PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 28 - numero 6026 di Mercoledì 25 febbraio 2026

UNI EN 18037:2025, la nuova frontiera della cybersecurity

Un approccio strutturato per misurare la sicurezza informatica di sistemi e processi in vari settori, con linee guida per controlli, valutazione dei rischi e armonizzazione tra enti e stakeholder.

La UNI EN 18037: 2025 è una norma innovativa e priva di precedenti.

Questo documento è stato preparato dalla commissione tecnica CEN / CLC / JTC 13, che si occupa di protezione dei dati e cybersicurezza. Questa norma indica le modalità di valutazione del livello di sicurezza informatica per specifici settori di mercato o nelle aree di sviluppo di applicazioni.

È un documento che rappresenta un passo preparatorio per la elaborazione di processi di certificazione di sicurezza informatica, sia per prodotti ICT, sia per processi e per sistemi, che vengano utilizzati in uno specifico settore di mercato, per garantire servizi affidabili ai propri clienti.

Come esempi di settori di mercato, vengono presi in considerazione le reti mobili, l'identità digitale, la sanità elettronica, il trasporto pubblico ed i sistemi di pagamento.

Appare evidente come questi sistemi informatici comprendono un gran numero di stakeholder che operano, ognuno nel proprio ruolo, per garantire la sicurezza nel settore specifico affidato allo stakeholder. Come avviene per qualunque sistema informatico, che voglia raggiungere un elevato livello di garanzia di sicurezza, occorre trovare un punto di incontro fra la necessità di rispettare regole di sicurezza informatica e il costo di questi interventi. Il grande vantaggio di questa norma è proprio quello di permettere di allineare le esigenze di sicurezza di tutti gli enti, che danno il proprio contributo ad un settore tecnico o commerciale specifico.

La norma, come oggi ormai è regola, si apre con un glossario, che permette di allineare e coordinare il significato di termini, talvolta di così recente origine, da creare dubbi nei soggetti coinvolti nell'utilizzo di queste espressioni.

La norma indi illustra le modalità con cui possono essere impostate le valutazioni di cybersecurity per il settore specifico, indicando quali sono i principi da attuare, quali sono le informazioni da raccogliere e come sia possibile applicare in modo coordinato i controlli di sicurezza informatica.

Successivamente la norma analizza specifici sistemi settoriali informatici dando dettagliate indicazioni sulle modalità con le quali la valutazione deve essere condotta.

Un paragrafo di particolare interesse riguarda la modalità con cui sia possibile ipotizzare potenziali attacchi al sistema informatico, nonché le modalità con cui tali attacchi possano essere messi sotto controllo.

La norma è accompagnata da vari annessi informativi, di grande importanza, come ad esempio l'annesso A, che mette a disposizione delle scale di valutazione nell'effettuazione della valutazione del rischio.

Un altro annesso offre numerosi esempi di come possano essere utilizzati degli approcci coordinati ai livelli di sicurezza da raggiungere, a fronte dei vari scenari esaminati.

Come accennato, questa norma funge da base per futuri sviluppi di sistemi di certificazione della sicurezza informatica.

Ringrazio l'ente normativo dell'Estonia, che cortesemente ha messo a disposizione dei lettori un estratto della norma stessa, in lingua inglese, che potrà essere assai utile ai lettori per comprendere i temi esaminati e valutare l'opportunità di un tempestivo acquisto.

UNI EN 18037:2025 - Guidelines on a sectoral cybersecurity assessment (pdf)

Adalberto Biasiotti

www.puntosicuro.it