G.D
a coesia company

# Politica di divulgazione coordinata delle vulnerabilità

# Politica di divulgazione coordinata delle vulnerabilità

## Indice



Data di rilascio: 11/09/2026

# 1. Scopo

Lo scopo della presente politica di divulgazione coordinata delle vulnerabilità è descrivere le modalità mediante le quali G.D S.p.A. riceve, gestisce e divulga le vulnerabilità dei prodotti con elementi digitali di cui G.D S.p.A. è fabbricante.

# 2. Applicabilità

Quanto descritto nella presente politica di divulgazione coordinata delle vulnerabilità si applica ai prodotti con elementi digitali, di cui G.D S.p.A. è fabbricante, rientranti nel campo di applicazione del regolamento (UE) 2024/2847.

## 2.1 Revisione e data di applicazione

La presente politica di divulgazione coordinata delle vulnerabilità è la revisione 0 ed è applicabile a partire dal 11 settembre 2026.

# 3. Documento di riferimento

- Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio del 23 ottobre 2024 relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828 (regolamento sulla ciberresilienza).
- UNI CEI EN ISO/IEC 29147:2020: Tecnologie informatiche. Tecniche di sicurezza. Divulgazione delle vulnerabilità.

# 4. Definizioni

- *Prodotto con elementi digitali:* qualsiasi prodotto software o hardware e le relative soluzioni di elaborazione dati da remoto, compresi i componenti software o hardware, immesso sul mercato separatamente; nel seguito

del presente documento per brevità si utilizzerà il termine "prodotto".

- *Vulnerabilità:* un punto debole, una suscettibilità o un difetto di prodotti TIC[1] o servizi TIC che può essere sfruttato da una minaccia informatica.
- *Vulnerabilità sfruttabile:* una vulnerabilità che può essere utilizzata efficacemente da un avversario in condizioni operative pratiche.
- *Vulnerabilità attivamente sfruttata:* una vulnerabilità per la quale esistono prove attendibili che un soggetto malintenzionato l'ha sfruttata in un sistema senza l'autorizzazione del proprietario del sistema.
- *Incidente:* un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi[2].
- *Incidente grave:* Un incidente che ha un impatto sulla sicurezza del prodotto con elementi digitali è considerato grave se[3]:
  - incide negativamente o è in grado di incidere negativamente sulla capacità di un prodotto con elementi digitali di proteggere la disponibilità, l'autenticità, l'integrità o la riservatezza di dati o funzioni sensibili o importanti; o
  - ha portato o è in grado di portare all'introduzione o all'esecuzione di un codice maligno in un prodotto con elementi digitali o nei sistemi informativi e di rete di un utilizzatore del prodotto con elementi digitali.

# 5. Principi generali

G.D S.p.A. riconosce il valore della collaborazione con la comunità dei ricercatori sulla sicurezza informatica e con gli utilizzatori dei prodotti di cui G.D S.p.A. è fabbricante e si impegna a:

- promuovere la segnalazione responsabile delle vulnerabilità;
- garantire la riservatezza delle informazioni ricevute;
- trattare le segnalazioni con diligenza, tempestività e imparzialità;
- coordinare la divulgazione pubblica delle vulnerabilità, ove appropriato;
- astenersi dall'intraprendere azioni legali nei confronti dei soggetti che segnalano vulnerabilità che operino in conformità alla presente politica di divulgazione coordinata delle vulnerabilità e alle disposizioni legislative vigenti.

[1] TIC: tenologie dell'informazione e della comunicazione.

[2] Direttiva (UE) 2022/2555, articolo 6, punto 6).

[3] Regolamento (UE) 2024/2847, articolo 14.

# 6. Segnalazione delle vulnerabilità

## 6.1 Modalità di segnalazione delle vulnerabilità

G.D S.p.A. ha istituito i seguenti punti di contatto mediante i quali chiunque può segnalare le vulnerabilità emerse sui prodotti:

- indirizzo di posta rpa.support@gidi.it, tramite il quale si può richiedere l'accesso alla piattaforma web RPA;
- modulo raggiungibile mediante il tasto "Segnala un incidente informatico" presente nella home page del sito internet aziendale di G.D S.p.A (www.gidi.it).

La ricezione della segnalazione è confermata al soggetto che ha segnalato la vulnerabilità tramite la piattaforma web RPA entro sette giorni.

## 6.2 Contenuto della segnalazione delle vulnerabilità

La segnalazione della vulnerabilità deve contenere almeno le seguenti informazioni:

- indirizzo di posta elettronica a cui può essere contattato il soggetto che segnala la vulnerabilità;
- identificativo del prodotto su cui è stata riscontrata la vulnerabilità, compresa la versione del prodotto se pertinente;
- descrizione della vulnerabilità rilevata e delle condizioni in cui si manifesta;
- ogni altra informazione utile a contestualizzare le condizioni in cui la vulnerabilità si manifesta.

# 7. Analisi e correzione delle vulnerabilità

Le vulnerabilità che sono state segnalate ai punti di contatto indicati nel paragrafo 6.1 vengono tempestivamente analizzate da G.D S.p.A. Dall'analisi può emergere che:

- la vulnerabilità riguarda un componente integrato nel prodotto; in questo caso G.D S.p.A.dà riscontro al soggetto che ha segnalato la vulnerabilità specificando che la segnalazione della vulnerabilità è stata inoltrata al fabbricante del componente interessato e indicando ogni eventuale altra azione intrapresa per attenuare l'impatto della vulnerabilità;
- la vulnerabilità riguarda un prodotto per il quale il periodo di assistenza è terminato; in questo caso G.D S.p.A. dà riscontro al soggetto che ha segnalato la vulnerabilità spiegando che il periodo di assistenza del prodotto è terminato;
- non sono necessari aggiornamenti software o modifiche del prodotto; in questo caso, G.D S.p.A. dà riscontro al soggetto che ha segnalato la vulnerabilità spiegando perché non può compromettere la sicurezza informatica del prodotto;
- è necessario effettuare una campagna di richiamo dei prodotti interessati dalla vulnerabilità per apportare le necessarie modifiche;
- sono necessari aggiornamenti software del prodotto; in questo caso gli aggiornamenti vengono gestiti secondo le modalità descritte nel paragrafo 7.1;
- la vulnerabilità riguarda un prodotto obsoleto per il quale non è possibile applicare aggiornamenti software o effettuare modifiche hardware; in questo caso G.D S.p.A. valuta quali sono le misure che è possibile adottare per minimizzare i rischi di sicurezza informatica del prodotto e, se del caso, ne dà comunicazione agli utilizzatori noti del prodotto.

Il processo di analisi e risoluzione della vulnerabilità deve terminare normalmente entro 30 giorni; se tale processo dovesse richiedere più tempo, ogni 15 giorni il team RPA invia, mediante posta elettronica, al soggetto che ha segnalato la vulnerabilità aggiornamenti sullo stato del processo di analisi e risoluzione della vulnerabilità.

## 7.1 Aggiornamenti software di sicurezza dei prodotti

Sulla base delle analisi effettuate secondo le modalità descritte nel paragrafo 7, G.D S.p.A.:

- appronta gli aggiornamenti software di sicurezza necessari;
- individua i prodotti a cui devono essere applicati gli aggiornamenti;
- identifica i soggetti che utilizzano questi prodotti;
- invia a questi soggetti un messaggio di posta elettronica contenente l'aggiornamento software, o le indicazioni per scaricare l'aggiornamento software, e le istruzioni per applicare l'aggiornamento software oppure, in alternativa, applica gli aggiornamenti software mediante attività di teleassistenza.

# 8. Divulgazione delle informazioni sulle vulnerabilità

Una volta reso disponibile un aggiornamento software di sicurezza oppure se è necessario effettuare una campagna di richiamo dei prodotti, G.D S.p.A. inserisce nella piattaforma RPA contenente le seguenti informazioni:

- codice identificativo univoco della segnalazione di vulnerabilità;
- tipo e modello del prodotto interessato dalle vulnerabilità ed eventualmente altre informazioni utili per identificarlo in modo univoco (ad esempio versione);
- descrizione, gravità e impatto delle vulnerabilità;
- indicazioni su come correggere le vulnerabilità (ad esempio, installazione di aggiornamenti software, configurazione del prodotto, modalità di richiamo dei prodotti, ecc.).

Tali informazioni sono comunicate immediatamente:

- mediante l'invio di messaggi di posta elettronica agli acquirenti e agli utilizzatori noti dei prodotti interessati dalle vulnerabilità;
- tramite la piattaforma RPA al soggetto che ha segnalato la vulnerabilità.

# 9. Condotte ammesse e non ammesse

## 9.1 Condotte ammesse

È consentito svolgere attività di test di sicurezza sul sistema oggetto di analisi esclusivamente nella misura strettamente necessaria a dimostrare l'esistenza della vulnerabilità, evitando qualsiasi impatto sui sistemi, sui dati e sugli utenti.

## 9.2 Condotte non ammesse

È fatto divieto di:

- accedere, modificare o estrarre dal sistema oggetto di analisi dati personali, riservati o sensibili non necessari alla segnalazione della vulnerabilità;

- compromettere la disponibilità dei servizi del sistema oggetto di analisi (ad esempio mediante attacchi di negazione del servizio);
- introdurre malware nel sistema oggetto di analisi;
- copiare, modificare o eliminare dati nel sistema oggetto di analisi;
- apportare modifiche al sistema oggetto di analisi;
- accedere ripetutamente al sistema oggetto di analisi o condividere l'accesso al sistema oggetto di analisi con altri;
- eseguire attacchi brute force per ottenere l'accesso a un sistema;
- sfruttare la vulnerabilità per finalità diverse dalla segnalazione;
- divulgare pubblicamente la vulnerabilità senza preventiva autorizzazione scritta di G.D S.p.A.

# 10. Riconoscimento dei soggetti che segnalano le vulnerabilità

Premesso che le informazioni ricevute saranno trattate esclusivamente ai fini della gestione della vulnerabilità e nel rispetto del Regolamento (UE) 2016/679 (GDPR), a discrezione esclusivaPagina 5 / 6 Politica di divulgazionecoordinata delle vulnerabilità Codice 5.2/B Rev. 00 Data di emissione 10/09/2026 di G.D S.p.A., i soggetti che segnalano le vulnerabilità che abbiano fornito contributi validi e conformi alla presente politica di divulgazione coordinata delle vulnerabilità potranno essere riconosciuti mediante:

- menzione in elenchi di ringraziamento pubblici, a seguito di autorizzazione da parte del soggetto interessato;
- citazione nei documenti di divulgazione delle vulnerabilità (vedi paragrafo 8), a seguito di autorizzazione da parte del soggetto interessato;
- eventuale accesso a programmi di incentivazione, ove previsti.

# 11. Aggiornamenti della politica di divulgazione coordinata delle vulnerabilità

La presente politica di divulgazione coordinata delle vulnerabilità potrà essere modificata o aggiornata in qualsiasi momento. La versione vigente è resa disponibile alla pagina dedicata del sito internet aziendale ed è vincolante a partire dalla data di applicazione indicata nella politica di divulgazione coordinata delle vulnerabilità.