piccolissimo, può mettere in crisi un operatore essenziale, con ripercussioni a cascata sull'intera catena di fornitura.

- I **soggetti essenziali e importanti** devono adottare misure che includano gli aspetti di sicurezza riguardanti i rapporti con i loro diretti fornitori o fornitori di servizi.
- Nel valutare l'adeguatezza delle misure, i soggetti devono considerare le vulnerabilità specifiche di ogni fornitore e la qualità complessiva dei prodotti e delle pratiche di sicurezza informatica dei propri fornitori, comprese le loro procedure di sviluppo sicuro.
- In altri termini, **ogni operatore ha l'obbligo di identificare e valutare, nella propria analisi dei rischi, anche le vulnerabilità dei propri fornitori**.

Grazie per l'attenzione!

Pirola
Pennuto
Zei
& Associati

studio di consulenza
tributaria e legale

Avv. Mario Valentini

mario.valentini@studiopirola.com

LinkedIn