Ciclo di webinar in diretta

La legge 90/2024 negli enti locali

Relatore: Dottor Antonio Guzzo

LE NUOVE DISPOSIZIONI NORMATIVE PREVISTE DALLA LEGGE 90 DEL 28 GIUGNO 2024 IN MATERIA DI CYBERSECURITY NEGLI ENTI LOCALI

03-10-2024

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

Sommario

- Gli obblighi di notifica degli incidenti informatici
- La struttura per la cybersicurezza
- Il referente per la cybersicurezza e la modalità di nomina da trasmettere all'Autorità Nazionale per la Cybersicurezza
- I criteri di cybersecurity nella disciplina degli appalti pubblici: gli elementi essenziali sulla cybersicurezza
- I criteri di premialità per le proposte o le offerte che contemplino l'uso di tecnologie di cybersicurezza italiane
- I nuovi reati informatici: l'estorsione informatica

• Gli obblighi di notifica degli incidenti informatici

Art. 1. Obblighi di notifica di incidenti

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.

• Gli obblighi di notifica degli incidenti informatici: la tempistica

Art. 1. Obblighi di notifica di incidenti

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 .

- # Gli obblighi di notifica degli incidenti informatici: il regime sanzionatorio

5. Nel caso di inosservanza dell'obbligo di notifica di cui ai commi 1 e 2, l'Agenzia per la cybersicurezza nazionale comunica all'interessato che la reiterazione dell'inosservanza, nell'arco di cinque anni, comporterà l'applicazione delle disposizioni di cui al comma 6 e **può disporre, nei dodici mesi successivi all'accertamento del ritardo o dell'omissione, l'invio di ispezioni, anche al fine di verificare l'attuazione, da parte dei soggetti interessati dall'incidente, di interventi di rafforzamento della resilienza agli stessi, direttamente indicati dall'Agenzia per la cybersicurezza nazionale ovvero previsti da apposite linee guida adottate dalla medesima Agenzia. Le modalità di tali ispezioni sono disciplinate con determinazione del direttore generale dell'Agenzia per la cybersicurezza nazionale, pubblicata nella Gazzetta Ufficiale .**

6. Nei casi di reiterata inosservanza, nell'arco di cinque anni, dell'obbligo di notifica di cui ai commi 1 e 2, **l'Agenzia per la cybersicurezza nazionale applica altresì, nel rispetto delle disposizioni dell'articolo 17, comma 4 -quater , del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, introdotto dall'articolo 11 della presente legge, una sanzione amministrativa pecuniaria da euro 25.000 a euro 125.000 a carico dei soggetti di cui al comma 1 del presente articolo. La violazione delle disposizioni del comma 1 del presente articolo può costituire causa di responsabilità disciplinare e amministrativo-contabile per i funzionari e i dirigenti responsabili**

CSIRT Italia - Computer Security Incident Response Team

• Gli obblighi di notifica degli incidenti informatici

L’ACN ha pubblicato la Guida alla notifica degli incidenti al CSIRT Italia. La corretta adozione della procedura di notifica degli incidenti cibernetici costituisce infatti un elemento cruciale per garantire sicurezza e resilienza delle reti, dei sistemi informativi e dei servizi informatici.
La prontezza e la precisione delle informazioni fornite durante il processo di notifica rivestono un ruolo fondamentale per consentire al CSIRT Italia di acquisire una conoscenza completa ed esaustiva dell’incidente occorso ai fini dell’attività di allertamento e per fornire ai soggetti impattati il supporto necessario nell’ottica del ripristino dei servizi stessi.
La Guida rappresenta un compendio – una sorta di “testo unico” - delle istruzioni per i diversi soggetti, pubblici e privati, tenuti per legge alla notifica degli incidenti, soggetti inclusi nel Perimetro di Sicurezza Nazionale Cibernetica (PSNC), quelli operanti in ambito NIS e Telco, cui si aggiungono quelle puntualmente rivolte alle entità oggi considerate dalla legge n. 90/2024*.
https://www.acn.gov.it/portale/w/acn-pubblica-la-guida-alla-notifica-degli-incidenti-informatici

• Gli obblighi di notifica degli incidenti informatici

Il flusso informativo verso il CSIRT Italia si snoda nelle seguenti fasi:

1. Una fase preparatoria, con l'obiettivo di raccogliere le prime informazioni idonee a garantire una sufficiente conoscenza dell'evento;
2. ad essa fa seguito la fase di segnalazione dell'incidente, che avviene attraverso la compila-zione di un modulo disponibile sul sito internet del CSIRT Italia: https://www.csirt.gov.it/segnalazione. Tale comunicazione occorre che venga effettuata al Csirt con una tempistica definita nelle linee guida, e diversamente declinata in funzione dell'appartenenza del soggetto ai diversi presidi normativi. In ogni caso, la segnalazione è strettamente correlata al principio di immediatezza della conoscenza dell'incidente, inteso nella sua magnitudo e nel suo carattere di impatto sistemico eventuale;
3. una terza fase attiene alla vera e propria gestione della notifica, cioè le operazioni di incident handling, da parte del personale del CSIRT Italia, per dare supporto alla vittima con efficaci azioni di contenimento e di ripristino dei servizi;
4. il processo si conclude, infine, con la fase di chiusura dell'incidente.

Le linee guida si rivolgono anche ai soggetti, pubblici e privati, che pur non essendo obbligati alla notifica intendono tuttavia, volontariamente segnalare l'incidente allo CSIRT, in questo modo contribuendo a una migliore condivisione della conoscenza del livello e dell'intensità della minaccia, per rafforzare la resilienza dell'ecosistema digitale italiano.

- # Gli obblighi di notifica degli incidenti informatici

Altra novità importante introdotta dalla nuova legge è quella di **segnalare gli incidenti indicati nella tassonomia** di cui all'articolo 1, comma 3-bis, del decreto-legge n. 105 del 2019, così come convertito con modificazioni dalla legge n. 133 del 2019_(il "Decreto Perimetro"). In particolare, il legislatore italiano prevede che le pubbliche amministrazioni poc'anzi richiamate debbano **notificare tali incidenti** utilizzando le procedure disponibili sul sito internet dell'Agenzia per la Cybersicurezza Nazionale

La struttura per la cybersicurezza

Art. 8. Rafforzamento della resilienza delle pubbliche amministrazioni e referente per la cybersicurezza

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.

La struttura per la cybersicurezza

Tale struttura, che potrà essere individuata anche in quella dell'**ufficio del responsabile per la transizione al digitale**, dovrà provvedere a:

a. lo sviluppo di politiche e procedure di sicurezza delle informazioni;

b. la produzione e l'aggiornamento di un piano per il rischio informatico, nonché di sistemi di analisi preventiva di rilevamento del rischio informatico;

c. la produzione e l'aggiornamento di un documento che definisca i ruoli e l'organizzazione del sistema per la sicurezza delle informazioni dell'amministrazione;

d. la pianificazione e l'attuazione di interventi di potenziamento delle capacità per la gestione dei rischi informatici, a partire dalla produzione dei piani precedentemente elencati;

e. la pianificazione e l'attuazione dell'adozione delle misure previste dalle linee guida per la cybersicurezza emanate dall'Agenzia per la Cybersicurezza Nazionale;

f. il monitoraggio e la valutazione continua delle minacce alla sicurezza e alla vulnerabilità dei sistemi per il loro pronto aggiornamento di sicurezza.

Tale struttura, inoltre, avrà anche il preciso obbligo di verificare che i programmi e le applicazioni informatiche e di comunicazione elettronica in uso presso la pubblica amministrazione, che impieghino soluzioni crittografiche, rispettino le linee guida sulla crittografia e quelle sulla conservazione delle password adottate dall'Agenzia per la Cybersicurezza Nazionale e dall'Autorità Garante per la Protezione dei Dati Personali.

Il referente per la cybersicurezza

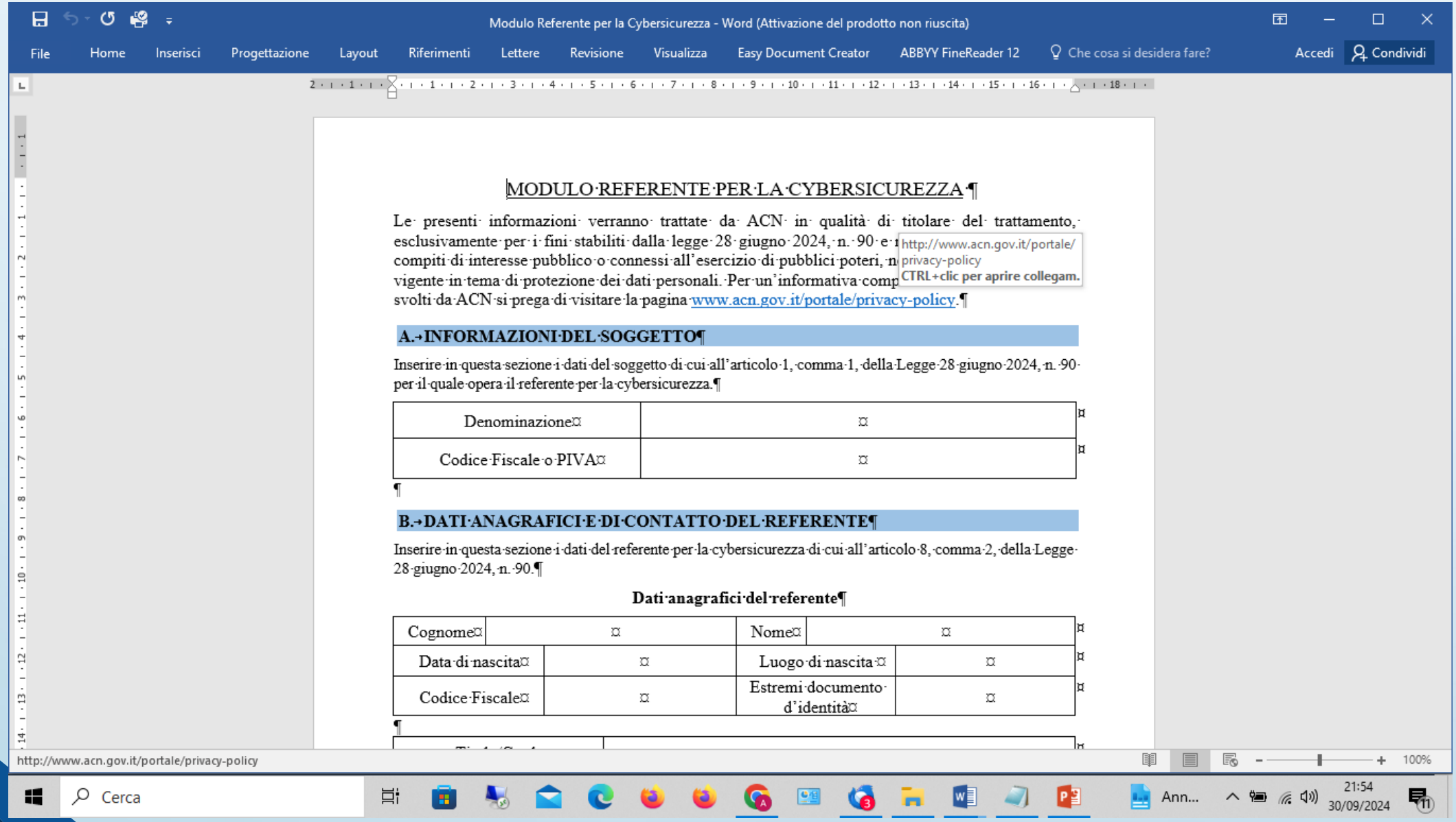
La comunicazione ad ACN (art. 8, comma 2) avviene inviando una PEC, attraverso il proprio domicilio digitale, all'indirizzo di posta elettronica certificata di ACN (acn@pec.acn.gov.it) e deve contenere:

la nomina del referente per la cybersicurezza (redatta in forma libera) firmata digitalmente dal rappresentante legale del soggetto, o da persona da lui delegata (in quest'ultimo caso allegare anche la delega);
il modulo referente per la cybersicurezza, compilato e firmato dal referente per la cybersicurezza.
https://www.acn.gov.it/portale/referente-per-la-cybersicurezza

Il referente per la cybersicurezza

Tutti i soggetti previsti dall'articolo 1, comma 1 della Legge 28 giugno 2024, n. 90 "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici", sono tenuti a comunicare all'Agenzia la nomina del Referente per la cybersicurezza.
https://www.acn.gov.it/portale/w/referente-cybersicurezza-le-modalita-di-comunicazione

Il modulo di nomina



Il modulo di nomina

Titolo/Grado	
Articolazione/Ufficio	
Ruolo/Incarico	
Sede di servizio	

Informazioni di contatto del referente

Indirizzo e-mail	
Numero telefono mobile	
Numero telefono fisso	

Altre informazioni utili

Data di aggiornamento

FIRMA (*)

_____

Il referente per la cybersicurezza

Perché un referente della cybersicurezza?
La figura del referente cybersicurezza è nata per difendere le PA dalle sfide della sicurezza digitale di fronte a un aumento massiccio delle minacce cyber e della dipendenza a livello amministrativo dalle tecnologie informatiche. Si tratta quindi di una figura poliedrica che deve essere in grado non solo di affrontare, ma anche di prevenire eventuali attacchi e quindi di garantire un ambiente tecnologico sicuro attraverso un approccio olistico. La sua formazione dunque deve comprendere conoscenze tecniche, capacità di anali, di comunicazione, di problem solving e di gestione del rischio.

Il referente per la cybersicurezza

Qual è il riferimento normativo?
La figura del referente è introdotta dalla legge 90 del 28 giugno 2024 “Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici”. In particolare, l’art 8 “Rafforzamento della resilienza delle pubbliche amministrazioni e referente per la cybersicurezza” prevede l’istituzione di una struttura per lo sviluppo delle politiche e delle procedure di sicurezza. All’interno di questa struttura, deve essere individuato il referente per la cybersicurezza.

Il referente per la cybersicurezza

Quali sono le PA interessate?
Devono nominare il referente le PA centrali, 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, 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.

Quali caratteristiche deve avere il referente?
La legge è chiara: il soggetto individuato deve possedere specifiche comprovate professionalità e competenze in materia di cybersicurezza. Se le amministrazioni non dispongono di personale dipendente che risponde a queste caratteristiche, possono nominare un dipendente di una pubblica amministrazione, previa autorizzazione di quest'ultima. La struttura e il referente cyber possono essere individuati, rispettivamente, nell' ufficio RTD e nel suo responsabile.

Il referente per la cybersicurezza

Quali sono i compiti del referente?
La struttura e il referente devono provvedere allo sviluppo delle politiche di sicurezza informatica; alla produzione e all' aggiornamento di sistemi di analisi preventiva e di un piano per la gestione del rischio; alla produzione e all' aggiornamento di un piano programmatico per la sicurezza di dati, sistemi e infrastrutture; alla pianificazione e all'attuazione di interventi di potenziamento delle capacità per la gestione dei rischi informatici; all' attuazione delle misure previste dalle linee guida ACN.

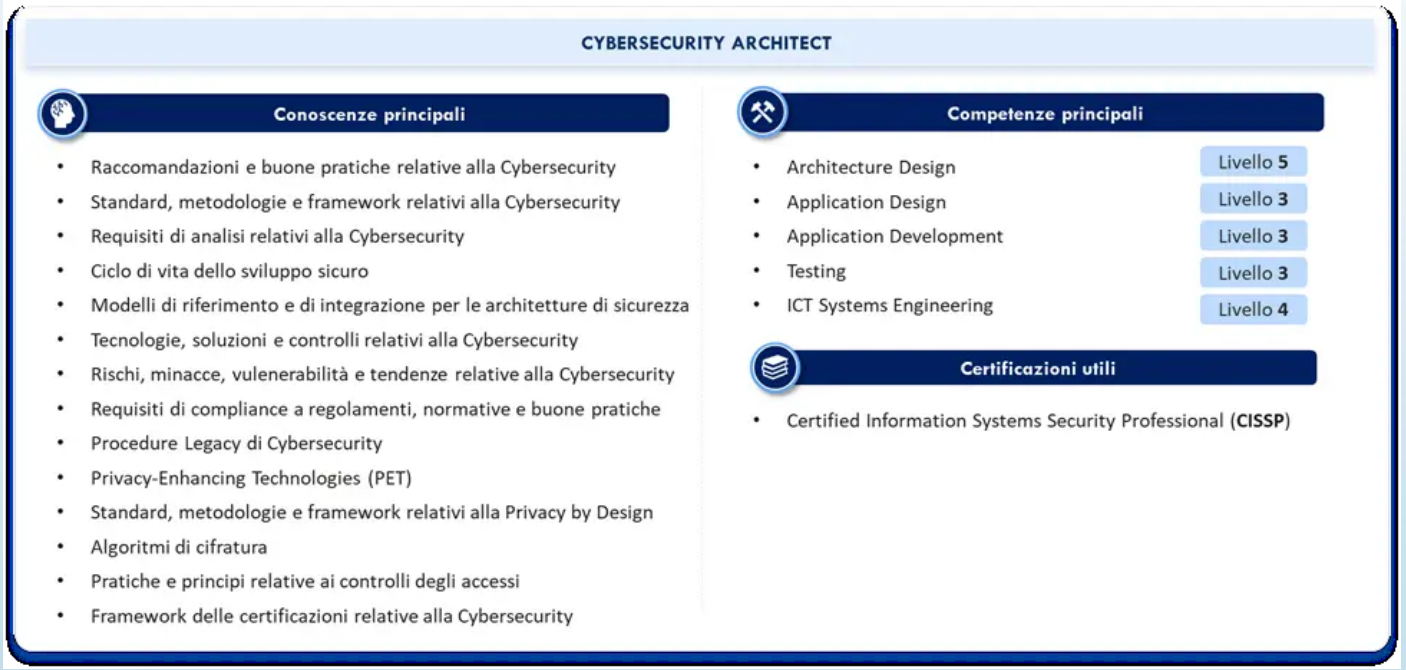
I criteri di cybersecurity

Art. 14. Disciplina dei contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici e disposizioni di raccordo con il decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133

Comma 1…. sono individuati, per specifiche categorie tecnologiche di beni e servizi informatici, **gli elementi essenziali di cybersicurezza** che i soggetti di cui all'articolo 2, comma 2, del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, tengono in considerazione nelle attività di approvvigionamento di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici nonché i casi in cui, per la tutela della sicurezza nazionale, devono essere previsti criteri di premialità per le proposte o per le offerte che contemplino l'uso di tecnologie di cybersicurezza italiane o di Paesi appartenenti all'Unione europea o di Paesi aderenti all'Alleanza atlantica (NATO) o di Paesi terzi individuati con il decreto di cui al presente comma tra quelli che sono parte di accordi di collaborazione con l'Unione europea o con la NATO in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione. **Ai fini del presente articolo, si intende per «elementi essenziali di cybersicurezza» l'insieme di criteri e regole tecniche la conformità ai quali, da parte di beni e servizi informatici da acquisire, garantisce la confidenzialità, l'integrità e la disponibilità dei dati da trattare in misura corrispondente alle esigenze di tutela di cui al primo periodo**.

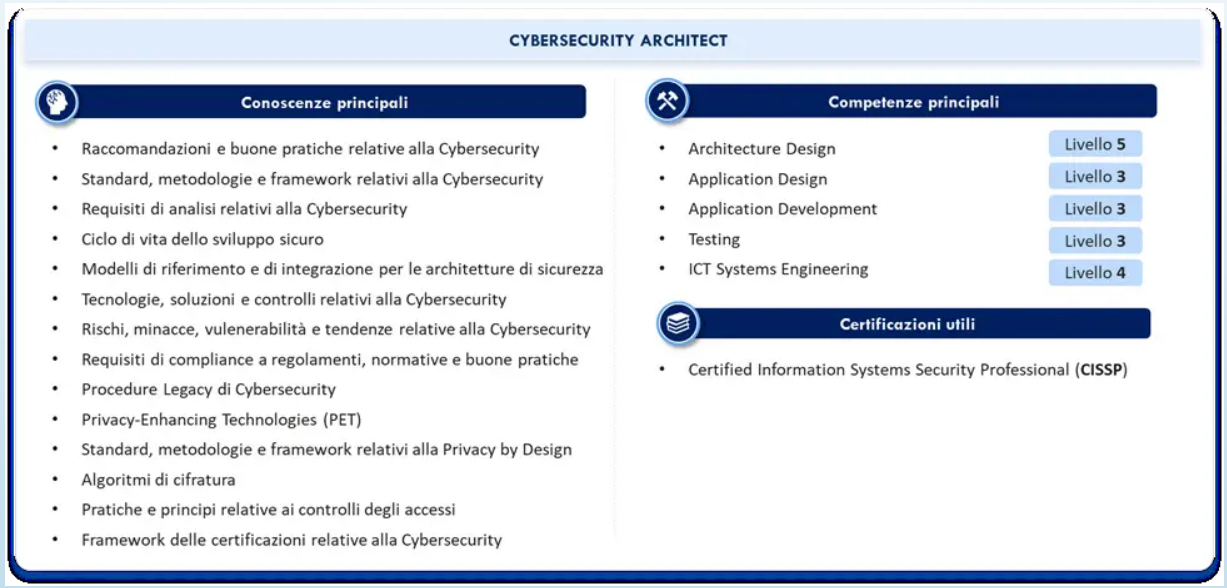
I criteri di cybersecurity

La Legge sulla Cybersicurezza inoltre introduce nella disciplina dei **contratti pubblici di beni e servizi informatici** alcuni **criteri di cybersecurity**, definiti dal legislatore come l'insieme di criteri e regole tecniche la conformità ai quali, da parte di beni e servizi informatici da acquisire, garantisce la confidenzialità, l'integrità e la disponibilità dei dati da trattare in misura corrispondente alle esigenze di tutela degli interessi nazionali strategici. Tali **elementi essenziali di cybersicurezza** saranno individuati da uno specifico Decreto del Presidente del Consiglio dei Ministri da **emanarsi entro 120 giorni** dall'entrata in vigore della Legge sulla Cybersicurezza. Tale Decreto del Presidente del Consiglio dei Ministri, peraltro, provvederà anche a dettagliare i casi in cui, per la tutela della sicurezza nazionale, debbano essere previsti **criteri di premialità per le proposte o le offerte che contemplino l'uso di tecnologie di cybersicurezzaitaliane** o di Paesi appartenenti all'**Unione europea** o di Paesi aderenti all'Alleanza atlantica (**NATO**) o di **Paesi terzi** –individuati nel medesimo decreto – tra quelli che hanno **accordi di collaborazione con l'Unione europea o con la NATO in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione.**



I criteri di cybersecurity

2. Nei casi individuati ai sensi del comma 1, le stazioni appaltanti, comprese le centrali di committenza:
a) possono esercitare la facoltà di cui agli articoli 107, comma 2, e 108, comma 10, del codice dei contratti pubblici, di cui al decreto legislativo 31 marzo 2023, n. 36, se accertano che l'offerta non tiene in considerazione gli elementi essenziali di cybersicurezza individuati con il decreto di cui al comma 1;
b) tengono sempre in considerazione gli elementi essenziali di cybersicurezza di cui al comma 1 nella valutazione dell'elemento qualitativo, ai fini dell'individuazione del miglior rapporto qualità/prezzo per l'aggiudicazione;
c) nel caso in cui sia utilizzato il criterio del minor prezzo, ai sensi dell'articolo 108, comma 3, del codice di cui al decreto legislativo n. 36 del 2023, inseriscono gli elementi di cybersicurezza di cui al comma 1 del presente articolo tra i requisiti minimi dell'offerta;
d) nel caso in cui sia utilizzato il criterio dell'offerta economicamente più vantaggiosa, ai sensi dell'articolo 108, comma 4, del codice di cui al decreto legislativo n. 36 del 2023, nella valutazione dell'elemento qualitativo ai fini dell'individuazione del migliore rapporto qualità/prezzo, stabiliscono un tetto massimo per il punteggio economico entro il limite del 10 per cento;

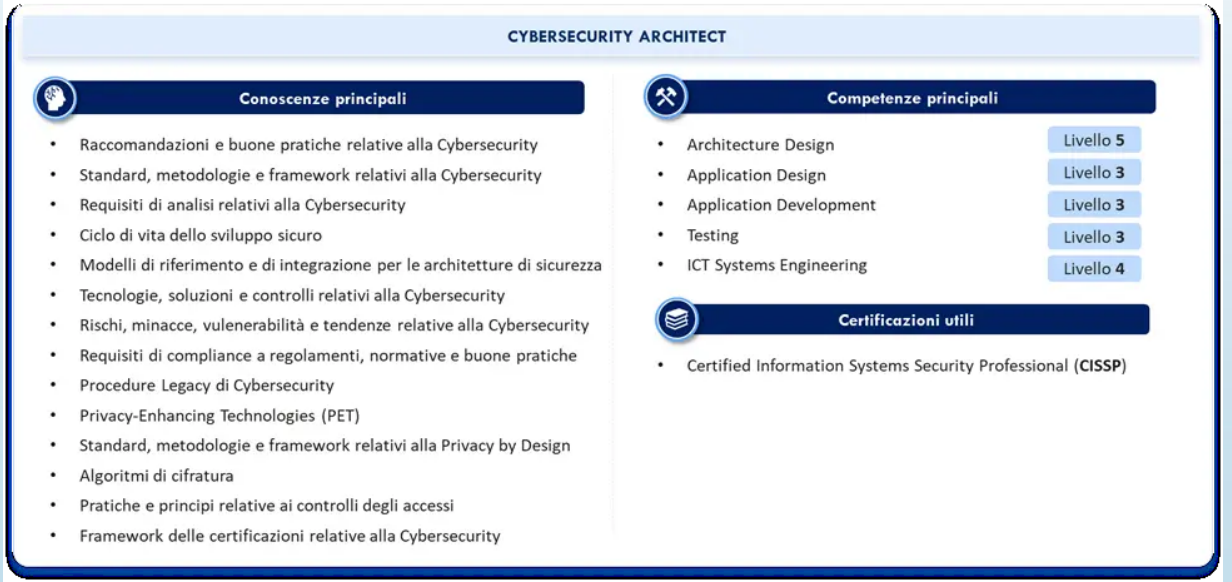


I criteri di cybersecurity: la premialità

e) **prevedono criteri di premialità per le proposte o per le offerte che contemplino l'uso di tecnologie di cybersicurezza italiane o di Paesi appartenenti all'Unione europea o di Paesi aderenti alla NATO** o di Paesi terzi individuati con il decreto di cui al comma 1 tra quelli che sono parte di accordi di collaborazione con l'Unione europea o con la NATO in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione, al fine di tutelare la sicurezza nazionale e di conseguire l'autonomia tecnologica e strategica nell'ambito della cybersicurezza.

3. Le disposizioni di cui al comma 1 si applicano anche ai soggetti privati non compresi tra quelli di cui all'articolo 2, comma 2, del codice di cui al decreto legislativo 7 marzo 2005, n. 82, e inseriti nell'elencazione di cui all'articolo 1, comma 2 -bis, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133.

4. Resta fermo quanto stabilito dall'articolo 1 del citato decreto-legge n. 105 del 2019 per i casi ivi previsti di approvvigionamento di beni, sistemi e servizi di information and communication technology destinati ad essere impiegati nelle reti e nei sistemi informativi nonché per l'espletamento dei servizi informatici di cui alla lettera b) del comma 2 del medesimo articolo 1.



La responsabilità amministrativa

Infine la legge introduce alcune principali novità in materia di responsabilità amministrativa degli enti e sui reati informatici con l'inasprimento severo delle pene per i dirigenti e funzionari pubblici

La responsabilità amministrativa

«Art. 615 *-ter (Accesso abusivo ad un sistema informatico o telematico)*
Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.
La pena è della reclusione *da due a dieci anni* :
«Art. 615 *-quater (Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici)* .
Chiunque, al fine di procurare a sé o ad altri un *vantaggio* o di arrecare ad altri un danno, abusivamente si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti, codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto
scopo, è punito con la reclusione sino a due anni e con la multa sino a euro 5.164.
La pena è della reclusione da due anni a sei anni quando ricorre taluna delle circostanze di cui all'articolo 615 -ter *, secondo comma, numero 1).*

La responsabilità amministrativa

«Art. 617 *-bis (Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni o conversazioni telegrafiche o telefoniche)*
Chiunque, fuori dei casi consentiti dalla legge, al fine di prendere cognizione di una comunicazione o di una conversazione telefonica o telegrafica tra altre persone o comunque a lui non diretta, ovvero di impedirla o di interromperla, si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti o parti di apparati o di strumenti idonei a intercettare, impedire o interrompere
comunicazioni o conversazioni telefoniche o telegrafiche tra altre persone, è punito con la reclusione da uno a quattro anni.
La pena è della reclusione da due a sei anni quando ricorre taluna delle circostanze di cui all'articolo 615 -ter *, secondo comma, numero 1).*
Art. 617 *-quater (Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche)* .
Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da un anno e sei mesi a cinque anni. Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma. I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.
Tuttavia si procede d'ufficio e la pena è della reclusione *da quattro a dieci anni* se il fatto è commesso:
1) in danno di taluno dei sistemi informatici o telematici indicati nell'articolo 615 -ter *, terzo comma* ;
2) *in danno di un pubblico ufficiale nell'esercizio o a causa delle sue funzioni o da un pubblico ufficiale* o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, *o da chi esercita, anche abusivamente, la professione di investigatore privato, o* con abuso della qualità di operatore del sistema;

La responsabilità amministrativa

«Art. 617 *-quinquies (Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche)*
Chiunque, fuori dai casi consentiti dalla legge, al fine di intercettare comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero di impedirle o interromperle, si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparecchiature, programmi, codici, parole chiave o altri mezzi atti ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni.
Quando ricorre taluna delle circostanze di cui all'articolo 617 -quater *, quarto comma, numero 2), la pena è della reclusione da due a sei anni.*
Art. 617 *-sexies (Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche)*
Chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, forma falsamente ovvero altera o sopprime, in tutto o in parte, il contenuto, anche occasionalmente intercettato, di taluna delle comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, è punito, qualora ne faccia uso o lasci che altri ne facciano uso, con la reclusione da uno a quattro anni.
La pena è della reclusione *da tre a otto anni* nei casi previsti dal quarto comma dell'articolo 617 *-quater* .
Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa.».

La responsabilità amministrativa

«Art. 629 ***(Estorsione)***
Chiunque, mediante violenza o minaccia, costringendo taluno a fare o ad omettere qualche cosa, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da cinque a dieci anni e con la multa da euro 1.000 a euro 4.000.
La pena è della reclusione da sette a venti anni e della multa da euro 5.000 a euro 15.000, se concorre taluna delle circostanze indicate *nel terzo comma dell'articolo 628* .
«Art. 635 ***-bis (Danneggiamento di informazioni, dati e programmi informatici)***

Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione *da due a sei anni* .
La pena è della reclusione da tre a otto anni:

La responsabilità amministrativa

«Art. 635 *-ter (Danneggiamento di informazioni, dati e programmi informatici pubblici o di interesse pubblico)*.
Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici *di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, è punito con la reclusione da due a*
sei anni .
La pena è della reclusione da tre a otto anni:
Art. 635 *-quater (Danneggiamento di sistemi informatici o telematici)*
Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635 *-bis* , ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione *da due a sei anni* .
La pena è della reclusione da tre a otto anni

La responsabilità amministrativa

«Art. 640 ***(Truffa)***
Chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa
da euro 51 a euro 1.032.
La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549: