Nuovi strumenti di comunicazione e utilizzo dei dispositivi digitali in ambito professionale

17 gennaio 2025

Aspetti legali e di cyber security

Avv. Alessio Cicchinelli

JUST4CYBER

ROMELAW

La Commissione Europea ha presentato il 15 gennaio un **piano d'azione volto a rafforzare la cybersicurezza degli ospedali e dei prestatori di servizi sanitari.** Tale piano d'azione è stato annunciato dalla presidente von der Leyen come una priorità fondamentale entro i primi cento giorni del nuovo mandato.

La ragione di questa scelta discende dal fatto **che la digitalizzazione a tappe forzate di tutta la società sta portando anche una notevole rivoluzione nell'assistenza sanitaria, consentendo di offrire servizi migliori ai pazienti attraverso innovazioni quali il fascicolo elettronico, la telemedicina e la diagnostica basate sull'intelligenza artificiale. Tuttavia, gli attacchi informatici possono interferire con le procedure mediche, creare ingorghi nei pronto soccorso e interrompere i servizi vitali che, nei casi più gravi, potrebbero avere un impatto diretto sulla vita degli europei. Solo nel 2023 gli Stati membri hanno segnalato 309 incidenti significativi di cybersicurezza che hanno colpito il settore sanitario, più che in qualsiasi altro settore critico**.

L'Agenzia per la cybersicurezza nazionale sin dai suoi esordi si è occupata di garantire la resilienza delle strutture sanitarie attraverso una serie di azioni, intervenendo anche direttamente per ripristinarne i servizi di oncologia, radiologia, Cup e pronto soccorso. Consapevoli dell'importanza della protezione dei dati sanitari e del ruolo cruciale degli operatori del settore nel garantire la loro sicurezza, il Servizio Operazioni e gestione delle crisi cyber di ACN ha realizzato dei report specifici sul tema della protezione delle strutture medico-sanitarie che è stato presentato in Regione Lazio e Regione Lombardia alla presenza dei vertici istituzionali.

Adesso il piano d'azione europeo propone che l'ENISA, istituisca un **centro paneuropeo di sostegno alla cybersecurity per gli ospedali e i prestatori di assistenza sanitaria, fornendo loro strumenti, servizi e formazione su misura**. L'iniziativa si basa sul più ampio quadro dell'UE per rafforzare la cibersicurezza in tutte le infrastrutture critiche e segna la prima iniziativa settoriale specifica per attuare l'intera gamma di misure dell'UE in materia di cibersicurezza.

La disciplina della cyber sicurezza

1. Quando si parla di cybersicurezza, quali fonti devo consultare?

2. Come faccio a capire quale, tra queste fonti, si applica al mio Ente?

3. Cosa mi impone di fare la normativa sulla cyber sicurezza che si applica al mio Ente?

4. Quando devo fare le cose che la normativa sulla cyber sicurezza impone al mio Ente di realizzare?

JUST4CYBER

1) Quando si parla di cybersicurezza, quali fonti devo consultare?

LEGGE 28 giugno 2024, n. 90

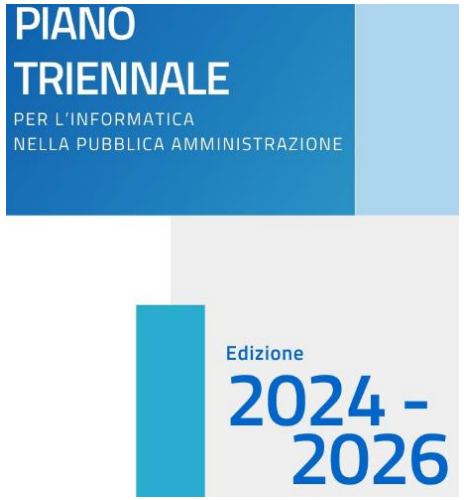
Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici. (24G00108)

(GU n.153 del 2-7-2024)

Vigente al: 17-7-2024

DECRETO LEGISLATIVO 4 settembre 2024 , n. 138

Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148. (24G00155)



JUST4CYBER

2) Come faccio a capire quale, tra queste fonti, si applica al mio Ente?

Art. 1, co. 1, legge 90/24

1. Le pubbliche amministrazioni centrali individuate ai sensi dell'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196, le regioni e le province autonome di Trento e di Bolzano, le città metropolitane, i comuni con popolazione superiore a 100.000 abitanti e, comunque, i comuni capoluoghi di regione, nonché le società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti, le società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane e ***le aziende sanitarie locali*** *segnalano e notificano, con le modalità e nei termini di cui al comma 2 del presente articolo, gli incidenti indicati nella tassonomia di cui all'articolo 1, comma 3-bis, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, come modificato dall'articolo 3 della presente legge, aventi impatto su reti, sistemi informativi e servizi informatici. Tra i soggetti di cui al presente comma sono altresì comprese le rispettive società in house che forniscono servizi informatici, i servizi di trasporto di cui al primo periodo del presente comma ovvero servizi di raccolta, smaltimento o trattamento di acque reflue urbane, domestiche o industriali, come definite ai sensi dell'articolo 2, punti 1), 2) e 3), della direttiva 91/271/CEE del Consiglio, del 21 maggio 1991, o di gestione dei rifiuti, come definita ai sensi dell'articolo 3, punto 9), della direttiva 2008/98/CE del Parlamento europeo e del Consiglio, del 19 novembre 2008.*

JUST4CYBER

2) Come faccio a capire quale, tra queste fonti, si applica al mio Ente?

Art. 3, co. 1, d.lgs. NIS2

1. Nell'ambito di applicazione del presente decreto **rientrano i soggetti pubblici e privati delle tipologie di cui agli allegati I, II, III e IV, che costituiscono parte integrante del presente decreto, che sono sottoposti alla giurisdizione nazionale ai sensi dell'articolo 5**. Gli allegati I e II descrivono i settori ritenuti, rispettivamente, altamente critici e critici, nonché i relativi sottosettori e le tipologie di soggetti. **Gli allegati III e IV descrivono, rispettivamente, le categorie di pubbliche amministrazioni e le ulteriori tipologie di soggetto a cui si applica il presente decreto**.

JUST4CYBER

2) Come faccio a capire quale, tra queste fonti, si applica al mio Ente?

ALLEGATO III

Amministrazioni centrali, regionali, locali e di altro tipo

1. Ai fini dell'articolo 3, comma 6, sono individuatele seguenti categorie:

a) amministrazioni centrali:

1) gli Organi costituzionali e di rilievo costituzionale;
2) la Presidenza del Consiglio dei ministri e i Ministeri;
3) le Agenzie fiscali;
4) le Autorita' amministrative indipendenti;

b) amministrazioni regionali:

1. le Regioni e le Province autonome.

c) amministrazioni locali

1. le Citta' metropolitane;
2. i Comuni con popolazione superiore a 100.000 abitanti;
3. i Comuni capoluoghi di regione;
4. le Aziende sanitarie locali.

JUST4CYBER

2) Come faccio a capire quale, tra queste fonti, si applica al mio Ente?

d) altri soggetti pubblici:

1. gli Enti di regolazione dell'attivita' economica;
2. gli Enti produttori di servizi economici;
3. gli Enti a struttura associativa;
4. gli Enti produttori di servizi assistenziali, ricreativi e culturali;
5. gli Enti e le Istituzioni di ricerca;
6. gli Istituti zooprofilattici sperimentali.

JUST4CYBER

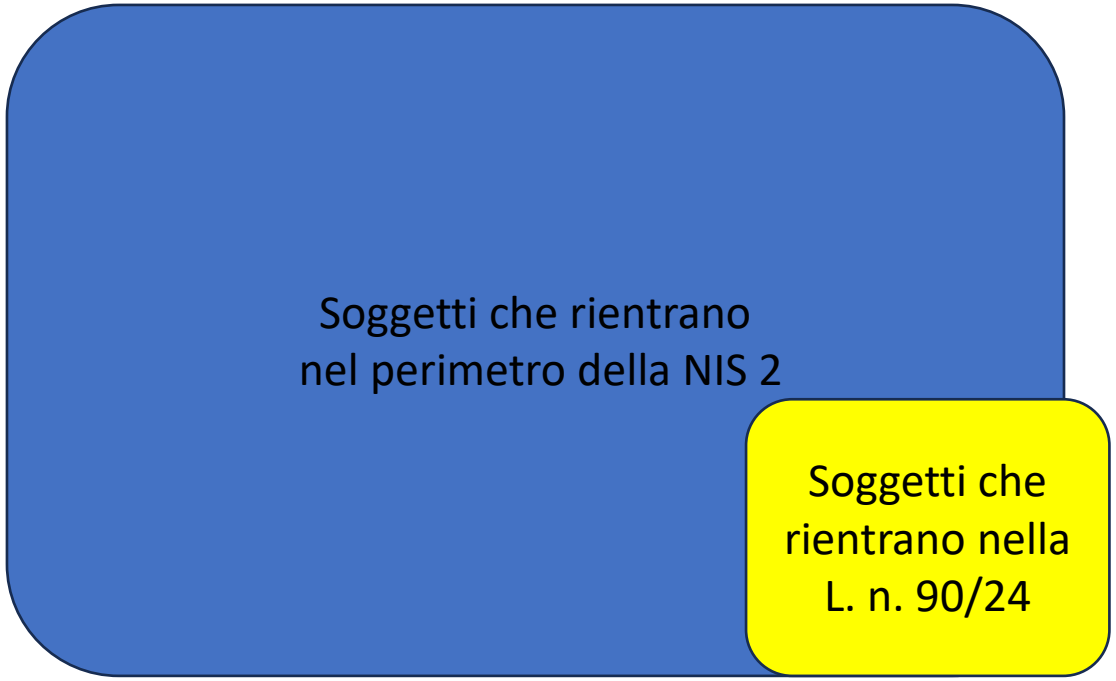
2) Come faccio a capire quale, tra queste fonti, si applica al mio Ente?

Art. 3, co. 8, d.lgs. NIS2

8. Il presente decreto si applica, altresì, indipendentemente dalle loro dimensioni, anche ai soggetti delle tipologie di cui all'allegato IV, individuati secondo le procedure di cui al comma 13.

JUST4CYBER

2) Come faccio a capire quale, tra queste fonti, si applica al mio Ente?



JUST4CYBER

3) Cosa mi impone di fare la normativa sulla cyber sicurezza che si applica al mio Ente?

A. Notifica degli incidenti informatici

Art. 1, co. 2, legge n. 90/24

2. I soggetti di cui al comma 1 segnalano, senza ritardo e comunque **entro il termine massimo di ventiquattro ore dal momento in cui ne sono venuti a conoscenza** a seguito delle evidenze comunque ottenute, qualunque incidente riconducibile a una delle tipologie individuate nella tassonomia di cui al comma 1 **ed effettuano, entro settantadue ore a decorrere dal medesimo momento, la notifica completa di tutti gli elementi informativi disponibili**. La segnalazione e la successiva notifica sono effettuate tramite le apposite procedure disponibili nel sito internet istituzionale dell'Agenzia per la cybersicurezza nazionale.

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

JUST4CYBER

3) Cosa mi impone di fare la normativa sulla cyber sicurezza che si applica al mio Ente?

A. Notifica degli incidenti informatici

Art. 25, d.lgs. NIS 2

2. I soggetti essenziali e i soggetti importanti notificano, senza ingiustificato ritardo, al CSIRT Italia ogni incidente che, ai sensi del comma 4, ha un impatto significativo sulla fornitura dei loro servizi, secondo le modalità e i termini di cui agli articoli 30, 31 e 32.

5. Ai fini della notifica di cui al comma 1, i soggetti interessati trasmettono al CSIRT Italia: a) senza ingiustificato ritardo, **e comunque entro 24 ore** da quando sono venuti a conoscenza dell'incidente significativo, una pre-notifica che, ove possibile, indichi se l'incidente significativo possa ritenersi il risultato di atti illegittimi o malevoli o può avere un impatto transfrontaliero; b) senza ingiustificato ritardo, **e comunque entro 72 ore** da quando sono venuti a conoscenza dell'incidente significativo, una notifica dell'incidente che, ove possibile, aggiorni le informazioni di cui alla lettera a) e indichi una valutazione iniziale dell'incidente significativo, comprensiva della sua gravità e del suo impatto, nonché, ove disponibili, gli indicatori di compromissione; c) su richiesta del CSIRT Italia, una relazione intermedia sui pertinenti aggiornamenti della situazione; d) una relazione finale entro un mese dalla trasmissione della notifica dell'incidente di cui alla lettera b), che comprenda:
1) una descrizione dettagliata dell'incidente, ivi inclusi la sua gravità e il suo impatto;
2) il tipo di minaccia o la causa originale (root cause) che ha probabilmente innescato l'incidente;
3) le misure di attenuazione adottate e in corso;
4) ove noto, l'impatto transfrontaliero dell'incidente;
e) in caso di incidente in corso al momento della trasmissione della relazione finale di cui alla lettera d), una relazione mensile sui progressi e una relazione finale entro un mese dalla conclusione della gestione dell'incidente.

JUST4CYBER

3) Cosa mi impone di fare la normativa sulla cyber sicurezza che si applica al mio Ente?

A. Notifica degli incidenti informatici

Nozione di incidente informatico…

….nel decreto NIS 2

t) «incidente»: un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informativi e di rete o accessibili attraverso di essi;
u) «quasi-incidente»: cd. near-miss, un evento che avrebbe potuto configurare un incidente senza che quest'ultimo si sia tuttavia verificato, ivi incluso il caso in cui l'incidente sia stato efficacemente evitato;
v) «incidente di sicurezza informatica su vasta scala»: un incidente che causa un livello di perturbazione superiore alla capacità di uno Stato membro di rispondervi o che ha un impatto significativo su almeno due Stati membri; (art. 2, d.lgs. NIS 2)

JUST4CYBER

3) Cosa mi impone di fare la normativa sulla cyber sicurezza che si applica al mio Ente?

A. Notifica degli incidenti informatici

Entità dell'incidente informatico da notificare…

….nel decreto NIS 2

4. *Un incidente è considerato significativo se:*
a) ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato;
b) ha avuto ripercussioni o è idoneo a provocare ripercussioni su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli. (art. 25, co. 4 d.lgs. NIS 2)

JUST4CYBER

3) Cosa mi impone di fare la normativa sulla cyber sicurezza che si applica al mio Ente?

B. Gestione del rischio cyber

Art. 8, legge n. 90/24

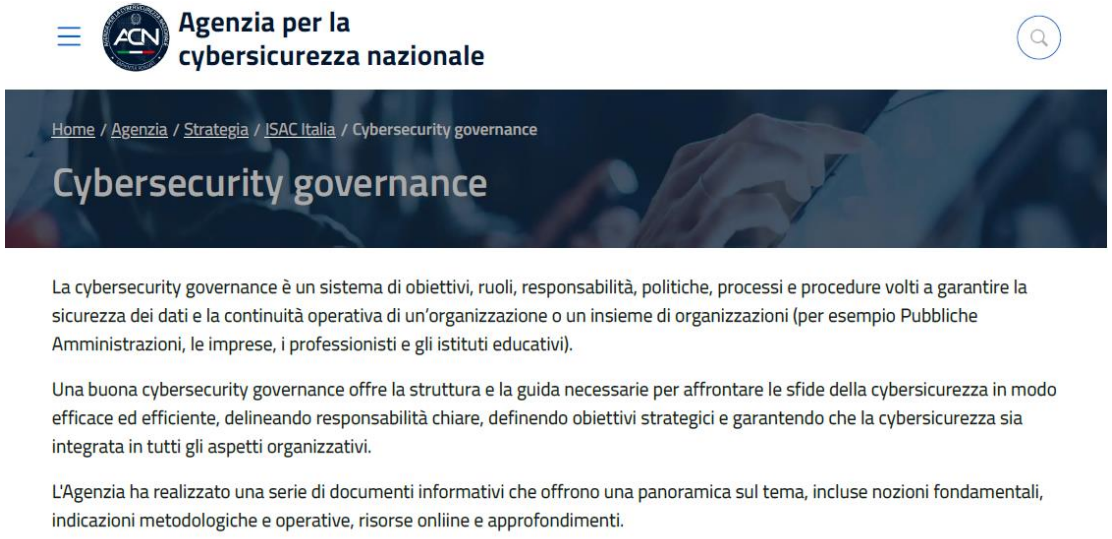
1. I soggetti di cui all'articolo 1, comma 1, **individuano, ove non sia già presente, una struttura, anche tra quelle esistenti, nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente**, che provvede: a) allo sviluppo delle politiche e delle procedure di sicurezza delle informazioni; b) alla produzione e all'aggiornamento di sistemi di analisi preventiva di rilevamento e di un piano per la gestione del rischio informatico; c) alla produzione e all'aggiornamento di un documento che definisca i ruoli e l'organizzazione del sistema per la sicurezza delle informazioni dell'amministrazione; d) alla produzione e all'aggiornamento di un piano programmatico per la sicurezza di dati, sistemi e infrastrutture dell'amministrazione; e) alla pianificazione e all'attuazione di interventi di potenziamento delle capacità per la gestione dei rischi informatici, in coerenza con i piani di cui alle lettere b) e d); f) alla pianificazione e all'attuazione dell'adozione delle misure previste dalle linee guida per la cybersicurezza emanate dall'Agenzia per la cybersicurezza nazionale; g) al monitoraggio e alla valutazione continua delle minacce alla sicurezza e delle vulnerabilità dei sistemi per il loro pronto aggiornamento di sicurezza.

2. Presso le strutture di cui al comma 1 opera il **referente per la cybersicurezza**, individuato in ragione di specifiche e comprovate professionalità e competenze in materia di cybersicurezza.

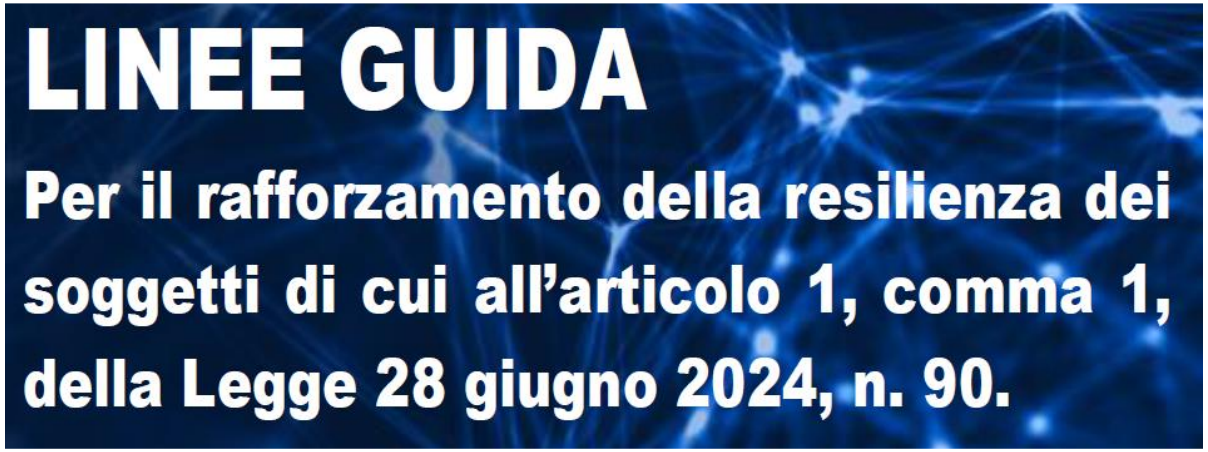
3) Cosa mi impone di fare la normativa sulla cyber sicurezza che si applica al mio Ente?

B. Gestione del rischio cyber

https://www.acn.gov.it/portale/isac-italia/cybersecurity-governance



https://www.acn.gov.it/portale/linee-guida-rafforzamento-resilienza



3) Cosa mi impone di fare la normativa sulla cyber sicurezza che si applica al mio Ente?

B. Gestione del rischio cyber

Art. 24, decreto NIS 2

1. I soggetti essenziali e i soggetti importanti adottano **misure tecniche, operative e organizzative adeguate e proporzionate**, secondo le modalità e i termini di cui agli articoli 30, 31 e 32, alla gestione dei rischi posti alla sicurezza dei sistemi informativi e di rete che tali soggetti utilizzano nelle loro attività o nella fornitura dei loro servizi, nonché per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei loro servizi e per altri servizi. Tali misure:
a) assicurano un livello di sicurezza dei sistemi informativi e di rete adeguato ai rischi esistenti, tenuto conto delle conoscenze più aggiornate e dello stato dell'arte in materia e, ove applicabile, delle pertinenti norme nazionali, europee e internazionali, nonché dei costi di attuazione;
b) sono proporzionate al grado di esposizione a rischi del soggetto, alle dimensioni del soggetto e alla probabilità che si verifichino incidenti, nonché alla loro gravità, compreso il loro impatto sociale ed economico.
2. Le misure di cui al comma 1 sono basate su un **approccio multi-rischio**, volto a proteggere i sistemi informativi e di rete nonché il loro ambiente fisico da incidenti

3) Cosa mi impone di fare la normativa sulla cyber sicurezza che si applica al mio Ente?

B. Gestione del rischio cyber

Art. 24, decreto NIS 2

2. Le misure di cui al comma 1 sono basate su un **approccio multi-rischio**, volto a proteggere i sistemi informativi e di rete nonché il loro ambiente fisico da incidenti

d) «approccio multi-rischio»: cosiddetto approccio all-hazards, l'approccio alla gestione dei rischi che considera quelli derivanti da tutte le tipologie di minaccia ai sistemi informativi e di rete nonché al loro contesto fisico, quali furti, incendi, inondazioni, interruzioni, anche parziali, delle telecomunicazioni e della corrente elettrica, e in generale accessi fisici non autorizzati;

3) Cosa mi impone di fare la normativa sulla cyber sicurezza che si applica al mio Ente?

B. Gestione del rischio cyber. Responsabilità

Art. 23, decreto NIS 2

1. Gli **organi di amministrazione** e gli **organi direttivi** dei soggetti essenziali e dei soggetti importanti: **a) approvano le modalità di implementazione delle misure di gestione dei rischi per la sicurezza informatica adottate da tali soggetti ai sensi dell'articolo 24; b) sovrintendono all'implementazione degli obblighi di cui al presente capo e di cui all'articolo 7; c) sono responsabili delle violazioni di cui al presente decreto.**

2. Gli organi di amministrazione e gli organi direttivi dei soggetti essenziali e dei soggetti importanti: **a) sono tenuti a seguire una formazione in materia di sicurezza informatica; b) promuovono l'offerta periodica di una formazione coerente a quella di cui alla lettera a) ai loro dipendenti, per favorire l'acquisizione di conoscenze e competenze sufficienti al fine di individuare i rischi e valutare le pratiche di gestione dei rischi per la sicurezza informatica e il loro impatto sulle attività del soggetto e sui servizi offerti.**

3) Cosa mi impone di fare la normativa sulla cyber sicurezza che si applica al mio Ente?

B. Gestione del rischio cyber. Responsabilità

Art. 40, decreto NIS 2

5. Qualsiasi persona fisica responsabile di un soggetto essenziale o che agisca in qualità di suo rappresentante legale con l'autorità di rappresentarlo, di prendere decisioni per suo conto o di esercitare un controllo sul soggetto stesso, assicura il rispetto delle disposizioni di cui al presente decreto. **Tali persone fisiche possono essere ritenute responsabili dell'inadempimento in caso di violazione del presente decreto da parte del soggetto di cui hanno rappresentanza**

6. Qualora il soggetto non adempia nei termini stabiliti dalla diffida di cui all'articolo 37, commi 6 e 7, **l'Autorità nazionale competente NIS può disporre nei confronti delle persone fisiche di cui al comma 5 del presente articolo, ivi inclusi gli organi di amministrazione e gli organi direttivi di cui all'articolo 23 dei soggetti essenziali e dei soggetti importanti, nonché di quelle che svolgono funzioni dirigenziali a livello di amministratore delegato o rappresentante legale di un soggetto essenziale o importante, l'applicazione della sanzione amministrativa accessoria della incapacità a svolgere funzioni dirigenziali all'interno del medesimo soggetto. Tale sospensione temporanea è applicata finchè il soggetto interessato non adotta le misure necessarie a porre rimedio alle carenze o a conformarsi alle diffide di cui all'articolo 37, commi 6 e 7.**

7. Ai dipendenti pubblici che esercitano i poteri di cui al comma 5, si applicano le norme in materia di responsabilità dei dipendenti pubblici e dei funzionari eletti o nominati. In particolare, la violazione degli obblighi di cui al presente decreto può costituire causa di responsabilità dirigenziale, disciplinare e amministrativo-contabile.

4) Quando devo fare le cose che la normativa sulla cyber sicurezza impone al mio Ente di realizzare?

Art. 1, co. 3, legge n. 90/24

3. Per i comuni con popolazione superiore a 100.000 abitanti e i comuni capoluoghi di regione, per le società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti, per le società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane, per le aziende sanitarie locali e per le società in house che forniscono servizi informatici, i servizi di trasporto di cui al presente comma ovvero servizi di raccolta, smaltimento o trattamento di acque reflue urbane, domestiche o industriali, come definite ai sensi dell'articolo 2, punti 1), 2) e 3), della direttiva 91/271/CEE del Consiglio, del 21 maggio 1991, o di gestione dei rifiuti, come definita ai sensi dell'articolo 3, punto 9), della direttiva 2008/98/CE del Parlamento europeo e del Consiglio, del 19 novembre 2008, gli obblighi di cui ai commi 1 e 2 del presente articolo si applicano a decorrere dal centottantesimo giorno successivo alla data di entrata in vigore della presente legge.

Entrata in vigore del provvedimento: 17/07/2024

+ 180 giorni: **13 GENNAIO 2025**

JUST4CYBER

4) Quando devo fare le cose che la normativa sulla cyber sicurezza impone al mio Ente di realizzare?

Artt. 7 e 43, decreto NIS 2

1. **Dal 1° gennaio al 28 febbraio** di ogni anno successivo alla data di entrata in vigore del presente decreto, i soggetti di cui all'articolo 3, si registrano o aggiornano la propria registrazione sulla piattaforma digitale resa disponibile dall'Autorità nazionale competente NIS ai fini dello svolgimento delle funzioni attribuite all'Agenzia per la cybersicurezza nazionale anche ai sensi del presente decreto. A tal fine, tali soggetti forniscono o aggiornano almeno le informazioni seguenti: a) la ragione sociale; b) l'indirizzo e i recapiti aggiornati, compresi gli indirizzi e-mail e i numeri di telefono; c) la designazione di un punto di contatto, indicando il ruolo presso il soggetto e i recapiti aggiornati, compresi gli indirizzi e-mail e i numeri di telefono; d) ove applicabile, i pertinenti settori, sottosettori e tipologie di soggetto di cui agli allegati I, II, III e IV;
2. Entro il 31 marzo di ogni anno successivo alla data di entrata in vigore del presente decreto, l'Autorità nazionale competente NIS, redige, secondo le modalità di cui all'articolo 40, comma 5, l'elenco dei soggetti essenziali e dei soggetti importanti, sulla base delle registrazioni di cui al comma 1 e delle decisioni adottate ai sensi degli articoli 3, 4, e 6.
3. Tramite la piattaforma digitale di cui al comma 1, l'Autorità nazionale competente NIS comunica ai soggetti registrati di cui al comma 2: a) l'inserimento nell'elenco dei soggetti essenziali o importanti; b) la permanenza nell'elenco dei soggetti essenziali o importanti; c) l'espunzione dall'elenco dei soggetti.

3. Ai sensi dell'articolo 7, comma 1, i soggetti essenziali e i soggetti importanti possono registrarsi a partire dalla data di pubblicazione della piattaforma di cui al medesimo comma.

JUST4CYBER

Avv. Alessio Cicchinelli

alessio.cicchinelli@just4cyber.eu
a
alessio.cicchinelli@aclegal.org

Grazie per l'attenzione!

JUST4CYBER

ROMELAW