Tutela della privacy e cybersecurity
Indicazioni operative per gli enti locali

A domanda risponde Avv. Michele IASELLI

23 Settembre 2021 - dalle ore 15:00 alle 17:00

ASMEL - Associazione per la Sussidiarietà e la Modernizzazione
degli Enti Locali
Email info@dpoinrete.it
Numero Verde 800.16.56.54 (int.3)
Web: www.dpoinrete.it
www.asmel.eu

Quadro normativo

Il tema della sicurezza informatica riveste un’importanza fondamentale perché necessaria per garantire la disponibilità, l'integrità e la riservatezza delle informazioni del Sistema informativo.
Un’area tecnologica in continua evoluzione, quasi giornaliera, nella quale gli investimenti devono essere rafforzati in continuazione tenendo conto anche dei principi di privacy previsti dall’ordinamento giuridico.

Negli ultimi anni il numero complessivo di attacchi e di incidenti legati alla sicurezza informatica, specialmente nella PA, è aumentato in modo esponenziale. Tutti gli studi e le ricerche che analizzano e studiano questi fenomeni sono concordi nell'affermare una preoccupante tendenza alla crescita.

Le pubbliche amministrazioni, dal punto di vista sicurezza, possono essere considerate come organizzazioni fortemente regolate, in considerazione del fatto che la loro attività si svolge nell'ambito e nei limiti di norme che hanno valore di legge. Il problema è che fino a poco tempo fa erano state poche le norme giuridiche che si erano occupate di cyber security.

In effetti le norme di maggiore rilevanza sono quelle contenute nel Codice dell'Amministrazione Digitale (CAD - D.Lgs. 7 marzo 2005 s.m.i.), che all'art. 17 al fine di garantire l'attuazione delle linee strategiche per la riorganizzazione e digitalizzazione dell'amministrazione definite dal Governo, prevede che le pubbliche amministrazioni individuino mediante propri atti organizzativi, un unico ufficio dirigenziale generale responsabile della transizione digitale.

Questo Ufficio sostituisce il Centro di competenza previsto dalla normativa previgente e il responsabile dei sistemi informativi automatizzati di cui all'articolo 10 del decreto legislativo 12 febbraio 1993, n. 39. Inoltre alla luce delle recenti riforme del CAD lo stesso ufficio deve assicurare la transizione alla modalità operativa digitale e i conseguenti processi di riorganizzazione finalizzati alla realizzazione di un'amministrazione digitale e aperta, di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità.

Naturalmente anche l'Agenzia per l'Italia Digitale (AgID) deve assicurare il coordinamento delle iniziative nell’ambito delle attività di indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica con particolare riferimento al Sistema Pubblico di Connettività.

In materia, difatti, occorrono ulteriori regole tecniche che in coerenza con la disciplina in materia di tutela della privacy introducano elementi utili per riconoscere l'esattezza, la disponibilità, l'integrità e per verificare l'accessibilità e la riservatezza dei dati.

Proprio per questi motivi è stata pubblicata sulla G.U. (Serie Generale n. 79 del 04/04/2017) la **Circolare AgID del 17 marzo 2017 n. 1/2017** contenente le "Misure minime di sicurezza ICT per le pubbliche amministrazioni" successivamente sostituita dalla circolare n. 2/2017 del 18 aprile 2017.

Le stesse misure sono parte integrante del più ampio disegno delle Regole Tecniche per la sicurezza informatica della Pubblica Amministrazione, emesso come previsto dal Piano Triennale per l'Informatica nella PA e dalla **Direttiva 1 agosto 2015** del Presidente del Consiglio dei Ministri, che assegna all'Agenzia per l'Italia Digitale il compito di sviluppare gli standard di riferimento per le amministrazioni.

Tale Direttiva in considerazione dell'esigenza di consolidare un sistema di reazione efficiente, che raccordi le capacità di risposta delle singole Amministrazioni, a fronte di eventi quali incidenti o azioni ostili che possono compromettere il funzionamento dei sistemi e degli assetti fisici controllati dagli stessi, sollecita tutte le Amministrazioni e gli Organi chiamati ad intervenire nell'ambito degli assetti nazionali di reazione ad eventi cibernetici a dotarsi, secondo una tempistica definita e comunque nel più breve tempo possibile, di standard minimi di prevenzione e reazione ad eventi cibernetici.

In tale ottica assume rilevanza anche **la direttiva sulla protezione cibernetica e la sicurezza informatica nazionale** emanata con DPCM del 17 febbraio 2017 (pubblicato sulla GU n. 87 del 13-4-2017) che si pone l'obiettivo di aggiornare la precedente direttiva del 24 gennaio 2013 e di conseguenza anche la relativa architettura di sicurezza cibernetica nazionale e di protezione delle infrastrutture critiche.

L’esigenza di nuovi provvedimenti ed anche di nuove strategie nasce innanzitutto dall’emanazione della **direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016**, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (c.d. Direttiva NIS) recepita in Italia con il **d.lgs. 18 maggio 2018, n. 65** nonché da quanto previsto dall'art. 7-bis, comma 5, del decreto-legge 30 ottobre 2015, n. 174, convertito, con modificazioni, dalla **legge n. 198 del 2015**, al fine di ricondurre a sistema e unitarietà le diverse competenze coinvolte nella gestione della situazione di crisi, in relazione al grado di pregiudizio alla sicurezza della Repubblica e delle Istituzioni democratiche poste dalla Costituzione a suo fondamento.

Del resto (come si è anticipato) lo stesso art. 51 del CAD specifica che l'AgID attui, per quanto di competenza e in raccordo con le altre autorità competenti in materia, il Quadro strategico nazionale per la sicurezza dello spazio cibernetico e il Piano nazionale per la sicurezza cibernetica e la sicurezza informatica. AgID, in tale ambito:

a) coordina, tramite il Computer Emergency Response Team Pubblica Amministrazione (CERT-PA) istituito nel suo ambito, le iniziative di prevenzione e gestione degli incidenti di sicurezza informatici;
b) promuove intese con le analoghe strutture internazionali;
c) segnala al Ministro per la pubblica amministrazione e l'innovazione il mancato rispetto delle regole tecniche da parte delle pubbliche amministrazioni.

Contenuti della Direttiva NIS (Network ed Information Security)

La Direttiva contiene una serie di misure legislative che hanno lo scopo di creare un livello comune, quanto più elevato possibile, di sicurezza delle reti e in generale dei sistemi informativi all'interno dell'Unione Europea.
Lo scopo principale di questa normativa europea è di ottenere che:

- ogni singolo Stato Membro dell'Unione Europea migliori la propria capacità di gestire la sicurezza delle reti;
- che insieme se ne aumenti il livello, in modo comune e cooperato;
- che tutti gli Stati riescano a riconoscere e gestire i rischi, nonché gli errori più gravi da parte degli operatori e dei fornitori dei servizi digitali.

Il d.lgs. n. 65/2018

Nel mese di Maggio del 2018 l'Italia ha adottato la Direttiva (UE) 2016/1148 con un decreto che ha inteso da una parte promuovere una cultura di gestione del rischio e di segnalazione degli incidenti tra i principali attori economici e, dall'altra, rafforzare la cooperazione a livello nazionale e in ambito Ue.

A chi si applica?

Il d.lgs. n. 65/2018 si applica agli Operatori di Servizi Essenziali (OSE) e ai Fornitori di Servizi Digitali (FSD).
Gli Operatori di Servizi Essenziali (OSE) sono i soggetti, pubblici o privati, che forniscono servizi essenziali per la società e l'economia nei settori sanitario, dell'energia, dei trasporti, bancario, delle infrastrutture dei mercati finanziari, della fornitura e distribuzione di acqua potabile e delle infrastrutture digitali.
I Fornitori di Servizi Digitali (FSD) sono le persone giuridiche che forniscono servizi di e-commerce, cloud computing o motori di ricerca, con stabilimento principale, sede sociale o rappresentante designato sul territorio nazionale. Gli obblighi previsti per gli FSD non si applicano alle imprese che la normativa europea definisce "piccole" e "micro", quelle cioè che hanno meno di 50 dipendenti e un fatturato o bilancio annuo non superiore ai 10 milioni di Euro.

Il CSIRT

Il decreto prevede, inoltre, l'istituzione presso la Presidenza del Consiglio dei Ministri di un unico Computer Security Incident Response Team, detto CSIRT italiano, che andrà a sostituire, fondendoli, gli attuali CERT Nazionale (operante presso il Ministero dello Sviluppo Economico) e CERT-PA (operante presso l'Agenzia per l'Italia Digitale). Proprio questo processo di fusione potrebbe essere di non facile gestione, il che potrebbe dilatare i tempi di adozione del decreto del Presidente del Consiglio dei Ministri che dovrà essere adottato più avanti per disciplinare nel dettaglio l'organizzazione ed il funzionamento del CSIRT. In ogni caso, lo CSIRT italiano avrà compiti di natura tecnica nella prevenzione e risposta ad incidenti informatici svolti in cooperazione con gli altri CSIRT europei.

In particolare:

- definisce le procedure per la prevenzione e la gestione degli incidenti informatici;
- riceve le notifiche di incidente, informandone il DIS (Dipartimento Informazioni per la Sicurezza), quale punto di contatto unico e per le attività di prevenzione e preparazione a eventuali situazioni di crisi e di attivazione delle procedure di allertamento affidate al Nucleo per la Sicurezza Cibernetica;
- fornisce al soggetto che ha effettuato la notifica le informazioni che possono facilitare la gestione efficace dell'evento;
- informa gli altri Stati membri dell'UE eventualmente coinvolti dall'incidente, tutelando la sicurezza e gli interessi commerciali dell'OSE o del FSD nonché la riservatezza delle informazioni fornite;
- garantisce la collaborazione nella rete di CSIRT, attraverso l'individuazione di forme di cooperazione operativa, lo scambio di informazioni e la condivisione di *best practices*.

Obblighi in materia di sicurezza informatica

Tanto gli Operatori di Servizi essenziali che i Fornitori di Servizi Digitali:

- sono chiamati ad adottare misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi e a prevenire e minimizzare l'impatto degli incidenti a carico della sicurezza delle reti e dei sistemi informativi, al fine di assicurare la continuità del servizio;
- hanno l'obbligo di notificare, senza ingiustificato ritardo, gli incidenti che hanno un impatto rilevante, rispettivamente sulla continuità e sulla fornitura del servizio, al CSIRT, informandone anche l'Autorità competente NIS di riferimento.

Gli FSD sono tenuti ad applicare le prescrizioni dettate dal decreto di recepimento a partire dal 24 giugno 2018, data di entrata in vigore del provvedimento, valutando la rilevanza degli incidenti sulla base dei criteri e delle soglie indicati nel Regolamento (UE) 2018/151 del 30 gennaio 2018.

Un incidente a carico di un FSD è rilevante se si verifica almeno una delle seguenti condizioni:
Indisponibilità del servizio fornito per oltre 5.000.000 di ore utente
Perdita di integrità, autenticità o riservatezza dei dati per oltre 100.000 utenti dell'UE
Rischio per la sicurezza e/o l'incolumità pubblica, o in termini di perdite di vite umane
Danni materiali superiori a 1.000.000 di EUR per almeno un utente nell'UE

Autorità Competenti NIS

Autorità Competenti NIS	Ambito di competenza
Ministero dello sviluppo economico	• Settore dell'energia – Sottosettori energia elettrica, gas e petrolio • Settore delle infrastrutture digitali • Servizi digitali
Ministero delle infrastrutture e dei trasporti	Settore dei trasporti – Sottosettori trasporto aereo, trasporto ferroviario, trasporto per vie d'acqua e trasporto su strada
Ministero dell'economia e delle finanze in collaborazione con Banca d'Italia e Consob	• Settore bancario • Settore delle infrastrutture dei mercati finanziari
Ministero della salute, Regioni e Province autonome di Trento e di Bolzano (direttamente o per il tramite delle Autorità sanitarie territorialmente competenti)	Settore sanitario
Ministero dell'ambiente e della tutela del territorio e del mare, Regioni e Province autonome di Trento e di Bolzano (direttamente o per il tramite delle Autorità territorialmente competenti)	Settore della fornitura e distribuzione di acqua potabile

Compiti

Vigilano sulla sua applicazione ed esercitano le relative potestà ispettive e sanzionatorie, fatte salve le attribuzioni e le competenze degli organi preposti alla tutela dell'ordine e della sicurezza pubblica. Salvo che il fatto costituisca reato, la violazione da parte di OSE e FSD degli obblighi previsti dal decreto legislativo comporta l'irrogazione di sanzioni amministrative pecuniarie fino ad un massimo di 150.000 euro; la reiterazione determina l'aumento fino al triplo della sanzione prevista.

Procedono ad identificare gli OSE entro il 9 novembre 2018 (consultando, laddove necessario, le Autorità competenti NIS degli altri Stati Membri), individuando anche le soglie in ragione delle quali un incidente è da considerarsi pregiudizievole per la sicurezza delle reti e dei sistemi informativi.
Se un evento implica anche violazione di dati personali, le Autorità competenti NIS operano in stretta cooperazione con il Garante per la protezione dei dati personali. Al riguardo, sono in corso approfondimenti per propiziare un raccordo tra gli obblighi introdotti dal Decreto legislativo di recepimento della Direttiva NIS e quelli previsti dal nuovo Regolamento europeo per la protezione dei dati personali (GDPR).

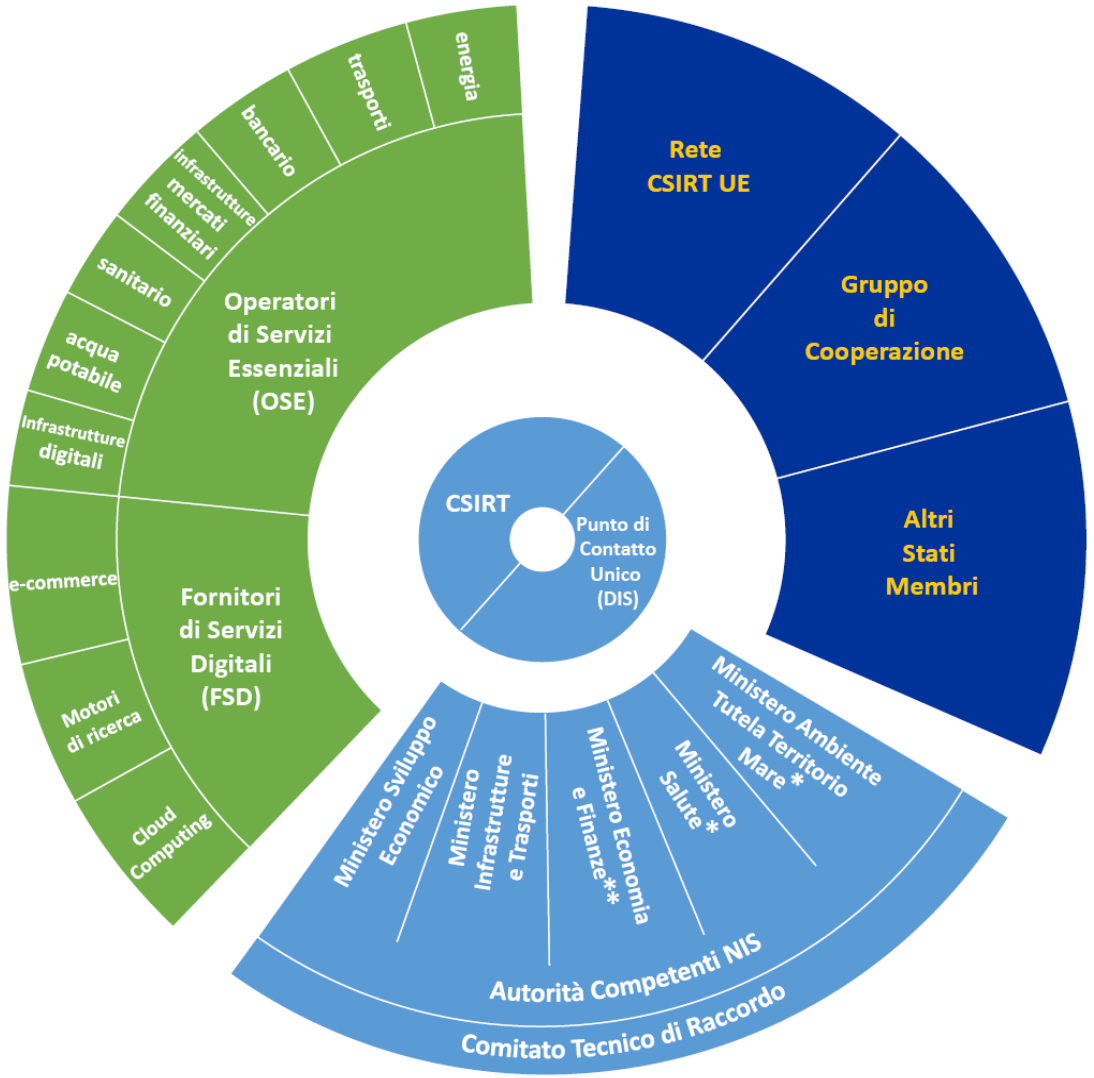
Possono predisporre linee guida per la notifica degli incidenti e dettare specifiche misure di sicurezza, sentiti gli OSE.

Comitato tecnico di raccordo

Il Comitato verrà istituito con apposito DPCM allo scopo di agevolare le Autorità competenti NIS nell'adempimento dei compiti loro affidati.
Il Comitato opererà presso la Presidenza del Consiglio dei ministri, riunendo i delegati dei Ministeri-Autorità competenti NIS e i rappresentanti delle Regioni e Province autonome in numero non superiore a due, designati in sede di Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e di Bolzano.

Regime Sanzionatorio

La Direttiva NIS lascia agli Stati membri un margine di discrezionalità riguardo al tipo e alla natura delle sanzioni applicabili, a condizione che siano effettive, proporzionate e dissuasive.
Nell'esercitare tale discrezionalità, il governo ha ritenuto di stabilire che le autorità competenti potranno applicare sanzioni amministrative fino a 150.000 Euro in caso di violazione da parte degli operatori di servizi essenziali (e dei fornitori di servizi digitali) degli obblighi previsti dal decreto.



Servizi interessati

Attori governativi NIS

Meccanismi della cooperazione europea

* più regioni e province autonome di Trento e di Bolzano

** in collaborazione con le autorità di vigilanza di settore, Banca d'Italia e Consob

Il perimetro di sicurezza nazionale cibernetica

Successivamente, il decreto-legge n. 105 del 2019 è stato adottato al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, nonché degli enti e degli operatori nazionali, pubblici e privati, attraverso l'istituzione di un perimetro di sicurezza nazionale cibernetica e la previsione di misure volte a garantire i necessari standard di sicurezza rivolti a minimizzare i rischi. Talune modifiche sono state apportate, a tale provvedimento, dal decreto-legge n. 162 del 2019, in materia di proroga dei termini e altre disposizioni sulla pubblica amministrazione.

In attuazione del decreto-legge n. 105 sono stati definiti in particolare il DPCM 30 luglio 2020, n. 131, che ha dettato criteri e modalità per l'individuazione dei soggetti inclusi nel perimetro nazionale di sicurezza cibernetica, e il DPCM 14 aprile 2021, n. 81 che definisce le modalità per la notifica nel caso di incidenti riguardanti beni ITC.

Inoltre, il decreto-legge n. 162 (all'art. 26) ha previsto che il Computer security incident response team – CSIRT italiano, istituito presso la Presidenza del Consiglio, sia incardinato nel Dipartimento delle informazioni per la sicurezza – DIS, in aderenza con il decreto del Presidente del Consiglio dell'8 agosto 2019 che ha previsto la costituzione del CSIRT presso il DIS.

E' stata, inoltre, disposta l'istituzione della **Direzione generale per lo sviluppo della prevenzione e tutela informatiche** presso il Dipartimento della pubblica sicurezza del Ministero dell'interno ad opera del decreto-legge 34/2020 (cd. decreto Rilancio, art. 240).

Si attendono gli ultimi due DPCM:

- il terzo è relativo alle categorie per le quali sarà necessario effettuare la notifica al Centro di valutazione e certificazione nazionale (Cvcn);
- il quarto è relativo ai criteri per l'accreditamento dei laboratori competenti per le verifiche delle condizioni di sicurezza.

Infine, con il decreto-legge 14 giugno 2021, n. 82, convertito con modificazioni nella legge 4 agosto 2021, n. 10 si è proceduto alla definizione dell'architettura nazionale di cybersicurezza e all'istituzione dell'Agenzia per la cybersicurezza nazionale.

Nell’individuazione delle diverse disposizioni normative che disciplinano la cybersecurity non poteva ovviamente mancare il **cybersecurity act** e cioé il Regolamento 881/2019 che oltre a specificare il mandato ed il ruolo dell’Enisa (Agenzia dell’Unione europea per la sicurezza delle reti e dell’informazione) definisce il quadro europeo per la certificazione della sicurezza informatica dei dispositivi connessi a internet e di altri prodotti e servizi digitali.

Il provvedimento costituisce una parte fondamentale della nuova strategia dell'UE per la sicurezza cibernetica, che mira a:

- rafforzare la resilienza dell'Unione agli attacchi informatici;
- a creare un mercato unico della sicurezza cibernetica in termini di prodotti, servizi e processi;
- ad accrescere la fiducia dei consumatori nelle tecnologie digitali.

Ma cosa si intende per cyber risk?

La rivoluzione digitale sta portando molti benefici alla nostra società, ma, come spesso accade, bisogna considerare anche il rovescio della medaglia. Difatti, accanto agli innumerevoli benefici, l'uso incontrollato di Internet può comportare una quantità notevole di insidie e problematiche che rientrano nell'ambito di quel fenomeno definito cyber risk "rischio informatico (o ICT)".

Il rischio informatico può essere definito come il rischio di danni economici (rischi diretti) e di reputazione (rischi indiretti) derivanti dall'uso della tecnologia, intendendosi con ciò sia i rischi impliciti nella tecnologia (i cosiddetti rischi di natura endogena) che i rischi derivanti dall'automazione, attraverso l'uso della tecnologia, di processi operativi aziendali (i cosiddetti rischi di natura esogena).

In particolare questi ultimi possono essere:
- danneggiamento di hardware e software;
- errori nell’esecuzione delle operazioni nei sistemi;
- malfunzionamento dei sistemi;
- programmi indesiderati.

Tali rischi possono verificarsi in diversi casi:

1. i programmi “virus” destinati ad alterare od impedire il funzionamento dei sistemi informatici;
2. le truffe informatiche;
3. l’accesso abusivo a sistemi informatici o telematici;
4. il cyberstalking;
5. il cyberbullismo;
6. la pedo-pornografia;
7. il revenge porn.

Solo una piena consapevolezza del concetto di sicurezza informatica può davvero metterci al riparo da sgradevoli sorprese.

Ogni giorno vengono compiuti migliaia di attacchi informatici attraverso le tecniche più varie e termini come malware, ransomware, trojan horse, account cracking, phishing, sono diventati parte del vocabolario anche per i non esperti.

J. Edgar Hoover, capo dell'FBI (Federal Bureau of Investigation) moltissimi anni fa affermava: "*L'unico computer a prova di hacker è quello spento, non collegato ad Internet e chiuso a chiave in una cassaforte*". Appena viene riacceso diventa potenzialmente vulnerabile e può essere attaccato, ad esempio durante l'installazione di eventuali aggiornamenti al sistema operativo.

Naturalmente per evitare attacchi informatici, o almeno per limitarne le conseguenze, è necessario adottare delle contromisure; i calcolatori e le reti di telecomunicazione necessitano di protezione anche se come in qualsiasi ambiente la sicurezza assoluta non è concretamente realizzabile.
Il modo per proteggersi è imparare a riconoscere le origini del rischio. Gli strumenti di difesa informatica sono molteplici, si pensi antivirus, antispyware, blocco popup, firewall ecc., ma tuttavia non sempre si rivelano efficienti, in quanto esistono codici malevoli in grado di aggirare facilmente le difese, anche con l'inconsapevole complicità degli stessi utenti.