

RILABS

Checklist di sicurezza IT e OT per le aziende manifatturiere

37 controlli per una autovalutazione iniziale

Inventario, reti, protezione dei sistemi, ripristino, accessi e monitoraggio. Un percorso documentale da svolgere insieme a IT, manutenzione e produzione.

Luca Errico

Versione 2.2 | 29 settembre 2026

Questa checklist aiuta a individuare informazioni mancanti e aree da approfondire. Non sostituisce un assessment tecnico, un penetration test o un audit di conformità. Le verifiche non autorizzano modifiche o prove sui sistemi produttivi.

rilabs.it | lucaerrico@rilabs.it

Conserva la copia compilata come documentazione interna. Non inserirvi password, chiavi o altri segreti.

A chi serve e come utilizzarla

Per aziende manifatturiere che vogliono esaminare la gestione della sicurezza dei propri sistemi IT e OT. Da compilare insieme a IT, manutenzione e produzione, coinvolgendo gli altri referenti indicati nelle sezioni.

Impegno: anche in più sessioni, secondo il perimetro e la documentazione disponibile. **Risultato:** informazioni disponibili, lacune da approfondire e priorità da discutere con la direzione.

Limiti: non è un audit di conformità, non sostituisce un penetration test e non autorizza interventi sui sistemi.

Guida alla compilazione

Definisci il perimetro, raccogli le evidenze e registra gli esiti nei riepiloghi. Nel PDF compilabile scegli un esito e inserisci note sintetiche, referente e data. Per note estese usa un allegato interno. Salva una copia e verifica i dati prima di condividerla o stamparla.

Azienda e stabilimento:

Linee e sistemi compresi:

Esclusioni e limiti della verifica:

Referente della compilazione:

Data della verifica e prossimo riesame:

Esiti da utilizzare

Sì: requisito soddisfatto con evidenze. **Parzialmente:** copertura incompleta. **No:** assenza accertata. **Non verificato:** informazioni insufficienti. **Non applicabile:** esclusione motivata.

Non sommare gli esiti per ricavare un giudizio di sicurezza. Per ogni lacuna identifica un referente, una data e un approfondimento proporzionato alle conseguenze sul processo.

Indice delle sezioni

1 Inventario dei sistemi di produzione

2 Separazione delle reti e controllo dei collegamenti

3 Protezione dei sistemi industriali

4 Backup e ripristino della produzione

5 Gestione degli accessi e fattore umano

6 Governo della sicurezza monitoraggio e miglioramento

Cosa fare dopo la compilazione | Glossario

Ogni sezione termina con una tabella di registrazione e indicazioni per utilizzare i risultati. Per note estese, usa un allegato interno e riportare il riferimento nella tabella.

1 Inventario dei sistemi di produzione

Sai quali dispositivi e software permettono alla tua azienda di produrre?

Una macchina può dipendere da un PC industriale, da un programma di controllo, da uno switch o da un collegamento gestito dal manutentore. Se queste dipendenze non sono documentate, diventa più difficile valutare una vulnerabilità, pianificare la manutenzione o ripartire dopo un guasto.

Questa sezione ti aiuta a verificare se l'azienda dispone delle informazioni essenziali sui propri sistemi OT: i dispositivi e i software che controllano o supportano i processi produttivi.

Chi coinvolgere: referente IT, responsabile della manutenzione e, quando necessario, costruttore della macchina o integratore.

Come svolgere i controlli: consulta inventari, schemi, documentazione e informazioni già disponibili. Eventuali riscontri sui sistemi devono essere eseguiti dal personale autorizzato con modalità compatibili con il funzionamento dell'impianto. Non collegare nuovi computer alla rete di produzione, non avviare scansioni e non scollegare dispositivi per compilare questa sezione.

Come registrare le risposte

Per ogni controllo scegli un esito:

- **Sì:** il requisito è soddisfatto nel perimetro esaminato ed è supportato da evidenze.
- **Parzialmente:** le informazioni esistono, ma sono incomplete o coprono solo alcuni sistemi.
- **No:** è stata accertata l'assenza del requisito.
- **Non verificato:** mancano informazioni sufficienti per rispondere.
- **Non applicabile:** il controllo non riguarda il perimetro esaminato; indica il motivo.

Una rassicurazione verbale, da sola, non basta per assegnare "Sì". Annota il documento consultato o il riscontro ottenuto, la data e il referente.

1.1 Elenco dei dispositivi che supportano la produzione

Domanda di controllo: Esiste un inventario aggiornato dei dispositivi che controllano o supportano le linee produttive?

Conseguenze operative: Un inventario incompleto può allungare la diagnosi e il ripristino dopo un guasto o un incidente, complicando l'identificazione dei ricambi e delle dipendenze della linea.

Considera, se presenti: PLC e controllori, pannelli operatore HMI, PC industriali, postazioni di programmazione, server di supervisione, robot, gateway, dispositivi di rete e apparati ausiliari collegati all'ambiente produttivo.

Come verificarlo: Richiedi l'inventario al referente IT o alla manutenzione. Controlla quando è stato aggiornato e confrontalo con la documentazione delle macchine e degli ultimi interventi.

Verifica che permetta di identificare almeno:

- dispositivo, produttore e modello;
- ubicazione e macchina o linea servita;
- funzione e conseguenze di un'eventuale indisponibilità;
- referente interno e fornitore di assistenza;
- identificativo di rete, quando applicabile e disponibile.

Un controllo a campione può far emergere omissioni, ma non dimostra la completezza dell'intero inventario.

Evidenza da annotare: Nome o riferimento dell'inventario, data dell'ultimo aggiornamento e linee comprese.

Se emergono lacune: Assegna a un referente il completamento dell'elenco, iniziando dai sistemi necessari alla produzione. Un dispositivo sconosciuto deve essere identificato insieme alla manutenzione prima di decidere qualsiasi intervento.

1.2 Versioni firmware e aggiornamenti dei controllori

Domanda di controllo: Per PLC, HMI e altri controllori sono note le versioni firmware ed esiste un processo per valutare gli avvisi di sicurezza del produttore?

Conseguenze operative: Versioni e avvisi non valutati possono lasciare problemi rilevanti senza una decisione e rendere più difficile pianificare aggiornamenti compatibili con la produzione.

Il firmware è il software di base che consente al dispositivo di funzionare.

Come verificarlo: Consulta le schede degli apparati, i rapporti di manutenzione e le informazioni disponibili presso il costruttore o l'integratore. Se occorre leggere la versione direttamente dal dispositivo, richiedi il riscontro al tecnico autorizzato.

Verifica che siano registrati modello esatto e versione firmware e che qualcuno sia incaricato di controllare gli avvisi di sicurezza pertinenti.

Per gli aggiornamenti non applicati, verifica se esistono una valutazione, una motivazione e un'azione pianificata.

Evidenza da annotare: Registro delle versioni, ultimo riscontro del manutentore o avviso del produttore con relativa valutazione.

Se emergono lacune: Richiedi le informazioni mancanti e assegna la verifica degli avvisi a un responsabile. Gli aggiornamenti devono essere valutati rispetto a compatibilità, continuità operativa e possibilità di ripristino, quindi pianificati con il fornitore.

La presenza di una versione precedente non dimostra, da sola, che il dispositivo sia vulnerabile. La disponibilità di una versione più recente non autorizza un aggiornamento immediato.

1.3 Sistemi operativi non più supportati

Domanda di controllo: Sono identificati i sistemi di produzione il cui sistema operativo non riceve più aggiornamenti di sicurezza nell'ambito del supporto effettivamente disponibile?

Conseguenze operative: La mancanza di supporto può limitare le opzioni di correzione e ripristino, aumentando la dipendenza da componenti e competenze difficili da reperire.

Come verificarlo: Richiedi l'elenco dei sistemi operativi dei PC industriali e dei server OT, indicando versione ed edizione esatte. Verifica con IT e fornitore lo stato del supporto, comprese eventuali coperture estese.

Per ogni sistema non più supportato, controlla che siano documentati:

- funzione produttiva e software da cui dipende;
- collegamenti necessari e possibilità di accesso remoto;
- misure adottate per ridurre l'esposizione;
- piano di sostituzione o motivazione del mantenimento;
- disponibilità di backup e procedura di ripristino.

Evidenza da annotare: Elenco dei sistemi interessati e relativo piano di gestione.

Se emergono lacune: Richiedi una valutazione congiunta a IT, manutenzione e fornitore. Non aggiornare il sistema operativo, disabilitare servizi o cambiare collegamenti senza verificare le dipendenze della macchina.

Un sistema datato non è automaticamente compromesso, ma richiede una gestione consapevole e documentata.

1.4 Dispositivi di rete e responsabilità di gestione

Domanda di controllo: Switch, router, firewall, access point e gateway dell'ambiente produttivo sono censiti ed è chiaro chi li gestisce?

Conseguenze operative: Un apparato senza un responsabile identificato può ritardare gli interventi e il recupero delle comunicazioni necessarie a una o più linee.

Come verificarlo: Consulta lo schema di rete e l'inventario insieme al referente IT. Per ciascun apparato verifica la disponibilità di modello, ubicazione, funzione, versione firmware e responsabile della gestione.

Richiedi inoltre conferma documentata che gli accessi amministrativi siano gestiti e che le eventuali credenziali iniziali del produttore siano state sostituite, ove previsto e tecnicamente possibile. Non provare password per eseguire questo controllo.

Evidenza da annotare: Schema di rete aggiornato, elenco degli apparati e riferimento alla verifica degli accessi amministrativi. Non riportare password nella checklist.

Se emergono lacune: Identifica il soggetto che gestisce ciascun apparato, soprattutto quando è stato installato da un fornitore esterno. Pianifica con lui la verifica delle configurazioni e delle eventuali carenze.

Le modifiche alla rete richiedono la valutazione delle comunicazioni necessarie alla produzione.

1.5 Software industriali licenze e assistenza

Domanda di controllo: Esiste un elenco dei software necessari alla produzione, con versioni, stato del supporto e informazioni utili al loro ripristino?

Conseguenze operative: L'assenza di installatori, licenze recuperabili o riferimenti di assistenza può impedire la riattivazione del software anche dopo la sostituzione dell'hardware guasto.

Come verificarlo: Consulta gli inventari IT, la documentazione delle macchine e i contratti di assistenza. Considera software di supervisione SCADA, progetti HMI, strumenti di programmazione, database, applicazioni di produzione e componenti necessari al loro funzionamento.

Per i software critici verifica che siano noti:

- nome, versione e sistema su cui sono installati;
- produttore e referente di assistenza;
- stato del supporto;
- disponibilità di installatori, configurazioni e modalità di recupero delle licenze;
- eventuali vincoli di compatibilità o dipendenze da hardware specifico.

Evidenza da annotare: Inventario software e riferimento alla documentazione di assistenza e ripristino. Non inserire chiavi di licenza o altri segreti nella checklist.

Se emergono lacune: Completa prima le informazioni sui software la cui indisponibilità fermerebbe una linea. Verifica con il fornitore le opzioni disponibili per i prodotti non più supportati e documenta come recuperarli in caso di guasto.

Riepilogo della sezione 1

Esiti: Sì / Parzialmente / No / Non verificato / Non applicabile. Motiva le esclusioni e annota data e riferimento delle evidenze.

Controllo	Esito	Evidenza o informazione mancante	Referente / data prevista
1.1 Inventario dispositivi	<input type="text"/>	<input type="text"/>	Referente <input type="text"/> Data prevista <input type="text"/>
1.2 Firmware e avvisi di sicurezza	<input type="text"/>	<input type="text"/>	Referente <input type="text"/> Data prevista <input type="text"/>
1.3 Sistemi operativi e supporto	<input type="text"/>	<input type="text"/>	Referente <input type="text"/> Data prevista <input type="text"/>
1.4 Apparati di rete e gestione	<input type="text"/>	<input type="text"/>	Referente <input type="text"/> Data prevista <input type="text"/>
1.5 Software licenze e assistenza	<input type="text"/>	<input type="text"/>	Referente <input type="text"/> Data prevista <input type="text"/>

Come usare i risultati

Non sommare le risposte per stabilire se l'impianto è sicuro. Questa sezione misura quanto conosci i sistemi che sostengono la produzione.

Dai precedenza alle informazioni mancanti sui dispositivi che possono fermare una linea, sugli apparati con collegamenti verso l'esterno e sui sistemi per i quali non è chiaro chi possa intervenire o come ripristinarli.

Per ogni lacuna assegna un referente e una data di approfondimento. Se un'informazione non è disponibile, registra "Non verificato": rendere visibile un'incertezza è già un risultato utile.

Riservatezza: conserva la checklist compilata e i relativi inventari come documentazione interna. Per un primo contatto con RILABS è sufficiente descrivere le aree da approfondire, senza inviare password, indirizzi di rete o schemi dettagliati dell'impianto.

2 Separazione delle reti e controllo dei collegamenti

Un problema sulla rete degli uffici può raggiungere i sistemi di produzione?

La segmentazione serve a limitare le comunicazioni tra ambienti con funzioni e necessità diverse. Aiuta a contenere gli effetti di un incidente, consentendo comunque i collegamenti necessari al lavoro.

Separare le reti non significa necessariamente scollegarle: un gestionale può aver bisogno di scambiare dati con la produzione e un manutentore può dover accedere a una macchina. Questi collegamenti devono essere conosciuti, autorizzati e limitati.

Chi coinvolgere: referente IT, responsabile della manutenzione, gestore della rete ed eventuali fornitori di teleassistenza.

Come svolgere i controlli: consulta schemi, configurazioni documentate e procedure insieme ai responsabili. Non collegare dispositivi a porte di rete per fare prove, non eseguire scansioni e non modificare VLAN, firewall o accessi remoti durante la compilazione.

Usa gli esiti della sezione precedente: **Sì / Parzialmente / No / Non verificato / Non applicabile**. Annota sempre l'evidenza e il perimetro esaminato. Se la configurazione non è comprensibile o disponibile, registra "Non verificato".

2.1 Separazione tra rete aziendale e rete di produzione

Domanda di controllo: La rete degli uffici e i sistemi di produzione appartengono ad ambienti distinti, con comunicazioni consentite solo dove necessario?

Conseguenze operative: Collegamenti non controllati possono consentire a un problema della rete degli uffici di coinvolgere supervisione e produzione, ampliando l'interruzione operativa.

Come verificarlo: Richiedi uno schema aggiornato che mostri rete IT, rete OT e punti di collegamento. Chiedi al gestore di indicare:

- dove avviene la separazione;
- quali dispositivi controllano il traffico tra gli ambienti;
- quali comunicazioni sono autorizzate e per quale motivo;
- eventuali percorsi alternativi, come PC con più collegamenti di rete o router installati dai fornitori.

Non dedurre la qualità della separazione dal nome delle reti, dagli indirizzi IP o dalla sola presenza di switch distinti. Anche una prova di ping, da sola, non dimostra che le comunicazioni siano correttamente limitate.

Evidenza da annotare: Schema di rete e riferimento alle regole che controllano i collegamenti IT/OT, con data e responsabile della verifica.

Se emergono lacune: Richiedi una revisione dell'architettura, partendo dalle comunicazioni indispensabili. Le modifiche devono essere pianificate con produzione e manutenzione, prevedendo verifiche e possibilità di ripristino.

2.2 Separazione interna degli ambienti produttivi

Domanda di controllo: All'interno della rete OT esistono zone distinte, definite in base a funzione, criticità e necessità di comunicazione?

Conseguenze operative: Una rete OT priva di separazioni adeguate può estendere gli effetti di un incidente da una cella ad altre linee, rendendo più difficile contenerlo.

Come verificarlo: Chiedi al gestore come sono raggruppati linee, celle produttive, postazioni di programmazione e sistemi di supervisione.

Verifica che la suddivisione abbia una motivazione documentata e che le comunicazioni tra le zone siano limitate. La presenza di più VLAN non è sufficiente se il traffico può passare liberamente dall'una all'altra.

Non è necessario assegnare automaticamente una VLAN a ogni macchina: la suddivisione deve rispettare le dipendenze del processo.

Evidenza da annotare: Schema delle zone produttive e descrizione dei collegamenti consentiti tra esse.

Se emergono lacune: Individua con i responsabili quali sistemi richiedono maggiore protezione e quali comunicazioni devono essere mantenute. Non spostare apparati tra VLAN senza aver verificato le conseguenze operative.

2.3 Regole di comunicazione tra IT e OT

Domanda di controllo: Le comunicazioni tra rete aziendale e produzione sono governate da regole specifiche, documentate e periodicamente riesaminate?

Conseguenze operative: Regole eccessivamente ampie possono consentire comunicazioni non necessarie verso la produzione; regole prive di documentazione rendono più rischiosa la loro revisione.

Come verificarlo: Richiedi al gestore una revisione delle regole del firewall o degli altri dispositivi che filtrano il traffico.

Verifica che per i collegamenti autorizzati siano identificabili:

- origine e destinazione;
- servizio o protocollo necessario;
- motivazione operativa;
- responsabile dell'autorizzazione;
- eventuale scadenza, se il collegamento è temporaneo.

Chiedi se il traffico non espressamente autorizzato viene bloccato e se esistono regole eccessivamente ampie o eccezioni rimaste attive dopo interventi di manutenzione.

Evidenza da annotare: Riferimento alla revisione delle regole, data, responsabile ed eventuali eccezioni da approfondire.

Se emergono lacune: Assegna la revisione al gestore della rete. Prima di restringere una regola, verifica quali servizi la utilizzano e concorda modalità di intervento e ripristino.

Non provare a raggiungere porte o servizi dei PLC per compilare questo controllo.

2.4 Sistemi intermedi per lo scambio di dati IT OT

Domanda di controllo: I sistemi che consentono scambi di dati o accessi tra IT e OT sono collocati e configurati per evitare collegamenti non controllati?

Conseguenze operative: Percorsi che aggirano i controlli possono esporre i sistemi produttivi attraverso servizi condivisi, compromettendo anche l'affidabilità degli scambi di dati.

Una **DMZ industriale** è una zona di rete intermedia in cui possono risiedere servizi di scambio dati o di accesso, protetti da regole verso entrambi gli ambienti.

Come verificarlo: Identifica con il gestore i sistemi coinvolti: raccolta dati di produzione, trasferimento file, aggiornamenti, accesso remoto e altri servizi condivisi.

Verifica:

- quali sistemi si trovano in una zona intermedia e perché;
- quali collegamenti sono ammessi da ciascun lato;
- se esistono computer con interfacce collegate a reti diverse;
- come vengono impediti percorsi che aggirano i controlli previsti.

La presenza di due schede di rete non dimostra, da sola, che un server sia un ponte; richiede però una verifica della configurazione e degli accessi.

Evidenza da annotare: Schema dei servizi intermedi e valutazione dei percorsi tra IT e OT.

Se emergono lacune: Richiedi una verifica architetturale. La necessità e la configurazione della DMZ devono essere valutate rispetto ai flussi effettivi: non tutti i server industriali devono essere spostati nella zona intermedia.

2.5 Accesso remoto e teleassistenza

Domanda di controllo: Tutti i collegamenti remoti alla produzione sono conosciuti, autorizzati, limitati e revocabili?

Conseguenze operative: Accessi remoti non controllati possono permettere interventi non autorizzati su macchine e configurazioni, con conseguenze sulla disponibilità e sulla qualità del processo.

Come verificarlo: Richiedi l'elenco delle modalità di accesso usate da personale interno, manutentori e fornitori. Includi VPN, software di controllo remoto, gateway del costruttore e router con connessione mobile.

Per ciascuna modalità verifica:

- chi può accedere e con quale identità;
- come viene approvato e, quando previsto, attivato l'accesso;
- quali sistemi sono raggiungibili;
- se viene utilizzata l'autenticazione a più fattori sul punto di accesso;
- quali eventi vengono registrati e chi li controlla;
- come vengono disabilitati gli accessi non più necessari.

Eventuali limiti tecnici devono essere documentati insieme alle misure alternative adottate.

Il nome del prodotto non basta per giudicare la sicurezza del collegamento: conta come viene configurato e gestito.

Evidenza da annotare: Elenco degli accessi remoti, procedura di autorizzazione e riferimento a una verifica recente delle utenze.

Se emergono lacune: Fai valutare con priorità gli accessi sconosciuti, non più necessari o privi di un responsabile. Concorda gli interventi con chi gestisce la macchina, evitando di interrompere una teleassistenza essenziale senza un'alternativa.

2.6 Reti Wi Fi in stabilimento

Domanda di controllo: Le reti Wi-Fi per ospiti, personale e produzione hanno accessi separati e coerenti con le rispettive necessità?

Conseguenze operative: Una rete wireless non adeguatamente separata può offrire un accesso indesiderato ai sistemi produttivi; modifiche improvvisate possono interrompere terminali e servizi di reparto.

Come verificarlo: Richiedi al gestore l'elenco delle reti wireless e delle relative configurazioni.

Verifica che:

- gli ospiti non possano accedere alle reti interne;
- i dispositivi aziendali raggiungano solo i servizi necessari;
- scanner, terminali e altri dispositivi wireless di produzione abbiano collegamenti limitati alla loro funzione;
- autenticazione e protezione delle comunicazioni siano adeguate ai dispositivi utilizzati;
- eventuali credenziali condivise abbiano un responsabile e modalità definite di sostituzione e revoca.

Nomi Wi-Fi differenti non dimostrano che le reti siano separate.

Evidenza da annotare: Elenco delle reti wireless e conferma documentata delle restrizioni applicate.

Se emergono lacune: Richiedi la revisione delle configurazioni. Prima di modificare autenticazione o credenziali, verifica la compatibilità dei terminali industriali e pianifica la riconnessione dei dispositivi interessati.

2.7 Collegamento di dispositivi personali o non autorizzati

Domanda di controllo: Esistono regole e misure per impedire il collegamento non autorizzato di dispositivi alla rete di produzione?

Conseguenze operative: Dispositivi non autorizzati possono introdurre software dannoso o collegamenti imprevisti, alterando le comunicazioni e rendendo più difficile ricostruire l'origine di un problema.

Come verificarlo: Consulta la procedura aziendale e chiedi come vengono gestiti:

- computer personali e dispositivi mobili;
- laptop dei manutentori;
- apparati temporanei usati per diagnosi o installazioni;
- porte di rete accessibili nelle aree produttive;
- accessi wireless alla produzione.

Verifica chi autorizza il collegamento, quali requisiti deve rispettare il dispositivo e come viene registrata o rimossa un'autorizzazione temporanea.

Il controllo riguarda qui l'accesso alla rete. La gestione delle periferiche USB viene affrontata nella sezione dedicata alla protezione dei sistemi.

Evidenza da annotare: Procedura di collegamento dei dispositivi ed esempio di autorizzazione o verifica recente.

Se emergono lacune: Definisci con IT e manutenzione un percorso di accesso per i dispositivi autorizzati. Valuta controlli tecnici compatibili con l'impianto, senza attivare blocchi indiscriminati che possano escludere apparati necessari.

Riepilogo della sezione 2

Esiti: Sì / Parzialmente / No / Non verificato / Non applicabile. Motiva le esclusioni e annota data e riferimento delle evidenze.

Controllo	Esito	Evidenza o informazione mancante	Referente / data prevista
2.1 Separazione IT/OT	<input type="text"/>	<input type="text"/>	Referente <input type="text"/> Data prevista <input type="text"/>
2.2 Zone interne alla produzione	<input type="text"/>	<input type="text"/>	Referente <input type="text"/> Data prevista <input type="text"/>
2.3 Regole di comunicazione	<input type="text"/>	<input type="text"/>	Referente <input type="text"/> Data prevista <input type="text"/>
2.4 Sistemi intermedi e DMZ	<input type="text"/>	<input type="text"/>	Referente <input type="text"/> Data prevista <input type="text"/>
2.5 Accessi remoti	<input type="text"/>	<input type="text"/>	Referente <input type="text"/> Data prevista <input type="text"/>
2.6 Reti Wi-Fi	<input type="text"/>	<input type="text"/>	Referente <input type="text"/> Data prevista <input type="text"/>
2.7 Dispositivi non autorizzati	<input type="text"/>	<input type="text"/>	Referente <input type="text"/> Data prevista <input type="text"/>

Come usare i risultati

Questa sezione verifica se la separazione delle reti e i collegamenti sono documentati e gestiti. Non dimostra, da sola, che le restrizioni siano efficaci contro un attacco.

Richiedono particolare attenzione gli accessi remoti senza un responsabile, le comunicazioni IT/OT prive di limitazioni e i collegamenti che aggirano i punti di controllo previsti.

Per ogni lacuna assegna un referente e una data di approfondimento. Se occorre verificare tecnicamente l'efficacia della segmentazione, pianifica un'attività dedicata con perimetro, autorizzazioni, modalità operative e criteri di interruzione concordati con la produzione.

3 Protezione dei sistemi industriali

I sistemi che sostengono la produzione sono configurati per ridurre gli accessi e le operazioni non necessari?

PC industriali, pannelli operatore HMI e server di supervisione possono avere configurazioni rimaste invariate dall'installazione. Account iniziali, servizi inutilizzati o protezioni non gestite possono aumentare l'esposizione dell'impianto.

Questa sezione riguarda l'**hardening**: la configurazione dei sistemi per limitarne le possibilità di uso improprio, mantenendo le funzionalità necessarie alla produzione.

Chi coinvolgere: referente IT, manutenzione, gestore dei sistemi e fornitore del software o della macchina.

Come svolgere i controlli: consulta configurazioni documentate, rapporti di manutenzione e informazioni delle console di gestione. Gli eventuali riscontri sui dispositivi devono essere eseguiti dal personale autorizzato. Non installare programmi, introdurre file di test antivirus, provare credenziali o modificare impostazioni durante la compilazione.

Usa gli esiti **Sì / Parzialmente / No / Non verificato / Non applicabile**. Le eccezioni devono essere motivate e accompagnate dalle misure adottate per gestirle.

3.1 Credenziali iniziali e account dei dispositivi

Domanda di controllo: Le credenziali iniziali dei dispositivi sono state gestite e gli account presenti hanno una funzione e un responsabile identificabili?

Conseguenze operative: Credenziali iniziali o accessi non governati possono consentire modifiche non autorizzate a parametri e programmi, con possibili scarti o interruzioni della lavorazione.

Come verificarlo: Richiedi al gestore una verifica degli account di HMI, PC industriali e sistemi di supervisione.

Controlla che siano documentati:

- sostituzione delle password iniziali, quando prevista e tecnicamente possibile;
- gestione degli account di installazione, assistenza e amministrazione;
- disabilitazione degli account non necessari, dopo verifica delle dipendenze;
- custodia delle credenziali e accesso riservato alle persone autorizzate;
- eventuali account non modificabili e relative misure di protezione.

Non chiedere agli operatori di comunicarti le password e non riportarle nella checklist.

Evidenza da annotare: Data e responsabile dell'ultima revisione degli account, sistemi coperti ed eventuali eccezioni.

Se emergono lacune: Assegna la revisione al gestore. Prima di cambiare una password, verifica se viene utilizzata anche da servizi, applicazioni o collegamenti automatici. Pianifica l'aggiornamento di tutte le dipendenze interessate.

3.2 Servizi e funzionalità non necessari

Domanda di controllo: I servizi attivi sui sistemi industriali sono conosciuti e limitati a quelli necessari al funzionamento, alla gestione o alla manutenzione?

Conseguenze operative: Funzionalità non necessarie possono offrire ulteriori punti di accesso ai sistemi e complicarne manutenzione e diagnosi.

Come verificarlo: Richiedi al gestore una revisione delle configurazioni, basata sulle funzioni effettive della macchina e sulle indicazioni del fornitore.

Considera servizi di accesso remoto, condivisione file, trasferimento dati, gestione web e database.

Verifica che:

- ogni servizio necessario abbia una funzione identificata;
- l'accesso sia limitato agli utenti e ai sistemi che ne hanno bisogno;
- eventuali protocolli obsoleti o privi di cifratura siano censiti;
- le eccezioni abbiano una motivazione e protezioni aggiuntive documentate.

La presenza di un servizio non dimostra, da sola, una vulnerabilità. Occorre valutarne versione, configurazione, esposizione e utilizzo.

Evidenza da annotare: Riferimento alla configurazione approvata o alla revisione dei servizi, con le eccezioni rilevate.

Se emergono lacune: Richiedi una valutazione tecnica. Non disabilitare servizi o protocolli prima di aver verificato se sono necessari alla comunicazione con macchine, applicazioni o strumenti di manutenzione.

3.3 Protezione da software dannoso e non autorizzato

Domanda di controllo: I sistemi dispongono di protezioni contro software dannoso o non autorizzato, compatibili con il loro utilizzo industriale?

Conseguenze operative: Software dannoso o non previsto può rendere indisponibili postazioni e applicazioni di linea oppure alterare i dati utilizzati dal processo.

Come verificarlo: Chiedi al gestore quali protezioni sono previste per ciascuna categoria di sistema: antivirus, protezione degli endpoint, controllo delle applicazioni eseguibili o altre misure.

Verifica attraverso le console di gestione o i rapporti disponibili:

- quali sistemi sono coperti;
- se le protezioni previste risultano attive e aggiornate;
- chi riceve e gestisce le segnalazioni;
- quali esclusioni sono configurate e perché;
- come sono gestiti i dispositivi sui quali non è possibile installare una protezione.

Non tutti gli apparati consentono l'installazione di un antivirus. L'assenza deve essere valutata rispetto alle caratteristiche del dispositivo e alle altre misure adottate.

Evidenza da annotare: Rapporto sullo stato delle protezioni, data della verifica, sistemi esclusi e relative motivazioni.

Se emergono lacune: Fai verificare configurazione e compatibilità con il fornitore. Evita installazioni autonome, esclusioni generalizzate o riattivazioni non concordate.

Gli eventuali test delle protezioni devono essere pianificati separatamente, considerando anche le risposte automatiche che potrebbero attivarsi.

3.4 Aggiornamenti e riavvii controllati

Domanda di controllo: Gli aggiornamenti di sicurezza dei sistemi operativi e delle applicazioni sono valutati e applicati attraverso un processo compatibile con la produzione?

Conseguenze operative: Aggiornamenti o riavvii non coordinati possono interrompere la produzione o introdurre incompatibilità; correzioni rinviate senza valutazione possono lasciare esposizioni non gestite.

Come verificarlo: Consulta il piano di manutenzione e gli ultimi rapporti di aggiornamento.

Verifica che siano definiti:

- responsabile della valutazione degli aggiornamenti;
- verifica della compatibilità con software e hardware industriali;
- modalità di prova prima dell'applicazione;
- finestra autorizzata e gestione dei riavvii;
- disponibilità di backup e procedura di ripristino;

- registrazione degli aggiornamenti rinviati e delle misure temporanee adottate.

L'obiettivo è evitare sia interventi imprevisti durante la produzione sia aggiornamenti rimandati senza valutazione.

Evidenza da annotare: Piano di aggiornamento, ultimo intervento eseguito e registro dei rinvii.

Se emergono lacune: Definisci il processo con IT, manutenzione e fornitore. Non modificare autonomamente le impostazioni di aggiornamento e non avviare riavvii per completare questo controllo.

3.5 Periferiche USB e supporti rimovibili

Domanda di controllo: L'uso di periferiche USB e supporti rimovibili sui sistemi industriali è autorizzato e controllato?

Conseguenze operative: Supporti rimovibili non gestiti possono trasferire file dannosi o versioni errate dei progetti tra macchine, anche quando le reti sono separate.

Come verificarlo: Richiedi la procedura per chiavette, dischi esterni e altri dispositivi collegabili.

Verifica che distingua i supporti di memoria dalle periferiche necessarie alla macchina, come tastiere, adattatori e chiavi hardware di licenza.

Controlla che siano definiti:

- dispositivi consentiti e persone autorizzate;
- modalità di verifica dei supporti prima dell'utilizzo;
- gestione dei supporti introdotti dai manutentori;
- custodia e impiego dei supporti dedicati;
- eventuali limitazioni tecniche o protezioni fisiche sulle porte non necessarie.

Non inserire una chiavetta per verificare se viene riconosciuta.

Evidenza da annotare: Procedura sui supporti rimovibili e riferimento alle restrizioni applicate.

Se emergono lacune: Concorda misure compatibili con le esigenze di manutenzione. Prima di bloccare una porta o una categoria di dispositivi, verifica che non serva a componenti indispensabili.

3.6 Avvio automatico dei contenuti rimovibili

Domanda di controllo: Sui sistemi Windows applicabili sono definite e verificate le impostazioni che limitano l'avvio automatico dei contenuti provenienti da supporti rimovibili?

Conseguenze operative: L'esecuzione automatica di contenuti può avviare programmi indesiderati al collegamento di un supporto, interferendo con il funzionamento della postazione.

Come verificarlo: Richiedi al gestore una verifica delle impostazioni effettivamente applicate per **AutoPlay** e **AutoRun**, tenendo conto della versione di Windows.

Verifica che:

- esista una configurazione aziendale di riferimento;
- sia stata controllata la sua applicazione sui sistemi interessati;
- eventuali eccezioni siano motivate;
- il controllo sia coordinato con le restrizioni sui supporti rimovibili.

La comparsa o l'assenza di una finestra dopo l'inserimento di una chiavetta non costituisce, da sola, una verifica sufficiente.

Evidenza da annotare: Riferimento alla configurazione applicata e data dell'ultimo controllo.

Se emergono lacune: Richiedi la revisione delle impostazioni al gestore. Le eventuali modifiche e i riavvii necessari devono essere pianificati.

Questo controllo non sostituisce la gestione degli aggiornamenti e delle periferiche autorizzate.

3.7 Credenziali nelle configurazioni e negli script

Domanda di controllo: Le credenziali utilizzate da software e servizi industriali sono custodite con modalità appropriate e accessibili solo ai soggetti necessari?

Conseguenze operative: Credenziali esposte in file o script possono consentire accessi ad altri sistemi; la loro modifica senza conoscere le dipendenze può interrompere servizi di produzione.

Come verificarlo: Chiedi al gestore delle applicazioni come vengono conservate le credenziali usate per database, servizi e collegamenti tra sistemi.

Verifica che siano stati esaminati:

- file di configurazione e script che possono contenere segreti;
- permessi di accesso a tali file e alle loro copie di backup;
- privilegi degli account utilizzati dalle applicazioni;
- possibilità di adottare meccanismi di custodia supportati dal software;
- modalità di sostituzione delle credenziali in caso di necessità.

Non cercare né copiare password per compilare la checklist. Richiedi un riscontro sull'esito della verifica, senza acquisire i segreti.

Evidenza da annotare: Riferimento alla revisione, applicazioni esaminate ed eventuali limitazioni documentate.

Se emergono lacune: Fai valutare la soluzione al gestore e al fornitore. Se l'applicazione richiede credenziali in un file, limita gli accessi e i privilegi associati, documentando il vincolo.

Non cancellare o sostituire credenziali senza verificare le dipendenze del servizio.

3.8 Registrazione degli eventi di sicurezza

Domanda di controllo: I sistemi industriali registrano gli eventi utili a riconoscere accessi impropri, modifiche e anomalie, nei limiti delle loro capacità?

Conseguenze operative: Eventi non registrati possono rendere difficile capire chi ha modificato un sistema e quando, rallentando diagnosi, contenimento e ripristino.

Come verificarlo: Richiedi al gestore un riscontro sulla registrazione degli eventi pertinenti, per esempio:

- accessi riusciti e falliti;
- creazione di utenti e modifiche ai privilegi;
- cambiamenti delle configurazioni;
- modifiche ai progetti o alla logica di controllo, quando tracciabili;
- arresti o anomalie dei servizi di sicurezza.

Verifica che gli orari siano coerenti, lo spazio disponibile sia gestito e le registrazioni siano accessibili solo al personale autorizzato.

Se un dispositivo non produce questi eventi, chiedi quali informazioni alternative siano disponibili, per esempio dai sistemi di accesso remoto o di supervisione.

Evidenza da annotare: Elenco delle sorgenti di log, tipi di eventi registrati e data di una verifica recente.

Se emergono lacune: Definisci gli eventi necessari con IT e manutenzione. Valuta l'impatto delle impostazioni di registrazione prima di modificarle, soprattutto sui dispositivi con risorse limitate.

Raccolta centralizzata, tempi di conservazione e gestione degli avvisi vengono approfonditi nella sezione dedicata al monitoraggio.

3.9 Protezione fisica dei sistemi e delle connessioni OT

Domanda di controllo: L'accesso fisico a quadri di controllo, armadi di rete, server OT e connessioni di reparto è limitato alle persone autorizzate?

Conseguenze operative: Accessi fisici non controllati possono consentire collegamenti, manomissioni o disconnessioni che alterano il processo o interrompono le comunicazioni di linea.

Come verificarlo: Consulta le procedure e richiedi un riscontro al personale autorizzato su:

- chiusura di quadri e armadi quando non occorre accedervi per esigenze operative o di sicurezza;
- custodia delle chiavi, assegnazione dei badge e revoca delle autorizzazioni non più necessarie;
- controllo degli accessi ai locali che ospitano server e apparati OT;
- identificazione delle prese e delle porte di rete accessibili, con protezioni fisiche o limitazioni tecniche coerenti con il loro utilizzo;
- autorizzazione e accompagnamento dei visitatori e dei tecnici esterni, secondo il perimetro;
- gestione delle eccezioni e degli accessi di emergenza.

Una serratura non è una protezione efficace se la chiave è liberamente disponibile. Le misure devono consentire le attività autorizzate e non ostacolare le procedure di emergenza.

Evidenza da annotare: Procedura di accesso, riferimento al registro delle autorizzazioni e riscontro del responsabile sulle aree esaminate. Non riportare codici di accesso o dettagli utili ad aggirare le protezioni.

Se emergono lacune: Concorda gli interventi con manutenzione, IT e responsabili della sicurezza dell'impianto. Per le porte inutilizzate valuta la disabilitazione o una protezione adeguata, dopo averne accertato funzione e dipendenze.

Non aprire quadri elettrici, collegare dispositivi o disabilitare porte durante la compilazione. Richiama i controlli 2.7 e 5.5 per dispositivi e interventi dei fornitori.

Riepilogo della sezione 3

Esiti: Sì / Parzialmente / No / Non verificato / Non applicabile. Motiva le esclusioni e annota data e riferimento delle evidenze.

Controllo	Esito	Evidenza o informazione mancante	Referente / data prevista
3.1 Credenziali iniziali e account	<input type="text"/>	<input type="text"/>	Referente <input type="text"/> Data prevista <input type="text"/>
3.2 Servizi necessari e autorizzati	<input type="text"/>	<input type="text"/>	Referente <input type="text"/> Data prevista <input type="text"/>
3.3 Protezione dal software dannoso	<input type="text"/>	<input type="text"/>	Referente <input type="text"/> Data prevista <input type="text"/>
3.4 Aggiornamenti e riavvii	<input type="text"/>	<input type="text"/>	Referente <input type="text"/> Data prevista <input type="text"/>
3.5 USB e supporti rimovibili	<input type="text"/>	<input type="text"/>	Referente <input type="text"/> Data prevista <input type="text"/>
3.6 AutoPlay e AutoRun	<input type="text"/>	<input type="text"/>	Referente <input type="text"/> Data prevista <input type="text"/>
3.7 Custodia delle credenziali applicative	<input type="text"/>	<input type="text"/>	Referente <input type="text"/> Data prevista <input type="text"/>
3.8 Registrazione degli eventi	<input type="text"/>	<input type="text"/>	Referente <input type="text"/> Data prevista <input type="text"/>
3.9 Protezione fisica	<input type="text"/>	<input type="text"/>	Referente <input type="text"/> Data prevista <input type="text"/>

Come usare i risultati

Dai precedenza alle carenze che riguardano sistemi essenziali alla produzione, soprattutto quando sono raggiungibili da altre reti o attraverso accessi remoti.

Credenziali iniziali ancora utilizzabili, protezioni disattivate senza valutazione e servizi esposti senza una necessità documentata richiedono un approfondimento prioritario. La priorità della verifica non equivale all'autorizzazione a modificare immediatamente il sistema.

Per ogni intervento individua responsabile, dipendenze, modalità di prova e ripristino. Una carenza può essere considerata risolta solo dopo aver verificato sia l'efficacia della misura sia il corretto funzionamento delle attività produttive interessate.

4 Backup e ripristino della produzione

Se un sistema diventasse inutilizzabile, avresti ciò che serve per ripartire?

Un backup è utile quando contiene le informazioni necessarie, è disponibile al momento del bisogno e può essere ripristinato con strumenti e competenze accessibili.

In produzione non basta recuperare i documenti. Possono servire programmi dei controllori, configurazioni, ricette, database, software, licenze e componenti hardware compatibili. Anche l'ordine delle operazioni può influire sulla ripartenza.

Questa sezione aiuta a verificare se l'azienda dispone di copie adeguate e di un percorso di ripristino documentato e provato.

Chi coinvolgere: referente IT, responsabile della produzione, manutenzione, integratore e fornitori dei sistemi critici.

Come svolgere i controlli: consulta registri dei backup, procedure e rapporti dei test già eseguiti. Non avviare esportazioni dai controllori, ripristini o prove sulle macchine operative per compilare la checklist. Le attività tecniche devono essere pianificate separatamente.

Usa gli esiti **Sì** / **Parzialmente** / **No** / **Non verificato** / **Non applicabile**. Se esiste una copia ma non è noto se sia utilizzabile, indica questa incertezza.

4.1 Programmi e configurazioni dei controllori

Domanda di controllo: Sono disponibili copie aggiornate dei programmi e delle configurazioni necessari a ripristinare PLC e altri controllori essenziali alla produzione?

Conseguenze operative: Senza una copia recuperabile dei programmi e delle configurazioni, sostituire un controllore guasto può non bastare a far ripartire la macchina.

Come verificarlo: Richiedi alla manutenzione o all'integratore l'elenco delle copie disponibili per le macchine comprese nel perimetro.

Verifica che per ciascun sistema siano noti:

- macchina e controllore a cui si riferisce la copia;
- versione e data dell'ultima modifica approvata;
- contenuti necessari al ripristino, comprese configurazioni e parametri pertinenti;
- software, versioni e strumenti richiesti per utilizzare la copia;
- luogo di conservazione e persone autorizzate ad accedervi;
- disponibilità del progetto e dell'assistenza, anche se gestiti dal fornitore.

La data del file, da sola, non dimostra che la copia corrisponda alla configurazione in uso. Chiedi come viene verificata questa corrispondenza.

Evidenza da annotare: Registro delle copie, riferimento all'ultima modifica approvata e responsabile della verifica.

Se emergono lacune: Concorda con il fornitore il recupero o la creazione delle copie mancanti. Verifica quali informazioni possono essere recuperate dal controllore: una lettura del dispositivo non equivale necessariamente al progetto completo necessario per manutenzione e ripristino.

Prevedi l'aggiornamento delle copie dopo le modifiche approvate e la conservazione delle versioni precedenti utili.

4.2 Progetti HMI supervisione e dati di produzione

Domanda di controllo: Sono protetti da backup i progetti delle interfacce operatore e della supervisione, insieme ai dati necessari alla ripartenza e alla continuità delle attività?

Conseguenze operative: La perdita di progetti, ricette o dati può impedire la supervisione, richiedere una ricostruzione manuale e compromettere la tracciabilità dei lotti.

Come verificarlo: Identifica con i responsabili i contenuti da recuperare in caso di perdita, considerando:

- progetti e configurazioni HMI e SCADA;
- ricette e parametri di produzione;
- database, dati storici e informazioni di tracciabilità;
- configurazioni dei collegamenti tra sistemi;
- certificati o altri elementi necessari al funzionamento, dove applicabili.

Verifica che la procedura distingua i contenuti inclusi nel backup da quelli che richiedono copie separate. Non presumere che il backup di un'applicazione comprenda anche database esterni, licenze e tutti i dati associati.

Chiedi inoltre come viene garantita la coerenza delle copie dei database e come viene scelta la frequenza di salvataggio.

Evidenza da annotare: Elenco dei contenuti coperti, procedure utilizzate e rapporto dell'ultima esecuzione.

Se emergono lacune: Completa il piano con il gestore delle applicazioni. Definisci la frequenza in base alla quantità di dati che l'azienda può permettersi di perdere e alla frequenza delle modifiche, anziché adottare un intervallo uguale per tutti i sistemi.

4.3 Backup dei sistemi e protezione delle copie

Domanda di controllo: Esistono copie sufficienti a ricostruire i PC industriali e i server critici, protette anche da incidenti che coinvolgano i sistemi originali?

Conseguenze operative: Copie incomplete o esposte allo stesso evento dei sistemi originali possono lasciare l'azienda senza una via di recupero utilizzabile.

Come verificarlo: Richiedi il piano di backup e verifica che comprenda, secondo le esigenze del sistema, immagini dei dischi oppure procedure di reinstallazione complete di software, configurazioni, dati, driver e modalità di recupero delle licenze.

Controlla inoltre:

- esito delle esecuzioni e gestione degli errori;
- presenza di copie separate dai sistemi originali;
- protezione degli accessi amministrativi ai backup;
- disponibilità di almeno una copia offline o con protezioni di immutabilità adeguate;
- conservazione di copie in un luogo distinto, rispetto a eventi che possano colpire lo stabilimento;
- disponibilità protetta delle chiavi e delle credenziali necessarie al recupero.

La regola **3-2-1** indica tre copie dei dati, su due tipi di supporto, con una copia fuori sede. La protezione offline o immutabile aggiunge una difesa contro alterazione e cancellazione: "fuori sede" e "offline" non significano la stessa cosa.

Evidenza da annotare: Piano di backup, rapporto delle esecuzioni e descrizione delle protezioni delle copie, senza riportare credenziali o chiavi.

Se emergono lacune: Valuta se un singolo incidente o account compromesso potrebbe rendere inutilizzabili tutte le copie. Assegna la correzione al gestore dei backup, includendo le modalità di accesso durante un'emergenza.

Un disco sempre collegato al sistema originale o una cartella sincronizzata non costituiscono, da soli, una protezione sufficiente.

4.4 Obiettivi di ripristino e perdita di dati tollerabile

Domanda di controllo: Produzione e IT hanno concordato quanto rapidamente devono essere ripristinate le attività critiche e quanti dati è accettabile perdere?

Conseguenze operative: Obiettivi di ripristino non concordati possono produrre soluzioni di backup incompatibili con il fermo e la perdita di dati che la produzione può tollerare.

Come verificarlo: Per ciascuna attività critica, verifica che siano definiti:

- **RTO - obiettivo di tempo di ripristino:** entro quanto tempo deve essere recuperato il servizio o processo individuato;
- **RPO - obiettivo di recupero dei dati:** quanto indietro nel tempo è accettabile tornare con i dati ripristinati.

Per esempio, un RPO di quattro ore indica che il piano deve consentire di recuperare dati con una perdita temporale non superiore a quattro ore. Non indica quanto durerà il ripristino.

Controlla che gli obiettivi considerino:

- disponibilità di hardware sostitutivo e ricambi;
- software, licenze e assistenza;
- dipendenze da rete, identità e altri servizi;
- personale necessario e sua reperibilità;
- verifiche funzionali e autorizzazione alla ripartenza.

Confronta gli obiettivi con i tempi rilevati nei test e con i punti di recupero effettivamente disponibili. Distingui sempre una stima da una misura.

Evidenza da annotare: Obiettivi approvati per le attività critiche, risultati disponibili e differenze ancora da risolvere.

Se emergono lacune: Definisci gli obiettivi con produzione e direzione, quindi verifica se il piano attuale può soddisfarli. Se non può, individua gli interventi necessari e rendi esplicito il rischio residuo.

Non ricavare l'RTO sommando semplicemente i tempi dei singoli componenti: alcune attività possono svolgersi in parallelo, altre dipendono da passaggi precedenti.

4.5 Prove di ripristino e validazione della ripartenza

Domanda di controllo: Sono state eseguite prove documentate che dimostrino la possibilità di recuperare i sistemi e le funzioni produttive comprese nel perimetro?

Conseguenze operative: Un backup mai provato può rivelarsi inutilizzabile nel momento del bisogno; una ripartenza non validata può generare lavorazioni errate o ulteriori interruzioni.

Come verificarlo: Richiedi il rapporto dell'ultimo test e verifica che riporti:

- sistemi, copie e scenario esaminati;
- ambiente utilizzato e precauzioni adottate;
- passaggi eseguiti e persone coinvolte;
- integrità dei dati e funzionamento delle applicazioni;
- tempo impiegato e punto temporale recuperato;
- problemi riscontrati e azioni correttive;
- criteri con cui è stato dichiarato riuscito il test.

L'avvio di un computer ripristinato non dimostra, da solo, che la linea possa ripartire. Devono essere considerate le funzioni e le dipendenze necessarie al processo.

Verifica anche che la procedura preveda, dopo un incidente informatico, il controllo delle copie da utilizzare e delle condizioni di sicurezza prima della riconnessione.

Evidenza da annotare: Data e riferimento del rapporto, copertura del test, risultati e azioni ancora aperte.

Se emergono lacune: Pianifica una prova in un ambiente adeguato e separato dalla produzione, evitando che i sistemi ripristinati possano inviare comandi agli impianti operativi.

Quando una prova completa non è possibile, documenta le verifiche parziali svolte e ciò che resta da dimostrare. Una simulazione organizzativa è utile, ma non sostituisce una prova tecnica di recupero.

Definisci la periodicità in base alla criticità e alle modifiche dei sistemi. Dopo un test fallito, assegna le correzioni e programma una nuova verifica.

Riepilogo della sezione 4

Esiti: Sì / Parzialmente / No / Non verificato / Non applicabile. Motiva le esclusioni e annota data e riferimento delle evidenze.

Controllo	Esito	Evidenza o informazione mancante	Referente / data prevista
4.1 Programmi e configurazioni dei controllori	<input type="text"/>	<input type="text"/>	Referente <input type="text"/> Data prevista <input type="text"/>
4.2 HMI supervisione e dati produttivi	<input type="text"/>	<input type="text"/>	Referente <input type="text"/> Data prevista <input type="text"/>
4.3 Backup dei sistemi e protezione delle copie	<input type="text"/>	<input type="text"/>	Referente <input type="text"/> Data prevista <input type="text"/>
4.4 Obiettivi RTO e RPO	<input type="text"/>	<input type="text"/>	Referente <input type="text"/> Data prevista <input type="text"/>
4.5 Prove di ripristino e ripartenza	<input type="text"/>	<input type="text"/>	Referente <input type="text"/> Data prevista <input type="text"/>

Come usare i risultati

Dai precedenza ai sistemi necessari alla produzione per i quali mancano copie utilizzabili, alle situazioni in cui tutte le copie potrebbero essere colpite dallo stesso incidente e ai ripristini mai verificati.

Non considerare “backup completato” equivalente a “produzione recuperabile”. Occorre poter accedere alle copie, disporre delle dipendenze necessarie e verificare il risultato del recupero.

Per ogni lacuna assegna un responsabile e una data. L’autorizzazione alla ripartenza deve coinvolgere chi può confermare il corretto funzionamento del processo e le condizioni di sicurezza dell’impianto.

5 Gestione degli accessi e fattore umano

Chi può intervenire sui sistemi produttivi e cosa deve fare quando qualcosa non torna?

La sicurezza dipende anche da come vengono assegnati gli accessi, gestiti i fornitori e affrontate le situazioni inattese.

Le persone devono poter svolgere il proprio lavoro con autorizzazioni appropriate e istruzioni comprensibili. Devono inoltre sapere a chi rivolgersi quando una richiesta sembra insolita o un sistema mostra un comportamento anomalo.

Questa sezione verifica se tali responsabilità sono definite e applicate, evitando di attribuire la sicurezza alla sola attenzione del singolo operatore.

Chi coinvolgere: referente IT, responsabile della produzione, manutenzione, risorse umane, amministrazione e responsabili dei fornitori interessati.

Come svolgere i controlli: consulta elenchi degli accessi, procedure, registri e materiali formativi. Puoi porre domande sulle modalità di lavoro, senza chiedere password. Non accedere con l'identità di altre persone, non modificare privilegi e non inviare messaggi ingannevoli per compilare la checklist.

Usa gli esiti **Sì** / **Parzialmente** / **No** / **Non verificato** / **Non applicabile**, indicando evidenze ed eventuali eccezioni.

5.1 Identità account condivisi e gestione delle utenze

Domanda di controllo: Gli accessi ai sistemi produttivi sono associati alle persone autorizzate e aggiornati quando cambiano ruoli, incarichi o rapporti di lavoro?

Conseguenze operative: Utenze non aggiornate possono mantenere accessi non più necessari e rendere difficile attribuire le operazioni, soprattutto nei passaggi di ruolo o di fornitore.

Come verificarlo: Richiedi al gestore una revisione delle utenze, distinguendo account personali, amministrativi, applicativi e condivisi.

Verifica che:

- ogni account abbia uno scopo e un responsabile;
- le persone utilizzino identità individuali dove tecnicamente possibile;
- creazione e modifica degli accessi richiedano un'autorizzazione;
- gli accessi vengano riesaminati e revocati quando non più necessari;
- eventuali account condivisi abbiano motivazione, privilegi limitati e modalità di utilizzo definite;
- la gestione delle credenziali sia coerente con le capacità del sistema e le esigenze operative.

Non confondere un account utilizzato da un servizio con un account personale: richiede una gestione specifica e un responsabile, ma non identifica necessariamente un operatore.

Evidenza da annotare: Riferimento alla revisione delle utenze, data, sistemi coperti ed eccezioni.

Se emergono lacune: Definisci un processo per autorizzare, aggiornare e revocare gli accessi. Per i sistemi che richiedono un account condiviso, documenta come viene controllato l'utilizzo e quali limiti di attribuzione delle operazioni rimangono.

Le modifiche devono considerare anche accessi di emergenza e continuità dei turni produttivi.

5.2 Privilegi coerenti con il ruolo

Domanda di controllo: Operatori, manutentori e amministratori dispongono dei soli permessi necessari alle rispettive attività?

Conseguenze operative: Permessi eccessivi possono trasformare un errore o un accesso compromesso in una modifica ai programmi, alle ricette o alle configurazioni della linea.

Come verificarlo: Richiedi al gestore una verifica dei ruoli e dei permessi effettivi nei sistemi operativi e nelle applicazioni industriali.

Controlla che siano distinti, ove applicabile:

- uso ordinario della macchina;
- modifica di parametri e ricette;
- modifica dei programmi di controllo;
- installazione di software;
- gestione degli utenti e delle configurazioni di sicurezza.

Verifica che gli account amministrativi siano utilizzati per le attività che li richiedono e che le eccezioni siano motivate e riesaminate.

Non installare programmi o tentare modifiche per accertare i privilegi. L'apertura di un pannello di configurazione, da sola, non dimostra la possibilità di modificarne le impostazioni.

Evidenza da annotare: Matrice dei ruoli o rapporto di revisione dei permessi, con eccezioni e responsabili.

Se emergono lacune: Valuta con il fornitore quali permessi richiede realmente il software. Prima di ridurli, verifica le funzioni interessate in condizioni controllate.

Se un'applicazione richiede privilegi elevati, documenta il vincolo e le protezioni aggiuntive adottate. Limitare i programmi eseguibili non elimina automaticamente tale requisito.

5.3 Formazione e segnalazione dei sospetti

Domanda di controllo: Il personale riceve indicazioni pertinenti al proprio lavoro e conosce un canale semplice per segnalare dubbi o anomalie?

Conseguenze operative: Istruzioni poco chiare e segnalazioni tardive possono ritardare la gestione di un problema e aumentarne gli effetti sulle attività quotidiane.

Come verificarlo: Consulta il piano formativo, i materiali e i registri delle attività svolte. Verifica che siano inclusi, secondo il ruolo:

- riconoscimento delle richieste insolite e verifica del mittente;
- uso delle credenziali e dei supporti rimovibili;
- regole per dispositivi personali e manutentori;
- segnalazione di messaggi sospetti o anomalie dei sistemi;
- comportamenti da seguire dopo un possibile errore.

Controlla che le indicazioni raggiungano anche nuovi assunti, turnisti e personale temporaneo interessato.

Puoi chiedere, senza mettere alla prova la persona con un inganno: "A chi segnaleresti una richiesta insolita di accesso?" oppure "Cosa faresti se avessi aperto un allegato sospetto?".

Evidenza da annotare: Data e destinatari dell'ultima formazione, materiali disponibili e canale di segnalazione.

Se emergono lacune: Organizza attività brevi e pertinenti alle mansioni, con esempi comprensibili e istruzioni di segnalazione. Favorisci la comunicazione tempestiva degli errori, evitando un approccio colpevolizzante.

Eventuali simulazioni di phishing devono avere autorizzazioni, obiettivi, destinatari e modalità di gestione definiti. Non avviarle come prova improvvisata della checklist e non interpretare una sola percentuale di clic come misura complessiva della preparazione aziendale.

5.4 Gestione iniziale degli incidenti ed escalation

Domanda di controllo: Il personale sa chi contattare e quali azioni sono previste quando si sospetta un incidente che coinvolge la produzione?

Conseguenze operative: Contatti o poteri decisionali non definiti possono ritardare il contenimento e favorire azioni scoordinate durante un incidente che coinvolge la produzione.

Come verificarlo: Richiedi la procedura e verifica che specifichi:

- segnali o situazioni da segnalare;
- contatti principali e alternativi, anche fuori dall'orario ordinario;
- informazioni da comunicare, come macchina, ora e comportamento osservato;
- azioni consentite agli operatori e decisioni riservate ai responsabili;
- chi coordina IT, manutenzione, produzione e fornitori;
- chi autorizza isolamento, arresto e successiva ripartenza;
- come comunicare se posta elettronica o rete aziendale non sono disponibili.

Verifica che le istruzioni siano accessibili anche durante un'interruzione dei sistemi.

Evidenza da annotare: Procedura vigente, data dell'ultima verifica dei contatti e riferimento a un'esercitazione o briefing.

Se emergono lacune: Prepara istruzioni specifiche per l'impianto insieme ai responsabili. Non adottare come regola universale "scollega il cavo" o "non spegnere": la scelta dipende dalle conseguenze sul processo e dalle procedure di sicurezza applicabili.

In presenza di pericolo per le persone, devono essere seguite le procedure di emergenza dell'impianto. La conservazione delle evidenze informatiche non deve ostacolare la tutela delle persone.

Organizza un'esercitazione guidata per verificare contatti e decisioni, senza intervenire sui sistemi operativi.

5.5 Manutentori e fornitori esterni

Domanda di controllo: Gli interventi dei fornitori sui sistemi produttivi sono autorizzati, delimitati e verificabili?

Conseguenze operative: Interventi non delimitati o documentati possono introdurre modifiche difficili da ricostruire e lasciare accessi attivi oltre il periodo necessario.

Come verificarlo: Esamina un intervento recente e controlla che risultino definiti:

- referente aziendale e identità dei tecnici autorizzati;
- macchine interessate, attività previste e finestra di intervento;
- modalità di accesso e requisiti dei dispositivi utilizzati;
- permessi assegnati e gestione degli accessi temporanei;
- autorizzazione delle modifiche e modalità di ripristino;
- rapporto delle attività svolte e aggiornamento della documentazione;
- contatti e obblighi di comunicazione in caso di problemi o sospetti incidenti.

Per i collegamenti remoti, richiama le verifiche del controllo 2.5.

La presenza di un accordo di riservatezza non sostituisce il controllo degli accessi e delle attività.

Evidenza da annotare: Autorizzazione e rapporto di un intervento recente, con verifica della chiusura degli accessi temporanei.

Se emergono lacune: Definisci una procedura condivisa con acquisti, manutenzione e IT. Per ogni intervento deve essere chiaro chi autorizza, chi segue l'attività e chi ne verifica la conclusione.

Concorda le eventuali revoche degli accessi permanenti rispetto agli impegni di assistenza e alle esigenze di emergenza.

5.6 Richieste di pagamento e modifiche delle coordinate bancarie

Domanda di controllo: Le richieste di pagamento insolite e le modifiche delle coordinate bancarie vengono verificate attraverso un canale indipendente?

Conseguenze operative: Una richiesta fraudolenta non verificata può dirottare un pagamento, causare una perdita economica e creare contestazioni o ritardi con il fornitore.

Le frodi possono utilizzare nomi di dirigenti o fornitori, messaggi contraffatti oppure caselle di posta realmente compromesse.

Come verificarlo: Richiedi all'amministrazione la procedura e verifica che consideri:

- cambi di IBAN o delle anagrafiche dei beneficiari;
- pagamenti urgenti, fuori procedura o verso nuovi destinatari;
- richieste di riservatezza o di aggiramento delle approvazioni;
- conferma tramite contatti già verificati, non quelli contenuti nel messaggio sospetto;
- approvazioni e separazione dei compiti proporzionate all'operazione;
- gestione delle eccezioni e segnalazione dei tentativi sospetti.

Controlla un caso documentato senza riportare nella checklist coordinate bancarie o dettagli riservati.

La soglia economica non deve essere l'unico criterio: anche una modifica delle coordinate per un pagamento ordinario richiede verifica.

Evidenza da annotare: Procedura di verifica e riferimento a un controllo recente su un pagamento o una variazione anagrafica.

Se emergono lacune: Definisci con l'amministrazione una modalità di conferma indipendente e un percorso per sospendere le operazioni dubbie fino alla verifica.

Le protezioni tecniche della posta sono complementari alla procedura: non eliminano il rischio di richieste inviate da un account legittimo compromesso.

Non inviare false richieste di bonifico per compilare questo controllo. Le eventuali simulazioni devono essere progettate e autorizzate separatamente.

Riepilogo della sezione 5

Esiti: Sì / Parzialmente / No / Non verificato / Non applicabile. Motiva le esclusioni e annota data e riferimento delle evidenze.

Controllo	Esito	Evidenza o informazione mancante	Referente / data prevista
5.1 Identità e gestione delle utenze	<input type="text"/>	<input type="text"/>	Referente <input type="text"/> Data prevista <input type="text"/>
5.2 Privilegi coerenti con il ruolo	<input type="text"/>	<input type="text"/>	Referente <input type="text"/> Data prevista <input type="text"/>
5.3 Formazione e segnalazioni	<input type="text"/>	<input type="text"/>	Referente <input type="text"/> Data prevista <input type="text"/>
5.4 Incidenti ed escalation	<input type="text"/>	<input type="text"/>	Referente <input type="text"/> Data prevista <input type="text"/>
5.5 Manutentori e fornitori	<input type="text"/>	<input type="text"/>	Referente <input type="text"/> Data prevista <input type="text"/>
5.6 Pagamenti e coordinate bancarie	<input type="text"/>	<input type="text"/>	Referente <input type="text"/> Data prevista <input type="text"/>

Come usare i risultati

Dai precedenza agli accessi ancora attivi senza un’esigenza o un responsabile, ai privilegi elevati non giustificati e all’assenza di contatti operativi per gestire un incidente.

Verifica inoltre che le richieste economiche insolite possano essere fermate e confermate senza pressioni a saltare i controlli.

Per ogni lacuna assegna un responsabile e una data. Una procedura scritta è un punto di partenza: servono evidenze della sua applicazione e persone che sappiano utilizzarla durante il lavoro quotidiano.

6 Governo della sicurezza monitoraggio e miglioramento

Chi controlla che le misure funzionino e che i problemi individuati vengano gestiti?

Inventari, protezioni e procedure devono essere mantenuti nel tempo. Una modifica all'impianto, un nuovo accesso remoto o un aggiornamento del software possono cambiare le condizioni esaminate nella checklist.

Questa sezione verifica se esistono responsabilità, criteri e attività per rilevare anomalie, conservare informazioni utili e seguire gli interventi fino alla loro verifica.

Chi coinvolgere: direzione, referente IT o sicurezza, responsabile della produzione, manutenzione, acquisti, qualità ed eventuali consulenti per gli obblighi applicabili.

Come svolgere i controlli: consulta politiche, registri, rapporti di monitoraggio e piani di intervento. Non installare strumenti, generare traffico di prova o modificare la registrazione degli eventi durante la compilazione.

Usa gli esiti **Sì / Parzialmente / No / Non verificato / Non applicabile**. La compilazione della checklist non costituisce una certificazione né dimostra la conformità a una normativa.

6.1 Responsabilità criteri di sicurezza e obblighi applicabili

Domanda di controllo: L'azienda ha definito chi decide in materia di sicurezza, quali criteri segue e quali obblighi riguardano le proprie attività?

Conseguenze operative: Responsabilità e criteri poco chiari possono bloccare decisioni, lasciare rischi senza un titolare e ritardare interventi necessari alla continuità produttiva.

Come verificarlo: Richiedi una politica di sicurezza o un documento equivalente, proporzionato alle dimensioni e all'organizzazione aziendale.

Verifica che siano identificati:

- sistemi e processi da proteggere;
- responsabilità della direzione, dell'IT, della manutenzione e della produzione;
- modalità per valutare i rischi e approvare gli interventi;
- soggetti autorizzati ad accettare eventuali rischi residui;
- requisiti contrattuali, normativi e di settore da considerare;
- occasioni di riesame, comprese modifiche significative e incidenti.

Chiedi se viene utilizzato un riferimento per organizzare le attività, per esempio NIST Cybersecurity Framework, serie IEC 62443 o ISO/IEC 27001. Utilizzare un riferimento non equivale a essere certificati o a soddisfarne tutti i requisiti.

Se viene richiamato il **NIST CSF 2.0**, le sei funzioni sono: Govern, Identify, Protect, Detect, Respond e Recover.

Evidenza da annotare: Politica approvata, elenco delle responsabilità e riferimento alla valutazione degli obblighi applicabili, con data e autore.

Se emergono lacune: Definisci innanzitutto responsabilità e criteri decisionali. Richiedi una verifica qualificata degli obblighi pertinenti, evitando di attribuirli automaticamente a tutte le aziende manifatturiere.

Per ciascun obbligo individuato devono essere chiari perimetro, fonte, adempimenti, scadenze e responsabile. Un richiamo generico a "NIS2" non è sufficiente.

6.2 Monitoraggio e gestione delle segnalazioni

Domanda di controllo: L'azienda dispone di informazioni utili a rilevare anomalie sui sistemi produttivi e di persone incaricate di gestire le segnalazioni?

Conseguenze operative: Anomalie non rilevate o segnalazioni senza un destinatario operativo possono prolungare un incidente prima che qualcuno intervenga.

Come verificarlo: Richiedi una descrizione del monitoraggio esistente e un esempio recente di segnalazione gestita o di verifica del servizio.

Distingui tra:

- **monitoraggio operativo:** disponibilità dei sistemi, guasti e prestazioni;
- **monitoraggio di sicurezza:** accessi insoliti, modifiche non autorizzate, disattivazione di protezioni e altri eventi sospetti.

Un dispositivo raggiungibile e funzionante non è necessariamente privo di problemi di sicurezza.

Verifica che siano definiti:

- sistemi e collegamenti coperti;
- eventi rilevati e principali limiti di visibilità;
- destinatari delle segnalazioni;
- orari di presidio e modalità di gestione fuori orario;
- criteri di priorità ed escalation;
- modalità per accorgersi se la raccolta degli eventi si interrompe.

Evidenza da annotare: Descrizione della copertura, responsabili del servizio e riferimento a una segnalazione o verifica documentata.

Se emergono lacune: Individua prima gli eventi che è necessario rilevare e chi può intervenire. Valuta poi gli strumenti e le modalità di raccolta compatibili con l'impianto.

L'introduzione di sonde, agenti o interrogazioni dei dispositivi deve considerare compatibilità, carico e possibili effetti operativi. Anche la configurazione dei punti di osservazione del traffico richiede una pianificazione.

Non generare scansioni o tentativi di accesso per verificare informalmente se scatta un allarme. Le prove di rilevamento devono essere concordate e separate dalla compilazione.

6.3 Raccolta conservazione e protezione dei log

Domanda di controllo: I log necessari sono raccolti, conservati per periodi motivati e protetti da accessi, modifiche o cancellazioni non autorizzati?

Conseguenze operative: Log indisponibili o alterati possono impedire di ricostruire la sequenza degli eventi, limitando la diagnosi e la verifica delle azioni correttive.

Come verificarlo: Richiedi una politica di gestione dei log o una descrizione equivalente.

Verifica che specifichi:

- sorgenti ed eventi da raccogliere;
- finalità della raccolta;
- tempi di conservazione per le diverse categorie;
- modalità di accesso, consultazione e cancellazione;
- protezioni contro alterazione e perdita;
- gestione dello spazio e delle interruzioni di raccolta;
- coerenza degli orari e identificazione dei sistemi di origine.

Chiedi come sono stati stabiliti i tempi di conservazione, considerando esigenze investigative, rischio, contratti e obblighi effettivamente applicabili.

Non adottare un periodo unico per tutti i log senza una motivazione. La presenza di dati personali richiede inoltre di considerare le relative esigenze di protezione e limitazione della conservazione.

Verifica che il personale autorizzato possa recuperare eventi del periodo previsto: la sola impostazione di una durata non dimostra che i dati siano effettivamente disponibili.

Evidenza da annotare: Politica di gestione dei log e risultato di una verifica documentata della disponibilità degli eventi.

Se emergono lacune: Definisci sorgenti e tempi con i responsabili tecnici e con chi segue gli obblighi applicabili. Valuta una raccolta separata dai sistemi di origine, evitando che un singolo account compromesso possa cancellare tutte le registrazioni.

Per gli eventi collegati a un incidente, prevedi modalità autorizzate di conservazione delle evidenze e registrazione delle operazioni effettuate.

La cifratura dei log protegge la riservatezza, ma da sola non impedisce a un soggetto autorizzato o a un account compromesso di cancellarli.

6.4 Gestione delle carenze e verifica degli interventi

Domanda di controllo: Le carenze individuate hanno un responsabile, una priorità motivata e un percorso di gestione fino alla verifica del risultato?

Conseguenze operative: Carenze senza responsabile o verifica finale possono restare aperte o ripresentarsi, assorbendo risorse senza ridurre il rischio per il processo.

Come verificarlo: Richiedi il registro delle azioni aperte. Può essere anche un foglio di lavoro, purché aggiornato e accessibile alle persone incaricate.

Verifica che per ogni voce siano riportati:

- problema ed evidenza che lo supporta;
- sistemi e processi interessati;
- possibili conseguenze;
- priorità e relativa motivazione;
- responsabile e data obiettivo;
- azione prevista ed eventuali misure temporanee;
- dipendenze da fornitori, ricambi o finestre di manutenzione;
- stato e risultato della verifica conclusiva.

La priorità deve considerare esposizione, possibilità di sfruttamento, impatto sulla produzione e sulle persone, protezioni esistenti e rischi dell'intervento.

Per le vulnerabilità software, un punteggio tecnico come il CVSS può contribuire alla valutazione, ma non determina da solo la priorità dell'impianto.

Evidenza da annotare: Registro aggiornato e un esempio di intervento concluso con verifica documentata.

Se emergono lacune: Crea il registro e assegna le prime responsabilità. Distingui tra:

- azioni per ridurre tempestivamente l'esposizione;
- correzioni definitive da pianificare;
- verifiche necessarie per chiarire una situazione ancora incerta.

Se una correzione deve essere rinviata, registra motivo, misure temporanee, approvazione del rischio residuo e data di riesame.

Non imporre scadenze uguali a tutti gli impianti sulla sola base della gravità tecnica. Rispetta gli eventuali termini applicabili e definisci gli altri tempi considerando il rischio concreto e le condizioni operative.

La chiusura deve comprendere la verifica dell'efficacia della misura e del corretto funzionamento dei processi interessati. L'esecuzione di un aggiornamento, da sola, non basta a dimostrare che il problema sia risolto.

6.5 Requisiti di sicurezza per acquisto e supporto degli impianti

Domanda di controllo: Per gli impianti critici sono definiti i requisiti di sicurezza e gli impegni di supporto del costruttore, dell'integratore e dei fornitori dei componenti?

Conseguenze operative: Supporto e responsabilità non definiti possono ritardare la gestione delle vulnerabilità e generare costi imprevisti quando un componente diventa obsoleto o non aggiornabile.

Come verificarlo: Coinvolgi acquisti, qualità, IT e manutenzione. Per gli impianti già installati consulta contratti, condizioni di assistenza e dichiarazioni del fornitore. Verifica che siano noti:

- soggetto responsabile del supporto e referente per le segnalazioni di sicurezza;
- periodo e perimetro del supporto, componenti esclusi e modalità di comunicazione della sua cessazione;
- modalità per ricevere e valutare avvisi di vulnerabilità pertinenti ai componenti installati;
- disponibilità di correzioni o mitigazioni, condizioni di fornitura e responsabilità per compatibilità, prove e installazione;
- gestione delle credenziali, compresi account predefiniti o non modificabili, e vincoli sugli accessi remoti;
- documentazione e materiali necessari alla manutenzione e al ripristino.

Per i nuovi acquisti, verifica che requisiti e criteri di accettazione siano concordati prima della consegna. Per gli impianti esistenti, distingui gli impegni contrattuali dalle informazioni ancora da ottenere.

Evidenza da annotare: Riferimento al contratto o alla conferma del fornitore, periodo di supporto e componenti coperti, con eccezioni e responsabile interno.

Se emergono lacune: Richiedi chiarimenti scritti e concorda come gestire i periodi non coperti dal supporto. La vita produttiva dell'impianto può superare quella dei suoi componenti: valuta misure compensative, sostituzioni o aggiornamenti pianificati.

Non presumere un obbligo di fornire patch per tutta la vita utile della macchina. Documenta gli impegni effettivi e assegna al referente interno la valutazione degli avvisi, anche quando vengono comunicati dall'OEM. Richiama i controlli 1.2, 1.3 e 1.5.

Riepilogo della sezione 6

Esiti: Sì / Parzialmente / No / Non verificato / Non applicabile. Motiva le esclusioni e annota data e riferimento delle evidenze.

Controllo	Esito	Evidenza o informazione mancante	Referente / data prevista
6.1 Responsabilità e obblighi applicabili	<input type="text"/>	<input type="text"/>	Referente <input type="text"/> Data prevista <input type="text"/>
6.2 Monitoraggio e segnalazioni	<input type="text"/>	<input type="text"/>	Referente <input type="text"/> Data prevista <input type="text"/>
6.3 Conservazione e protezione dei log	<input type="text"/>	<input type="text"/>	Referente <input type="text"/> Data prevista <input type="text"/>
6.4 Gestione e verifica degli interventi	<input type="text"/>	<input type="text"/>	Referente <input type="text"/> Data prevista <input type="text"/>
6.5 Acquisto e supporto degli impianti	<input type="text"/>	<input type="text"/>	Referente <input type="text"/> Data prevista <input type="text"/>

Come usare i risultati

Dai precedenza alle situazioni in cui nessuno riceve le segnalazioni rilevanti, gli eventi necessari non sono disponibili oppure le carenze restano aperte senza una decisione e un responsabile.

La presenza di strumenti o documenti non dimostra, da sola, che il processo funzioni. Cerca riscontri: una segnalazione presa in carico, un evento recuperato, un intervento verificato.

Definisci un riesame della checklist e aggiornala quando cambiano impianti, collegamenti, fornitori o condizioni operative. Conserva data e perimetro di ogni compilazione, così da distinguere i miglioramenti dimostrati dalle informazioni ancora da verificare.

Cosa fare dopo la compilazione

La checklist serve a decidere dove approfondire e intervenire. Non è un esame: una risposta negativa segnala una lacuna, mentre “Non verificato” indica un’informazione da ottenere. Non cercare di risolvere tutto contemporaneamente.

1 Dare priorità alle conseguenze sul processo

Parti dai sistemi critici e considera sicurezza delle persone, continuità produttiva, qualità e tracciabilità. Valuta esposizione, protezioni esistenti e possibilità di ripristino. Backup non provati o accessi remoti non controllati meritano un approfondimento tempestivo; il solo numero di risposte negative non determina la priorità.

2 Condividere le decisioni

Riunisci IT, manutenzione, produzione e direzione; coinvolgi acquisti e OEM quando necessario. Scegli le prime tre azioni, assegna un responsabile e fissa una data di riesame. Distingui le misure temporanee dagli interventi definitivi e dalle verifiche ancora necessarie.

3 Validare le situazioni incerte

Se mancano evidenze su sistemi critici, definisci un assessment mirato prima di scegliere gli interventi o acquistare nuovi strumenti. Il perimetro e le modalità devono essere compatibili con l’impianto. Eventuali VAPT richiedono una valutazione separata di obiettivi, autorizzazioni e impatto operativo.

Valutazione preliminare RILABS delle lacune IT e OT

RILABS può affiancare i referenti aziendali nella lettura delle evidenze, nell’individuazione delle lacune e nella definizione delle prime priorità. Il perimetro, i criteri di valutazione e la documentazione necessaria vengono concordati prima dell’attività.

Il risultato è un riepilogo delle criticità e delle informazioni da verificare, con priorità motivate, prime azioni e approfondimenti necessari. Eventuali stime di impegno e tempi sono indicative e riportano ipotesi e dipendenze da fornitori e finestre di manutenzione.

Una ricognizione iniziale su un perimetro limitato non equivale a un audit di conformità né a un penetration test. Durata e costo vengono definiti in funzione dell’ambito concordato.

Richiedi un confronto sui risultati

Scrivi a lucaerrico@rilabs.it con oggetto “Checklist IT OT”. Indica il tipo di attività, il perimetro generale e due o tre aree da approfondire. Per il primo contatto non inviare la checklist compilata, credenziali, indirizzi di rete o schemi dettagliati.

Luca Errico | lucaerrico@rilabs.it | rilabs.it

Sintesi per la direzione

Compila questa pagina dopo il confronto con i referenti. Riporta le decisioni e le incertezze rilevanti, senza attribuire un punteggio complessivo di sicurezza.

Azienda e stabilimento:

Perimetro esaminato e data:

Partecipanti al riesame:

Processi critici e conseguenze da evitare:

Informazioni mancanti che richiedono verifica:

Le prime tre azioni

Priorità e controllo	Responsabile	Azione ed evidenza attesa	Data obiettivo
1 <input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
2 <input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
3 <input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Motiva le priorità in base al processo, all'esposizione e alle protezioni già presenti. Per dettagli e avanzamento usa il registro previsto dal controllo 6.4.

Dipendenze da OEM e finestre di intervento:

Decisione o risorse richieste alla direzione:

Misure temporanee e rischi da riesaminare:

Data del prossimo riesame e referente:

Glossario essenziale

IT e OT: IT indica i sistemi informatici aziendali; OT indica dispositivi e software che controllano o supportano processi fisici, come le linee di produzione.

PLC: Controllore programmabile che esegue la logica di una macchina o di un processo, leggendo ingressi e comandando uscite.

HMI: Interfaccia operatore, per esempio il pannello usato per visualizzare stati, allarmi e parametri della macchina.

SCADA: Sistema di supervisione e acquisizione dati che raccoglie informazioni dagli impianti e può consentirne il controllo.

Firmware: Software di base di un dispositivo, per esempio un controllore o uno switch industriale.

OEM: Costruttore della macchina o dell'apparecchiatura. Il suo ruolo va distinto da quello dell'integratore e dei produttori dei singoli componenti.

DMZ industriale: Zona di rete intermedia per servizi di scambio dati o accesso tra IT e OT, protetta da regole verso entrambi gli ambienti.

VLAN: Suddivisione logica di una rete. La sua presenza non dimostra, da sola, che il traffico tra le reti sia limitato.

VPN: Collegamento protetto attraverso una rete, spesso usato per l'accesso remoto. La sua sicurezza dipende anche da utenti, autorizzazioni e configurazione.

Autenticazione a più fattori: Verifica dell'identità tramite fattori distinti, per esempio una password e un dispositivo in possesso dell'utente.

RTO: Obiettivo di tempo di ripristino: entro quanto tempo deve essere recuperato un servizio o processo.

RPO: Obiettivo di recupero dei dati: quanta perdita temporale di dati è tollerabile. Un RPO di quattro ore non indica la durata del ripristino.

CVSS: Sistema di punteggio della gravità tecnica delle vulnerabilità. Non determina da solo la priorità di intervento sullo specifico impianto.

Log: Registrazioni degli eventi di un sistema, utili per diagnosi, monitoraggio e ricostruzione delle attività.

VAPT: Vulnerability Assessment e Penetration Testing: attività di valutazione delle vulnerabilità e prove di attacco autorizzate, con obiettivi e modalità da definire separatamente.

Riferimenti per approfondire

NIST SP 800-82 Rev. 3, Guide to Operational Technology Security, settembre 2023: protezione fisica e gestione della sicurezza OT. IEC 62443-4-1:2018: sviluppo sicuro, gestione delle correzioni e fine vita dei prodotti.

Questi riferimenti non costituiscono una mappatura completa dei requisiti né un'attestazione di conformità.

Guida NIST OT | IEC 62443-4-1