GENNAIO

AVVERA

Società Benefit

NEWSLETTER 2026

AVVERA SRL SB

LA NOTIFICA DEGLI INCIDENTI NELLA DIRETTIVA NIS2 ALLA LUCE DELLE FAQ ACN: **PROFILI DI RESPONSABILITÀ, GOVERNANCE E IMPATTI ORGANIZZATIVI**

Con l'aggiornamento delle **FAQ pubblicate dall'Agenzia per la Cybersicurezza Nazionale (ACN)** in materia di **notifica degli incidenti significativi al CSIRT Italia**, il quadro applicativo della **Direttiva (UE) 2022/2555 (NIS2)** conosce un ulteriore momento di chiarificazione interpretativa.

L'intervento dell'Autorità assume particolare rilievo in quanto affronta una delle questioni più controverse nella prassi: **la relazione tra esternalizzazione dei servizi ICT e titolarità dell'obbligo di notifica**, chiarendo che tale obbligo **non è trasferibile mediante outsourcing.**

La NIS2 come disciplina di governance del rischio cyber

La Direttiva NIS2 si colloca in una prospettiva che supera la tradizionale impostazione tecnico-difensiva della sicurezza informatica, per adottare un modello fondato sulla **responsabilità organizzativa e sulla governance del rischio.**

L'obiettivo del legislatore europeo non è esclusivamente quello di prevenire o mitigare gli incidenti, ma di garantire che le entità essenziali e importanti siano in grado di:

- identificare tempestivamente eventi rilevanti;
- valutarne l'impatto;
- interagire in modo strutturato con le autorità competenti.
- In questo contesto, l'assetto contrattuale o tecnologico adottato dall'impresa non incide sulla titolarità degli obblighi,
- che restano in capo al soggetto qualificato come entità NIS.

Il principio di non delegabilità dell'obbligo di notifica

Le FAQ ACN ribadiscono un principio fondamentale per cui **l'obbligo di notifica degli incidenti significativi al CSIRT Italia permane in capo all'entità soggetta NIS2**, anche in presenza di:

- esternalizzazione della gestione infrastrutturale;
- affidamento del monitoraggio a SOC o MSSP;
- utilizzo di servizi cloud.
- Il fornitore può essere coinvolto nella fase di rilevazione e gestione tecnica dell'incidente, ma **non assume automaticamente la posizione giuridica del soggetto obbligato alla notifica.**

Tale impostazione è coerente con la logica di accountability che permea l'intero impianto della Direttiva.

Incidente riconducibile ai sistemi del cliente

Nel caso in cui l'incidente riguardi i sistemi del cliente soggetto NIS2, l'obbligo di notifica è **integralmente in capo al cliente**, indipendentemente dal supporto tecnico fornito da terzi.

L'eventuale coinvolgimento del fornitore non incide sulla titolarità dell'obbligo, ma esclusivamente sulle modalità operative di gestione dell'evento.

Incidente originato dal fornitore con impatto sul cliente

Qualora l'incidente abbia origine presso il fornitore e produca effetti sui servizi erogati al cliente soggetto NIS2, si configura uno scenario più complesso.
In tali casi:

- il fornitore soggetto NIS può essere tenuto a notificare l'incidente;
- il cliente deve autonomamente valutare se l'impatto subito integri i presupposti per una **propria notifica.**

Il profilo critico non risiede tanto nella possibile duplicazione delle notifiche, quanto nel rischio di disallineamento informativo, sintomatico di una governance inadeguata della relazione contrattuale.

Servizi cloud e modelli di controllo

Nel contesto dei servizi cloud, le FAQ ACN chiariscono che il criterio dirimente non è la qualificazione formale del servizio, bensì il **grado di controllo effettivo esercitato sulle risorse.**
Nei modelli in cui il cliente mantiene il controllo delle risorse (ad esempio IaaS), l'obbligo di notifica resta in capo a quest'ultimo.
In altri modelli, può configurarsi un obbligo concorrente, da valutare caso per caso.

La figura del Referente CSIRT quale strumento di governance operativa

Un ulteriore elemento di rilievo è rappresentato dalla valorizzazione della figura del **Referente CSIRT**, incaricato di:

- interfacciarsi operativamente con il CSIRT Italia;
- trasmettere le notifiche di incidente;
- gestire il flusso informativo durante l'evento.

Il Referente CSIRT può essere interno o esterno all'organizzazione, ma la sua nomina **non determina un trasferimento della responsabilità giuridica**, che resta in capo all'entità NIS.
Si tratta, dunque, di un presidio organizzativo e non di una delega sostanziale.

Implicazioni organizzative e contrattuali per le imprese

I chiarimenti ACN evidenziano come la compliance NIS2 non possa essere ridotta alla disponibilità di strumenti tecnologici o fornitori qualificati.

È necessario predisporre:

- processi decisionali interni strutturati;
- ruoli chiaramente definiti;
- meccanismi di valutazione tempestiva della significatività degli incidenti.

Nella gestione del rischio NIS2, un ruolo centrale è assunto dai contratti con i fornitori. In assenza di clausole che regolino elementi quali obblighi di segnalazione, tempistiche di comunicazione o cooperazione informativa, l'impresa rischia di non essere in grado di adempiere correttamente agli obblighi di notifica, pur non essendo responsabile dell'evento sotto il profilo tecnico.

Il principale rischio per le imprese non è esclusivamente quello sanzionatorio, ma quello di **non riuscire a dimostrare un adeguato livello di controllo e coordinamento** in sede di verifica da parte dell'Autorità competente.

Considerazioni conclusive

L'aggiornamento delle FAQ ACN contribuisce a chiarire un aspetto centrale dell'impianto NIS2:
la sicurezza informatica è una funzione di governo del rischio e non un'attività delegabile integralmente a terzi.

La gestione e la notifica degli incidenti diventano così un indicatore di **maturità organizzativa**, misurabile in termini di:
chiarezza dei ruoli;

- integrazione tra funzioni tecniche, legali e di compliance;
- capacità di controllo della supply chain digitale.

In tale prospettiva, la compliance NIS2 si configura non come un adempimento formale, ma come componente strutturale della resilienza organizzativa dell'impresa.

AVVERA | SB Società Benefit

IL CASO CLOUDFLARE–AGCOM: QUANDO L'ENFORCEMENT ANTIPIRATERIA ENTRA IN COLLISIONE CON L'ARCHITETTURA DI INTERNET

La sanzione da 14 milioni di euro inflitta dall'AGCOM a Cloudflare per la mancata ottemperanza agli ordini impartiti tramite la piattaforma Piracy Shield segna un punto di non ritorno nel rapporto tra regolazione nazionale, infrastrutture globali della rete e diritto europeo del digitale. Non si tratta più soltanto di una controversia in materia di diritto d'autore: il "caso Cloudflare" è ormai un banco di prova per la tenuta giuridica, tecnica e politica dell'enforcement amministrativo nell'era delle grandi piattaforme infrastrutturali.

Una sanzione formalmente legittima, ma sistemicamente problematica

Dal punto di vista strettamente formale, la posizione dell'Autorità appare difficilmente contestabile: AGCOM ha applicato una legge dello Stato (la l. 93/2023, cd. "legge antipezzotto") approvata all'unanimità dal Parlamento, che ha esteso gli obblighi di cooperazione antipirateria non solo agli access provider, ma anche ai fornitori di CDN e DNS. In questo quadro, l'inottemperanza reiterata di Cloudflare agli ordini di blocco veicolati tramite Piracy Shield integra, secondo l'Autorità, un illecito sanzionabile.

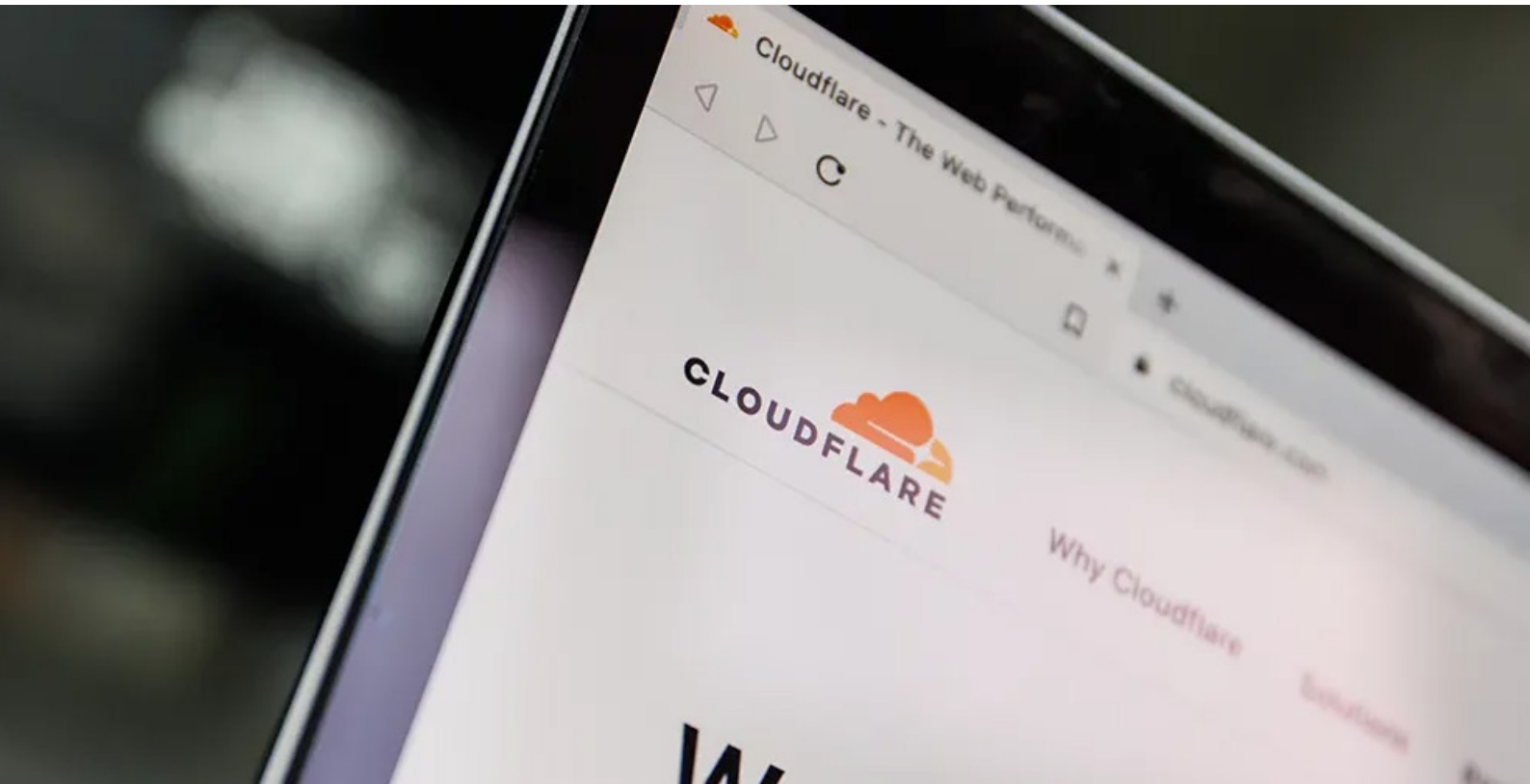
Tuttavia **la legittimità formale non esaurisce il problema.** La vera questione è se il meccanismo imposto **sia compatibile con il funzionamento tecnico di Internet**, con i principi di proporzionalità e con il diritto europeo dei servizi digitali.

Piracy Shield e il "peccato originale" dell'overblocking

Piracy Shield nasce con una finalità condivisibile – il contrasto alla pirateria, in particolare quella sportiva in tempo reale – ma sconta un vizio strutturale: è costruito come se Internet fosse una rete di risorse isolate, quando invece è un ecosistema basato su **indirizzamenti condivisi, IP dinamici, reverse proxy e infrastrutture multilivello.**

Il blocco di IP associati a CDN globali come Cloudflare comporta inevitabilmente effetti collaterali: l'oscuramento di servizi perfettamente leciti, l'assenza di notifiche agli interessati, l'impossibilità di un rimedio tempestivo. Episodi di overblocking si sono già verificati e non sono incidenti di percorso, ma conseguenze fisiologiche del modello adottato.

In questo senso, i numeri spesso richiamati a sostegno dell'efficacia dello strumento – decine di migliaia di domini e indirizzi IP bloccati – dicono poco o nulla sull'effettiva riduzione della pirateria. La logica del "morto un dominio se ne fa un altro" rende il sistema una rincorsa permanente, con costi crescenti per la rete e benefici tutti da dimostrare.



Cloudflare non è un hosting provider (e questo conta)

Uno degli equivoci che alimentano il dibattito pubblico riguarda la natura stessa di Cloudflare. L'azienda **non ospita contenuti**, non seleziona né promuove opere pirata. Fornisce servizi di sicurezza, CDN e DNS che, per loro natura, sono **agnostici rispetto ai contenuti** e utilizzati indistintamente da milioni di siti leciti e illeciti.

È vero che queste tecnologie possono essere sfruttate anche da soggetti criminali – come qualsiasi infrastruttura neutrale – ma questo non trasforma il fornitore in un corresponsabile automatico. Il diritto europeo ha sempre costruito la responsabilità degli intermediari su un delicato equilibrio tra cooperazione e neutralità, equilibrio che il DSA ha cercato di rafforzare, non di demolire.

Il paradosso europeo: sarà il DSA a salvare Cloudflare?

Qui emerge il paradosso più interessante dell'intera vicenda. La difesa più solida di Cloudflare potrebbe non venire dal diritto statunitense o da argomenti geopolitici, bensì proprio dal **Digital Services Act**: obblighi graduati, divieto di obblighi generali di sorveglianza, necessità di misure mirate, proporzionate e territorialmente limitate.

Non è un caso che a Bruxelles siano state sollevate perplessità sul funzionamento di Piracy Shield, né che la Commissione europea abbia richiamato l'Italia alla necessità di garantire coerenza con il quadro DSA. Ed è quantomeno singolare che l'autorità chiamata a vigilare sull'applicazione del DSA sia la stessa che gestisce uno strumento potenzialmente in tensione con esso.

Gli errori di Cloudflare: quando la difesa diventa ricatto

Se Piracy Shield presenta gravi criticità, la reazione di Cloudflare non è stata giuridicamente irreprensibile. Minacciare il ritiro di servizi essenziali, evocare la sicurezza delle Olimpiadi di Milano-Cortina, trasformare una controversia regolatoria in un caso diplomatico via X è una strategia comunicativa che indebolisce, anziché rafforzare, le ragioni dell'azienda.

L'uso di infrastrutture critiche come leva negoziale alimenta un altro timore: quello di una **privatizzazione del potere infrastrutturale**, in cui grandi operatori globali possono condizionare decisioni sovrane semplicemente "staccando la spina". È un rischio che nessuno Stato può ignorare.

Oltre Cloudflare: una questione di sovranità digitale (vera)

Il caso Cloudflare non riguarda solo la pirateria, né solo una singola azienda. Riguarda la **dipendenza strutturale dell'Europa da infrastrutture extra-UE**, l'assenza di alternative realistiche nel breve periodo e la difficoltà di conciliare enforcement rapido con garanzie giuridiche adeguate.

Difendere il diritto d'autore è sacrosanto. Farlo con strumenti tecnicamente inadeguati e giuridicamente fragili rischia però di produrre l'effetto opposto: indebolire la credibilità delle istituzioni, esporre il Paese a contenziosi europei e spingere gli operatori verso una logica di scontro anziché di cooperazione.

Conclusione

La sanzione a Cloudflare è formalmente legittima, ma il caso dimostra che l'attuale perimetro normativo dell'enforcement antipirateria **è tecnicamente e sistemicamente inadeguato.** La tutela del diritto d'autore non può tradursi in strumenti che ignorano l'architettura di Internet o che producono effetti sproporzionati e indiscriminati.

Una soluzione praticabile esiste ed è già stata adottata da Google, che ha applicato i blocchi richiesti da Piracy Shield **su base esclusivamente territoriale**, limitandoli agli utenti italiani e preservando il funzionamento globale dei propri servizi. È un modello imperfetto, ma coerente con i principi di proporzionalità, territorialità e con il Digital Services Act.

Cloudflare ha colto i limiti strutturali dello strumento, ma ha scelto una strategia comunicativa che indebolisce le sue ragioni, evocando ritorsioni e mettendo sul tavolo infrastrutture critiche. La sovranità digitale non si costruisce né con piattaforme tecnicamente fragili né con bracci di ferro tra Stati e big tech.

Se il caso Cloudflare porterà a una revisione di Piracy Shield alla luce del modello "territoriale" e del quadro europeo, potrà rappresentare un'occasione di maturazione normativa. In caso contrario, rischia di aprire una stagione di conflitti giuridici e sistemici che l'ecosistema digitale europeo non può permettersi.

AVVERA | SB Società Benefit

CHATGPT SALUTE E AI ACT: IL CONFINE SOTTILE TRA SUPPORTO INFORMATIVO E RISCHIO SISTEMICO

L'annuncio di *ChatGPT* Salute rappresenta uno spartiacque nel rapporto tra intelligenza artificiale general purpose e sanità. Non tanto per le funzionalità dichiarate — chiarimenti su sintomi, referti, stili di vita — quanto per il fatto che, per la prima volta, un modello di IA generalista entra in modo strutturato e continuativo nel trattamento di dati sanitari, assumendo un ruolo che, di fatto, incide sui processi decisionali dell'utente in materia di salute.

Dal punto di vista del diritto europeo dell'intelligenza artificiale, il nodo centrale non è ciò che OpenAI dichiara di fare, ma ciò che il sistema è concretamente idoneo a fare e l'impatto prevedibile sul comportamento degli utenti. Ed è proprio qui che l'AI Act offre una chiave di lettura particolarmente rigorosa.

Qualificazione del sistema: non basta negare la diagnosi

OpenAI insiste nel qualificare ChatGPT Salute come strumento informativo e non medico. Tuttavia, ai sensi dell'AI Act, la qualificazione giuridica di un sistema non dipende dall'etichetta attribuita dal fornitore, bensì dalla **finalità d'uso ragionevolmente prevedibile** (art. 3 e considerando).

Un sistema che:

- analizza sintomi,
- interpreta referti,
- suggerisce correlazioni tra valori clinici e patologie,
- dialoga in modo iterativo affinando le risposte,

opera in un'area di **influenza significativa sulle decisioni sanitarie individuali**, anche in assenza di una diagnosi formale.

In questo senso, ChatGPT Salute si colloca pericolosamente vicino ai sistemi di IA destinati a essere utilizzati in ambito sanitario, che l'AI Act qualifica come **high-risk** quando incidono su diagnosi, prevenzione o trattamento.

Il rischio giuridico è evidente: una piattaforma che, nella pratica, orienta le scelte dell'utente in materia di salute potrebbe rientrare nella disciplina dei sistemi ad alto rischio, con conseguente obbligo di:

- gestione del rischio,
- qualità dei dati,
- documentazione tecnica,
- supervisione umana effettiva,
- tracciabilità e accountability.

AI general purpose e sanità: un'accoppiata critica

ChatGPT è, per definizione, un **General Purpose AI (GPAI).** L'AI Act introduce obblighi specifici per i modelli GPAI, rafforzati ulteriormente quando essi presentano **rischi sistemici.**

L'uso strutturato di un GPAI su dati sanitari amplifica tali rischi:

- **allucinazioni** in ambito medico non sono un semplice bug, ma un potenziale danno alla persona;
- la **probabilisticità** del modello entra in tensione con il principio di affidabilità richiesto in sanità;
- **l'asimmetria** informativa tra utente e fornitore rende il consenso e la consapevolezza particolarmente fragili.

Non a caso, l'AI Act dedica una tutela rafforzata agli ambiti che incidono su diritti fondamentali, tra cui la salute. La scelta di escludere (almeno per ora) il mercato europeo non appare quindi prudenziale, ma quasi obbligata.

Il cortocircuito con il GDPR: dati di salute e fiducia tecnologica

Sul piano della protezione dei dati, il servizio tocca il cuore del GDPR: **i dati relativi alla salute**, categoria particolarmente protetta ex art. 9 del Regolamento UE 2016/679.

Le rassicurazioni di OpenAI — crittografia, separazione delle chat, esclusione dall'addestramento — pongono un problema tipicamente europeo: **la verificabilità**. La compliance non può basarsi sulla fiducia, ma su:

- accountability dimostrabile,
- auditabilità,
- controlli indipendenti.

In assenza di questi presidi, l'accesso a cartelle cliniche elettroniche da parte di un soggetto extra-UE solleva interrogativi seri anche in tema di trasferimenti internazionali di dati e sovranità digitale sanitaria.

Responsabilità: il grande assente

Forse il punto più critico, anche alla luce dell'AI Act e delle future norme sulla responsabilità da IA, è la **dissociazione tra influenza e responsabilità.**

ChatGPT Salute:

- incide sulle decisioni dell'utente,
- analizza dati sanitari,
- interagisce in modo personalizzato,

ma OpenAI esclude qualsiasi qualificazione come dispositivo medico e, di conseguenza, ogni responsabilità clinica.

Il confronto con la sperimentazione statunitense di Doctronic è illuminante: lì l'IA prescrive, ma è assicurata come un medico. Qui l'IA orienta, ma senza assumere alcun rischio giuridico. È esattamente questo squilibrio che il legislatore europeo tenta di correggere con l'AI Act: **chi trae valore dall'IA deve anche assumerne i rischi.**

Perché l'Europa frena (e probabilmente continuerà a farlo)

ChatGPT Salute mostra in modo plastico la distanza tra l'approccio statunitense — innovation first — e quello europeo — fundamental rights by design.

Nel contesto UE, un sistema simile difficilmente potrebbe operare senza:

- una chiara qualificazione giuridica,
- un inquadramento come high-risk AI,
- un'integrazione con il diritto sanitario e dei dispositivi medici,
- una responsabilità definita lungo tutta la filiera.

Non è un rifiuto dell'innovazione, ma una richiesta di **governance**.

Conclusione

ChatGPT Salute non vuole "sostituirsi al medico". Ma il diritto europeo non guarda alle intenzioni: guarda agli effetti. E quando un sistema di IA entra nella sfera più intima e vulnerabile della persona — la salute — non può restare in una zona grigia normativa.

L'AI Act nasce proprio per evitare che l'innovazione più potente si sviluppi dove la responsabilità è più debole. La sanità è il banco di prova. E ChatGPT Salute, più che una promessa tecnologica, è oggi un caso di studio giuridico perfetto.

AVVERA | SB Società Benefit

LE NUOVE SPECIFICHE ACN NIS2: **DALLA NORMA EUROPEA ALL'OBBLIGO OPERATIVO**

Con la determinazione n. 379907 del 2025, l'Agenzia per la Cybersicurezza Nazionale (ACN) ha aggiornato le specifiche di base per l'attuazione della Direttiva NIS2 in Italia. Non si tratta di un atto meramente interpretativo, ma di un passaggio operativo chiave: le specifiche ACN traducono gli obblighi astratti della direttiva europea in requisiti concreti, misurabili e verificabili per i soggetti essenziali e importanti.

L'entrata in vigore della determinazione è fissata al **15 gennaio 2026.** Da quel momento, per le organizzazioni rientranti nel perimetro NIS2, la cybersecurity non è più una materia "di principio", ma un insieme di adempimenti tecnici, organizzativi e procedurali che devono essere dimostrabili, documentati e sostenuti da una governance chiara.

Perché le specifiche di base cambiano il perimetro della compliance cyber

La Direttiva NIS2 nasce per rispondere a un dato strutturale: la crescente interdipendenza digitale tra settori critici, filiere produttive e servizi essenziali rende la sicurezza informatica un tema di interesse pubblico e di stabilità economica. In questo contesto, l'approccio europeo è esplicitamente risk-based, ma accompagnato da un rafforzamento significativo dell'accountability.

Le specifiche di base si inseriscono in questa cornice e svolgono una funzione precisa: **ridurre l'ambiguità**. Per le imprese – in particolare per le PMI che entrano per la prima volta nel perimetro NIS – questo significa passare da un "obbligo di protezione" generico a un set di misure minime che l'Autorità si aspetta di trovare implementate e descritte in sede di controllo.

Il principio in gioco non è solo la sicurezza, ma la **compliance come capacità organizzativa**: dimostrare di aver identificato i rischi cyber, di aver adottato misure proporzionate e di saper reagire agli incidenti in modo strutturato.

Accountability cyber: la sicurezza entra stabilmente nella governance aziendale

Le specifiche ACN si concentrano su alcuni assi fondamentali, che meritano una lettura integrata.

Governance e responsabilità

Il primo elemento di discontinuità riguarda la governance. La NIS2 – e le specifiche di base lo rendono esplicito – attribuisce ai vertici aziendali una responsabilità diretta in materia di cybersicurezza. Non è sufficiente delegare integralmente al reparto IT o al CISO: il management deve approvare le misure, allocare risorse e ricevere formazione adeguata.

Questo approccio è coerente con il modello già noto nel GDPR: accountability come capacità di governo, non come mero adempimento formale.

Gestione del rischio

Le organizzazioni devono adottare un processo strutturato di risk management, che includa:

identificazione dei rischi per reti e sistemi informativi;
valutazione dell'impatto su continuità operativa e servizi;
adozione di misure tecniche e organizzative adeguate.
Le specifiche non impongono uno standard unico, ma rendono evidente che modelli improvvisati o non documentati non sono più accettabili.

Incident menagement e notifiche

Altro punto centrale è la gestione degli incidenti. Le organizzazioni devono disporre di procedure chiare per:

- rilevare eventi significativi;
- valutarne la gravità;
- notificare tempestivamente l'incidente ad ACN secondo le tempistiche previste.
- Qui il rischio non è solo tecnico, ma anche organizzativo: senza processi interni definiti, la probabilità di errori o ritardi nella notifica aumenta sensibilmente.

La compliance NIS2 come processo continuo, non come adempimento isolato

Per le imprese e le PMI soggette a NIS2, le nuove specifiche ACN producono tre implicazioni immediate.

1. Fine dell'approccio "one-shot"

La compliance NIS2 non è un progetto da chiudere una tantum. È un processo continuo, che richiede aggiornamenti periodici, monitoraggio e revisione delle misure. Chi affronta l'adeguamento come un mero esercizio documentale rischia di trovarsi scoperto al primo audit.

2. Necessità di una roadmap operativa

In termini pratici, una roadmap minima dovrebbe includere:

- mappatura del perimetro NIS2 e dei sistemi critici;
- gap analysis rispetto alle specifiche ACN;
- definizione di policy e procedure (quali gestione dell'incidente, business continuity, gestione degli accessi);
- formazione del management e del personale chiave;
- test periodici e aggiornamento della documentazione.
- Questo approccio è particolarmente rilevante per le PMI, che spesso non dispongono di strutture interne dedicate alla cybersecurity.

3. Rischio sanzionatorio e reputazionale

La NIS2 introduce un regime sanzionatorio significativo, ma il rischio non è solo economico. Un incidente gestito male – o una non conformità evidente – può avere un impatto reputazionale rilevante, soprattutto nei rapporti con clienti, partner e pubbliche amministrazioni.

Essere audit-ready diventa, quindi, un obiettivo strategico.

NIS2 come leva strategica: dalla cybersecurity difensiva alla resilienza organizzativa

L'aggiornamento delle specifiche di base ACN segna un passaggio di maturità per l'ecosistema italiano della cybersecurity. La NIS2 non chiede alle imprese di essere invulnerabili, ma di essere **governate**: consapevoli dei propri rischi, organizzate nella risposta, responsabili nelle decisioni.

Per le imprese – e in particolare per le PMI – la vera sfida non è tecnica, ma culturale. Integrare la cybersecurity nella governance aziendale significa trasformare la compliance da costo percepito a **leva di affidabilità e competitività.**

In questo senso, la NIS2 non è solo un obbligo normativo. È un imperativo strategico: chi investe oggi in processi, competenze e governance sarà domani più resiliente, più credibile e, in ultima analisi, più solido sul mercato.

AVVERA | SB Società Benefit

NIS 2 E AUTENTICITÀ: **IL QUARTO PILASTRO SILENZIOSO DELLA CYBERSECURITY EUROPEA**

La Direttiva **NIS 2** segna un passaggio silenzioso ma strutturale nel modo in cui l'Unione europea concepisce la cybersecurity. Non si limita a rafforzare obblighi già noti o ad ampliare il perimetro dei soggetti coinvolti: introduce, in modo esplicito, un cambio di paradigma.
Accanto alla tradizionale triade della sicurezza delle informazioni – **riservatezza, integrità e disponibilità** – emerge un quarto elemento critico: **l'autenticità**.

La compromissione dell'autenticità non è più un effetto collaterale di un incidente, ma una delle sue forme tipiche. Ciò significa che, non è sufficiente che un sistema "funzioni" o che i dati non vengano alterati: è essenziale poter dimostrare che **utenti, dispositivi, comunicazioni e informazioni siano ciò che dichiarano di essere.**

Perché la fiducia digitale è diventata un requisito di governance

La scelta del legislatore europeo non è casuale. Le principali minacce cyber oggi non puntano solo a bloccare servizi o sottrarre dati, ma a **falsificare identità, fonti e processi decisionali.** Phishing avanzato, business email compromise, supply chain attack e deepfake operativi hanno tutti un denominatore comune: l'attacco alla fiducia.

In questo contesto, la NIS 2 si inserisce in una strategia più ampia di rafforzamento della **resilienza digitale europea**, in continuità con GDPR, eIDAS e con gli standard di sicurezza come **ISO/IEC 27001.** L'autenticità diventa così un **principio di governance**, prima ancora che una misura tecnica, perché incide direttamente sull'accountability dell'organizzazione e sulla sua capacità di dimostrare la conformità.

Autenticità: da concetto tecnico a requisito normativo

Secondo la definizione ISO/IEC, l'autenticità è la proprietà per cui un'entità è realmente ciò che afferma di essere. La NIS 2 recepisce questa nozione e la traduce in termini giuridici, includendo la **perdita di autenticità** tra gli impatti rilevanti di un incidente di cybersecurity.
Questo significa che:

- un accesso non autorizzato ottenuto tramite credenziali legittime compromesse;
- una comunicazione apparentemente valida ma proveniente da una fonte falsificata;
- un dato tecnicamente integro ma attribuito a un soggetto errato

possono costituire, a tutti gli effetti, un incidente rilevante ai fini NIS 2.

Il collegamento con gli obblighi di gestione del rischio

L'articolo 21 della Direttiva impone ai soggetti NIS 2 l'adozione di **misure tecniche, operative e organizzative adeguate e proporzionate.** Molte di queste, se lette in chiave sistemica, sono direttamente funzionali alla tutela dell'autenticità:

politiche di controllo degli accessi;
gestione delle identità e delle credenziali;
uso della crittografia e dei servizi fiduciari;
sicurezza della supply chain digitale;
formazione del personale.
L'autenticità non è quindi una misura isolata, ma il risultato di un **ecosistema di controlli** coerenti e governati.

Il rischio principale: una compliance solo formale

Il rischio più elevato per le organizzazioni non è tanto l'assenza di singole misure tecniche, quanto la **mancanza di un disegno di governance**. Implementare MFA o firme digitali senza una chiara attribuzione di ruoli, responsabilità e processi decisionali espone a due criticità:

inefficacia reale delle misure;
incapacità di dimostrare la conformità in caso di audit o incidente.
La NIS 2 richiede soggetti **audit-ready**, non semplicemente "dotati di strumenti".

AVVERA | SB Società Benefit

Guida operativa: come integrare l'autenticità nella governance NIS 2

Mappare identità e asset critici
Identificare utenti, sistemi, dispositivi e fornitori che accedono a funzioni o dati critici.
Classificare quali identità devono essere considerate "ad alto impatto" in caso di compromissione.
Rafforzare l'autenticazione in modo proporzionato
Implementare autenticazione forte (MFA) per ruoli critici.
Adottare certificati digitali e meccanismi PKI per sistemi e comunicazioni machine-to-machine.
Integrare servizi fiduciari qualificati
Utilizzare firme elettroniche e sigilli per garantire l'origine e l'integrità dei documenti rilevanti.
Valutare l'allineamento con il quadro eIDAS, soprattutto per processi transfrontalieri.
Governare la supply chain digitale
Verificare l'autenticità di software, aggiornamenti e componenti.
Inserire requisiti di autenticazione e tracciabilità nei contratti con i fornitori critici.
Documentare per dimostrare
Formalizzare policy, procedure e ruoli.
Collegare le misure di autenticità alla valutazione del rischio e al piano di gestione degli incidenti.
Garantire coerenza con il sistema di gestione della sicurezza delle informazioni (ISO/IEC 27001).

Autenticità come leva strategica: dalla cybersecurity alla fiducia dimostrabile

La Direttiva NIS 2 chiarisce un punto spesso sottovalutato: **la cybersecurity è prima di tutto una questione di fiducia strutturata.** L'autenticità diventa il perno su cui ruotano sicurezza tecnica, responsabilità legale e continuità operativa.

Per le organizzazioni, l'imperativo strategico è evidente: passare da una cybersecurity "difensiva" a una **cyber governance dimostrabile**, in cui ogni identità, ogni accesso e ogni informazione siano verificabili e tracciabili.
In questo scenario, la compliance non è un costo, ma una l**eva di resilienza e credibilità** nel mercato digitale europeo.

GMAIL NELL'ERA GEMINI: **L'EMAIL DIVENTA UN INTERMEDIARIO COGNITIVO**

L'ingresso di Gemini in Gmail segna un passaggio che va ben oltre l'aggiornamento di una piattaforma. Google non sta semplicemente arricchendo la posta elettronica di nuove funzioni basate sull'intelligenza artificiale: sta ridefinendo la natura stessa dell'email, trasformandola in un ambiente assistito, capace di leggere, sintetizzare, organizzare e suggerire azioni.

L'obiettivo dichiarato è ridurre il carico cognitivo dell'utente, aiutandolo a orientarsi in un flusso comunicativo sempre più denso. Dal punto di vista dell'efficienza, il risultato appare convincente.

Dal punto di vista giuridico e culturale, il cambiamento è molto più profondo: l'accesso sistematico al contenuto delle email. Non solo ai metadati, ma alle conversazioni, al contesto, alla storia delle relazioni. È qui che la trasformazione tecnologica si intreccia con temi centrali come privacy, controllo e fiducia.

Dalla funzione all'infrastruttura

Uno degli aspetti più significativi dell'integrazione di Gemini è che l'intelligenza artificiale non si presenta come una funzione opzionale. È progettata come livello infrastrutturale del servizio. L'AI Inbox non affianca l'esperienza tradizionale: tende a sostituirla, diventando il nuovo standard.

Questo spostamento ha effetti diretti sul modo in cui si configura il consenso.
Quando l'IA diventa condizione di funzionamento dell'esperienza "migliorata", la scelta dell'utente non è più se attivare o meno una singola funzione, ma se accettare un modello di servizio fondato sull'analisi continua dei contenuti, oppure rinunciare a parte dell'efficienza promessa.

In questo scenario, il consenso rischia di perdere la sua dimensione decisionale per assumere quella di presupposto implicito dell'esperienza digitale.

L'esperienza utente come architettura della scelta

Dal punto di vista della user experience, l'integrazione di Gemini è costruita per essere fluida, poco visibile, quasi naturale. Le funzionalità sono spesso attive di default o fortemente incentivate, mentre le opzioni di limitazione o disattivazione risultano meno evidenti e, in alcuni casi, penalizzanti sul piano funzionale.

Non si tratta di una scelta neutra.
È l'espressione di un design che orienta il comportamento, riducendo la frizione decisionale e rendendo l'adozione dell'IA la via più semplice, se non l'unica realmente praticabile.

L'utente non viene messo nella condizione di interrogarsi se delegare o meno all'intelligenza artificiale la lettura delle proprie email, ma solo di adattarsi a un livello di delega già incorporato nel servizio.

Privacy, fiducia e asimmetria informativa

La questione non riguarda esclusivamente la privacy intesa come conformità normativa. In gioco c'è qualcosa di più ampio: il rapporto di fiducia tra utente e piattaforma.

L'email è storicamente percepita come uno spazio semi-privato, un contenitore di comunicazioni personali, professionali e spesso sensibili. Trasformarla in un ambiente di analisi cognitiva permanente significa ridefinire, anche implicitamente, questa percezione.

Le rassicurazioni fornite dal fornitore — sull'uso dei dati, sull'assenza di lettura umana, sui limiti dichiarati del trattamento — sono elementi rilevanti, ma non eliminano l'asimmetria informativa strutturale tra chi progetta il sistema e chi lo utilizza.
L'utente non ha una reale visibilità sulle logiche dei modelli, sull'estensione concreta del trattamento, né sulle interazioni tra i diversi livelli dell'ecosistema.

Questo squilibrio rende difficile una valutazione pienamente consapevole del compromesso che si sta accettando.

Oltre l'utilità: una questione di governance

La questione non è se Gmail potenziato da Gemini sia utile. La questione è un'altra, più sottile e più strutturale: quanto controllo effettivo resta all'utente su come e fino a che punto delegare?
E quanto questa delega è il risultato di una scelta consapevole, piuttosto che di un'architettura dell'esperienza che la rende progressivamente inevitabile?

Siamo probabilmente all'inizio di una fase nuova dell'evoluzione digitale, che non riguarda più soltanto l'automazione dei compiti, ma la delega cognitiva: sistemi che filtrano, interpretano e organizzano le informazioni prima ancora che l'utente le incontri.

Conclusione: la privacy come scelta di progetto

In questo contesto, la privacy non può essere ridotta a un requisito formale o a un vincolo da gestire a valle. È una scelta di progettazione e di governance, che dovrebbe riflettersi direttamente nell'esperienza dell'utente.

L'innovazione davvero sostenibile non è quella che elimina ogni frizione, ma quella che rende le scelte esplicite, comprensibili e negoziabili.

E l'esperienza digitale più evoluta non sarà quella che rende l'intelligenza artificiale invisibile,
ma quella che consente alle persone di capirla, governarla e decidere consapevolmente quanto spazio concederle.

AVVERA

Società Benefit

SEDE LEGALE E OPERATIVA
20146 MILANO
VIA SARDEGNA, 21

SEDE OPERATIVA CERTIFICATA
21040 ORIGGIO (VA)
LARGO UMBERTO BOCCIONI, 1

ALTRE SEDI
61211 PESARO (PU)
VIA GIASONE DEL MAINO, 13
33100 UDINE (UD)
VIA G. TULLIO, 22

TELEFONO
+39 0296515401

FAX
0296515499

C.F./P.IVA 06047090961
CAP. SOC. 300.000 EURO I.V.
REG. IMPO. MI
06047090961
REA 1866500

WWW.AVVERA.IT
AVVERA@LEGALMAIL.IT

IMQ CERTIFIED
QUALITY MANAGEMENT SYSTEM
ISO 9001:2015

IMQ CERTIFIED
INFORMATION SECURITY MANAGEMENT SYSTEM
ISO/IEC 27001:2022

IMQ CERTIFIED
OCCUPATIONAL HEALTH AND SAFETY MANAGEMENT SYSTEM
ISO 45001:2018