PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 28 - numero 6185 di Lunedì 02 novembre 2026

Cybersicurezza dei macchinari: le linee guida della UNI/PdR 199

La prassi di riferimento UNI/PdR 199:2026 per la valutazione delle vulnerabilità e la mitigazione dei rischi di cybersicurezza delle macchine. Focus sulle indicazioni del Regolamento macchine.

Come evidenziato durante tutta la campagna europea " Lavoro sano e sicuro nell'era digitale", promossa dall'Agenzia europea per la sicurezza e la salute sul lavoro (EU-OSHA), l'**evoluzione della tecnologia** sta cambiando il mondo del lavoro e anche della tutella della salute e sicurezza dei lavoratori.

La crescente digitalizzazione dell'economia e l'uso di tecnologie digitali e nuovi macchinari industriali, tra sviluppo della robotica e dell' intelligenza artificiale, offrono sì opportunità di miglioramento di produttività ed efficienza, ma anche nuovi **rischi** emergenti.

Ad esempio, tra i rischi connessi all'evoluzione tecnologica, ci sono anche quelli che rientrano nella sfera della **cybersicurezza**, considerata ormai una componente fondamentale della sicurezza dei macchinari.

Come ricordato in uno spazio web dell'Ente italiano di Normazione (UNI), la **sicurezza informatica** è diventata ormai "un fattore critico da prendere in debita considerazione nella progettazione, produzione e utilizzo dei macchinari". E "individuare e valutare tempestivamente i rischi legati alla cibersicurezza industriale" è un aspetto di "particolare delicatezza".

Proprio a partire da queste considerazioni è stata realizzata, in collaborazione con Federmacchine, la nuova **prassi di riferimento UNI/PdR 199** "***Linee di indirizzo per la protezione dall'alterazione dei sistemi informatici delle macchine***". Una prassi che definisce, come indicato da UNI, un "**approccio metodologico** strutturato per l'analisi delle vulnerabilità, individuando, dove necessario, misure di mitigazione, al fine di garantire un livello di sicurezza accettabile per il contesto in cui il prodotto è destinato ad essere utilizzato".

Nell'articolo ci soffermiamo sulla UNI/PdR 199 affrontando i seguenti argomenti:

- Le prassi di riferimento e la UNI/PdR 199:2026
- La UNI/PdR 199:2026 e le indicazioni del Regolamento macchine
- La UNI/PdR 199:2026 e l'indice del documento

Pubblicità

Le prassi di riferimento e la UNI/PdR 199:2026

Nelle FAQ sul sito UNI è possibile, innanzitutto, approfondire cosa sia una **prassi di riferimento**.

Si indica che le **prassi di riferimento** sono "documenti UNI che introducono prescrizioni tecniche o modelli applicativi settoriali di norme tecniche, quando non ci sono norme né progetti di norma nazionali, europei o internazionali".

Possono anche essere "buone pratiche già in uso nei servizi al cittadino/consumatore, applicazioni settoriali di specifiche esistenti, disciplinari industriali, protocolli per la gestione di marchi proprietari, modelli di gestione sperimentati a livello locale, adozioni di CWA a livello nazionale". Queste prassi sono elaborate sulla base di un "**rapido processo di condivisione** tra i soli autori, non più di nove mesi, in appositi Tavoli e sotto la conduzione operativa di UNI".

Ricordiamo che anche i CWA (CEN Workshop Agreement) sono documenti tecnici sperimentali sviluppati in tempi rapidi con il confronto e il contributo di tutte le parti interessate.

Nelle FAQ si ricorda che **dopo due anni** dalla pubblicazione delle prassi, si valuta "se far evolvere la prassi di riferimento in un documento normativo. Dopo cinque anni o sono trasformate in norma UNI, UNI/TS, UNI/TR o sono ritirate".

In particolare la prassi **UNI/PdR 199:2026** "*Linee di indirizzo per la protezione dall'alterazione dei sistemi informatici delle macchine*", entrata in vigore il **primo ottobre 2026**, è stata sviluppata in collaborazione con la Federazione nazionale delle associazioni dei produttori di beni strumentali e loro accessori destinati allo svolgimento di processi manifatturieri dell'industria e dell'artigianato (Federmacchine) ed elaborata dal Tavolo *"Linea guida sulla cybersafety applicabile al settore delle macchine*" condotto da UNI e costituito da numerosi esperti.

Si ricorda che la prassi di riferimento non prende in considerazione i requisiti del Regolamento Cyber Resilience Act (UE) 2024/2847 e il Cybersecurity Act (Regolamento (UE) 2019/881).

La UNI/PdR 199:2026 e le indicazioni del Regolamento macchine

La prassi di riferimento segnala l'importanza di individuare e valutare in modo tempestivo tutti i rischi legati alla **cibersicurezza industriale**, integrandoli, dunque, nel processo di valutazione dei rischi già previsto dalla Direttiva macchine e dal **Regolamento (UE) 2023/1230**.

Ricordiamo che il Regolamento (UE) 2023/1230 stesso già al **considerando n. 25** spiega che «*Altri rischi relativi a nuove tecnologie digitali sono quelli provocati da terzi malintenzionati che incidono sulla sicurezza dei prodotti rientranti nell'ambito di applicazione del presente regolamento. A tale proposito i fabbricanti dovrebbero essere tenuti ad adottare misure proporzionate che si limitano alla protezione della sicurezza dei prodotti rientranti nell'ambito di applicazione del presente regolamento. Ciò non preclude l'applicazione ai prodotti rientranti nell'ambito di applicazione del presente regolamento di altri atti giuridici dell'Unione che affrontano specificamente aspetti di cibersicurezza*».

Riguardo a questi aspetti sono poi inseriti nel Regolamento specifici requisiti essenziali di sicurezza e di tutela della salute (RESS) relativi alla progettazione e alla costruzione di prodotti.

RESS 1.1.9. ? Protezione dall'alterazione

La macchina o il prodotto correlato devono essere progettati e costruiti in modo tale da fare sì che il collegamento ad essi di un altro dispositivo, tramite qualsiasi caratteristica del dispositivo connesso stesso o tramite qualsiasi dispositivo remoto che comunica con la macchina o il prodotto correlato, non determini una situazione pericolosa. I componenti hardware che trasmettono segnali o dati, importanti per il collegamento o l'accesso a software che sono fondamentali affinché la macchina o il prodotto correlato rispettino i pertinenti requisiti essenziali di sicurezza e di tutela della salute, devono essere progettati in modo tale da essere

adeguatamente protetti da un'alterazione accidentale o intenzionale. La macchina o il prodotto

correlato devono raccogliere prove in merito a un intervento legittimo o illegittimo su tali componenti hardware, se importante per il collegamento o l'accesso al software critico per la conformità della macchina o del prodotto correlato. Software e dati critici per il rispetto da parte della macchina o del prodotto correlato dei pertinenti requisiti essenziali di sicurezza e di tutela della devono essere individuati come tali e devono essere adeguatamente protetti da un'alterazione accidentale o intenzionale. La macchina o il prodotto correlato devono individuare il software installato sullo stesso, necessario per il suo funzionamento in condizioni di sicurezza, e devono essere in grado di fornire tali informazioni in qualsiasi momento in un formato facilmente accessibile. La macchina o il prodotto correlato devono raccogliere prove di un intervento legittimo o illegittimo sul software o di una modifica del software installato sulla macchina o sul prodotto correlato o della sua configurazione. (...)

Si ricorda poi che in una macchina dotata delle adeguate protezioni, gli aspetti di ***safety*** **e** ***security*** sono strettamente connessi. Un principio importante è che la cybersecurity non penalizzi mai la sicurezza funzionale: le misure di protezione informatica non devono compromettere le prestazioni dei dispositivi di sicurezza né alterare i dati critici.

A questo proposito ricordiamo ? nel documento è presente una parte che si sofferma proprio sui termini, definizioni e acronimi ? che con **cybersicurezza**, come traduzione letterale di *cyber security*, si intendono tutte quelle delle attività necessarie per proteggere rete e sistemi informatici, gli utenti dei sistemi e le altre persone interessate dalle minacce informatiche.

La prassi di riferimento affronta, in definitiva, vari aspetti.

Dall'identificazione delle vulnerabilità che possono essere sfruttate dalle minacce (punto 5), ai passaggi per una corretta valutazione del rischio di alterazione (punto 6) fino alle azioni correttive da intraprendere (punto 7). E al punto 8 presenta anche degli esempi di mitigazione del rischio.

La UNI/PdR 199:2026 e l'indice del documento

Concludiamo pubblicando l'indice della prassi di riferimento **UNI/PdR 199:2026**.

INTRODUZIONE

1 **SCOPO E CAMPO DI APPLICAZIONE**

2 **RIFERIMENTI NORMATIVI**

3 **TERMINI, DEFINIZIONI E ACRONIMI**

3.1 GENERALI

3.2 SOGGETTI COINVOLTI

3.3 LIVELLI DI SICUREZZA

4 **PRINCIPIO**

5 **IDENTIFICAZIONE DELLE VULNERABILITÀ CHE POSSONO ESSERE SFRUTTATE DALLE MINACCE**

6 **VALUTAZIONE DEL RISCHIO DI ALTERAZIONE DEI SISTEMI INFORMATICI DELLE MACCHINE**

6.1 PROCESSO DI VALUTAZIONE DEL RISCHIO

6.2 RACCOLTA DELLA DOCUMENTAZIONE E IDENTIFICAZIONE DEL PRODOTTO

6.3 ANALISI DELLE INTERAZIONI DEL PRODOTTO

6.4 STIMA DEI RISCHI

6.4.1 GENERALITÀ

6.4.2 PROBABILITÀ

6.4.3 IMPATTI E CONSEGUENZE

6.4.4 STIMA DEL RISCHIO COMPLESSIVO

6.5 DEFINIZIONE DI MISURE DI MITIGAZIONE DEL RISCHIO

7 **EVENTUALI MISURE DI MITIGAZIONE DEI RISCHI INFORMATICI**

7.1 LIMITI DEL SISTEMA SOTTO OSSERVAZIONE

7.2 COMPETENZE DELLE PARTI COINVOLTE

7.3 MISURE DI MITIGAZIONE CONTRO I RISCHI DI NATURA INFORMATICA

7.3.1 GENERALITÀ

7.3.2 PROTEZIONE DELLE COMUNICAZIONI (MP1_X)

7.3.3 AUTENTICAZIONE (MP2_X)

7.3.4 MEZZI FISICI DI PROTEZIONE (MP3_X)

7.3.5 MEZZI DI PROTEZIONE HARDWARE (MP4_X)

7.3.6 MEZZI DI PROTEZIONE SOFTWARE (MP5_X)

7.3.7 ARCHITETTURA DELLE IACS (MP6_X)

7.3.8 REAZIONE DELLE RISORSE AGLI ATTACCHI (MP7_X)

7.3.9 ALTRE MISURE DI PROTEZIONE (MP8_X)

7.3.10 ISTRUZIONI PER L'USO

8 **ESEMPIO DI MITIGAZIONE DEL RISCHIO**

APPENDICE A (INFORMATIVA) - CONSIDERAZIONI SU RESS E CIBERSICUREZZA NEL REGOLAMENTO (UE) 2023/1230 PER LA PROTEZIONE DALL'ALTERAZIONE DEI SISTEMI INFORMATICI

APPENDICE B (INFORMATIVA) - IDENTIFICAZIONE DELLE VULNERABILITÀ CHE POSSONO ESSERE SFRUTTATE DALLE MINACCE

APPENDICE C (INFORMATIVA) - MAPPING FRA MISURE DI MITIGAZIONE, SOGGETTI COINVOLTI E LIVELLI DI SICUREZZA RAGGIUNGIBILI

APPENDICE D (INFORMATIVA) - ESEMPI DI PERICOLI DI NATURA INFORMATICA

APPENDICE E (INFORMATIVA) - ESEMPIO DI PROTEZIONE DALL'ALTERAZIONE DEL SOFTWARE E DELLA TRACCIABILITÀ

APPENDICE F (INFORMATIVA) - INVENTARIO DELLE RISORSE

BIBLIOGRAFIA

RTM

Scarica il documento da cui è tratto l'articolo:

*La prassi di riferimento **UNI/PdR 199:2026** " Linee di indirizzo per la protezione dall'alterazione dei sistemi informatici delle macchine" è liberamente scaricabile sul sito UNI, attraverso quest'indirizzo, previa registrazione.*

***Scarica la normativa di riferimento*:**

Unione Europea - Regolamento (UE) 2023/1230 del Parlamento e del Consiglio del 14 giugno 2023 relativo alle macchine e che abroga la direttiva 2006/42/CE del Parlamento europeo e del Consiglio e la direttiva 73/361/CEE del Consiglio.

Licenza Creative Commons
I contenuti presenti sul sito PuntoSicuro non possono essere utilizzati al fine di addestrare sistemi di intelligenza artificiale.

www.puntosicuro.it