



Bacciardi  
Partners



*GUIDA OPERATIVA*

# IT GOVERNANCE & CYBERSECURITY

**La sicurezza dei software integrati nei  
prodotti è una responsabilità da governare**

---

Per le imprese che producono, distribuiscono  
o utilizzano prodotti e dispositivi connessi.

Aggiornata a ottobre 2026

## SCENARIO

# Un attacco digitale può diventare un danno fisico

Il rischio non si arresta ai confini dei sistemi informatici aziendali.

01

### **Dal software al prodotto**

Un accesso non autorizzato a un sistema di controllo può alterare parametri operativi, temperature e cicli di funzionamento. Le conseguenze possono coinvolgere merci, impianti e continuità dei servizi.

02

### **Dal prodotto alla filiera**

Quando l'apparecchiatura integra componenti software di terzi, il produttore deve governare anche le dipendenze tecnologiche: manutenzione, vulnerabilità, accessi remoti e tempi di intervento.

03

### **Dal problema tecnico alla responsabilità aziendale**

L'assenza di processi, contratti e presidi documentati può aggravare le conseguenze dell'incidente e rendere più complessa l'attribuzione delle responsabilità.

---

Il caso riportato in Francia nell'ottobre 2026 è uno spunto operativo: questa guida non attribuisce cause o responsabilità a specifici fornitori.

## PERIMETRO

# Quali prodotti e componenti mappare?

La prima decisione è individuare esattamente cosa compone il sistema digitale immesso sul mercato.

## Apparecchiature e componenti digitali

Frigoriferi, congelatori, controllori, gateway, sensori, moduli di rete, firmware e software incorporati. La valutazione dipende dalle funzioni e dalle connessioni del prodotto.

## Servizi collegati

Piattaforme cloud, manutenzione remota, telemetria, applicazioni di diagnostica, aggiornamenti e gestione degli accessi dei tecnici.

## Dipendenze esterne

Fornitori di software, integratori, componentisti, manutentori e prestatori di servizi digitali. Per ciascuno occorre individuare prodotti interessati, referenti e obblighi contrattuali.

---

**Output atteso:** inventario delle componenti, delle versioni e delle interfacce di accesso, collegato ai modelli venduti e al parco installato.

## GESTIONE DEL RISCHIO

# Quattro controlli prioritari

La governance diventa efficace quando i rischi producono decisioni responsabili e verifiche periodiche.

01

### Accessi e connessioni

Verificare autenticazione, privilegi, credenziali dei manutentori, registrazione degli accessi e disattivazione delle utenze non necessarie.

02

### Vulnerabilità e aggiornamenti

Definire canali di segnalazione, criteri di gravità, tempi di correzione, test, distribuzione delle patch e piani alternativi se l'aggiornamento non è immediato.

03

### Continuità e risposta

Stabilire procedure per isolare apparati compromessi, ripristinare configurazioni sicure, avvisare clienti e raccogliere evidenze.

04

### Monitoraggio del parco installato

Conoscere versioni software, durata del supporto, esposizioni note e destinatari delle comunicazioni di sicurezza.

## **FORNITORI**

# **La sicurezza deve entrare nei contratti**

Un contratto di fornitura tecnologica deve rendere verificabili gli impegni di sicurezza.

### **Obblighi di manutenzione**

Aggiornamenti di sicurezza, durata del supporto, fine vita, compatibilità e livelli minimi di servizio.

### **Incidenti e vulnerabilità**

Tempi di comunicazione, obblighi di cooperazione, informazioni necessarie e supporto tecnico nella gestione di un evento.

### **Accessi e subfornitura**

Regole per gli accessi remoti, autorizzazione dei subfornitori, standard di sicurezza e tracciabilità.

### **Allocazione del rischio**

Garanzie, indennizzi, limiti di responsabilità, coperture assicurative e rimedi contrattuali coerenti con i rischi effettivi.

## **FORNITORI**

# **Cyber Resilience Act: le scadenze**

Il Regolamento(UE) 2024/2847 disciplina la cybersecurity dei prodotti con elementi digitali, entro il suo ambito di applicazione.

### **Dall'11 settembre 2026: *obblighi di segnalazione***

I fabbricanti devono segnalare vulnerabilità attivamente sfruttate e incidenti gravi che incidono sulla sicurezza dei prodotti interessati. Sono previsti un preallarme entro 24 ore e una notifica entro 72 ore, con successivi rapporti nei termini applicabili.

### **Dall'11 dicembre 2027: *applicazione generale***

Diventano applicabili le principali prescrizioni relative alla progettazione sicura, alla valutazione del rischio, alla documentazione tecnica, alla gestione delle vulnerabilità e alla conformità dei prodotti.

### **Prodotti già sul mercato**

Gli obblighi di segnalazione riguardano anche prodotti già commercializzati. Per i requisiti generali occorre distinguere le nuove immissioni sul mercato e le modifiche sostanziali secondo le regole del Regolamento.

---

**Attenzione:** occorre valutare per ogni famiglia di prodotti il campo di applicazione, le esclusioni e il ruolo dell'impresa nella filiera.

## GOVERNANCE D'IMPRESA

# NIS2 e organizzazione interna

La sicurezza del prodotto e la sicurezza dell'impresa richiedono verifiche diverse ma coordinate.

01

## NIS2: verificare l'assoggettamento

La disciplina NIS2 può interessare imprese manifatturiere, tra cui attività relative ad apparecchiature elettriche e macchinari. Non basta però produrre frigoriferi: vanno verificati attività, dimensioni e criteri previsti dalla normativa nazionale.

02

## Assegnare ruoli decisionali

Direzione, IT/OT, ricerca e sviluppo, qualità, acquisti, legale e assistenza post-vendita devono conoscere responsabilità, flussi di escalation e poteri di intervento.

03

## Approvare procedure verificabili

Inventario degli asset, valutazione dei rischi, controllo dei fornitori, incident response, formazione, registri e riesami periodici devono formare un sistema coerente.

04

## Gestire le notifiche

Occorre verificare separatamente gli obblighi di notifica previsti dal CRA e quelli eventualmente applicabili all'organizzazione ai sensi della NIS2.

## PIANO DI AZIONE

# Cosa fare nei prossimi 90 giorni?

Un percorso in tre fasi per trasformare il rischio in un piano di intervento.

### **Giorni 1-30 | Diagnosi**

Censire famiglie di prodotti, software e fornitori. Identificare accessi da remoto, versioni, supporto e incidenti pregressi. Eseguire una prima verifica CRA e NIS2.

### **Giorni 31-60 | Priorità e contratti**

Classificare i rischi, assegnare i responsabili, pianificare gli interventi e rivedere le clausole critiche dei contratti con i fornitori.

### **Giorni 61-90 | Presidi e verifica**

Approvare le procedure di gestione delle vulnerabilità e degli incidenti, definire i flussi verso clienti e autorità competenti ed effettuare una simulazione di incidente.

---

**Risultato:** un registro delle criticità con responsabili, scadenze, misure adottate ed evidenze documentali.

## CHECKLIST

# Cosa fare adesso?

Una prima autovalutazione per i produttori di apparecchiature frigorifere.

- ☐ Individuare tutti i prodotti connessi e i software integrati, anche di terzi.
- ☐ Conoscere le versioni installate e il ciclo di supporto dei componenti.
- ☐ Verificare e limitare accessi e connessioni da remoto.
- ☐ Definire un processo documentato per vulnerabilità e aggiornamenti.
- ☐ Rivedere contratti, SLA e obblighi di cooperazione dei fornitori.
- ☐ Attribuire ruoli, responsabilità e poteri decisionali interni.
- ☐ Predisporre un piano di risposta agli incidenti e comunicazione ai clienti.
- ☐ Verificare gli obblighi CRA e l'eventuale assoggettamento NIS2.

*IL SUPPORTO DI BACCIARDI PARTNERS*

# **Governare i rischi, proteggere il business**

La cybersecurity non è soltanto un tema tecnico. Richiede decisioni organizzative, contratti e responsabilità chiaramente definite.

## **IT Governance e organizzazione**

Mappatura dei rischi, definizione di ruoli, policy, procedure e controlli periodici.

## **Contratti e filiera tecnologica**

Revisione di accordi con fornitori di software, integratori, manutentori e partner tecnologici.

## **Conformità e gestione degli incidenti**

Analisi degli obblighi applicabili, governance documentale, procedure di notifica e coordinamento legale nella risposta agli incidenti.

## RIFERIMENTI

# Fonti e perimetro della guida

Materiale informativo per una prima valutazione aziendale.

Aggiornato al 13 ottobre 2026.

## Regolamento (UE) 2024/2847 | *Cyber Resilience Act*

Articoli 13, 14 e 71; Allegato I. Testo ufficiale: [eur-lex.europa.eu/eli/reg/2024/2847/oj](https://eur-lex.europa.eu/eli/reg/2024/2847/oj)

## Commissione europea | *Guida all'attuazione del CRA*

Pagine tematiche sui fabbricanti, sulle segnalazioni e sulle scadenze: [digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act](https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act)

## Direttiva (UE) 2022/2555 | *NIS2*

Articolo 2 e Allegato II; da leggere insieme alla normativa nazionale di recepimento e ai provvedimenti applicabili.

## Notizia di contesto | *ottobre 2026*

Articolo di la Repubblica del 12 ottobre 2026 relativo ad attacchi ai sistemi di refrigerazione in Francia.

La guida non sostituisce l'analisi del singolo prodotto, dell'architettura tecnica o degli obblighi applicabili alla specifica società. L'efficacia delle misure richiede una valutazione congiunta di profili tecnici, organizzativi e legali.

La tua azienda ha già verificato i rischi informatici  
dei prodotti e le responsabilità nella filiera?

---

**Contatta Bacciardi Partners**  
per individuare le priorità di intervento.



**Avv. Lorenzo  
Bacciardi**

CEO



**Avv. Tommaso  
Mancini**

Head of International  
Commercial Law



**Avv. Federico  
Alessandri**

Of Counsel  
Tech & Law