sogei

IL FUNZIONAMENTO DEL CERT SOGEI (RFC 2350)

Compilato:	Scherin De Cesaris, Valentina Lavore
Rivisto:	Fabrizio Maria Bernini
Approvato:	Alessandro Brunacci
Data:	03/04/2026
Versione:	1.4
Classificazione:	Pubblico

INDICE

Versioni del documento

Revisione	Data	Sintesi dei cambiamenti
1.4	03/04/2026	Personale in organigramma e servizi offerti dal CERT

1. INFORMAZIONI SUL DOCUMENTO

Il presente documento contiene una descrizione del CERT Sogei secondo quanto previsto dalla norma "RFC 2350 - Expectation for CSIRT", fornendo le informazioni di base, le modalità con cui può essere contattato e descrivendone sommariamente i compiti e i servizi offerti.

La norma RFC 2350 stabilisce le linee guida circa l'organizzazione e le modalità di comunicazione di un "Computer Security Incident Response Team" (CSIRT), ovvero l'organizzazione che previene e supporta la gestione degli incidenti di sicurezza che possono coinvolgere sistemi informatici di una comunità di soggetti, chiamati Constituency.

In particolare, il suddetto Team prende il nome di CERT Sogei ed eroga servizi per la prevenzione e il supporto della gestione degli incidenti alla Constituency dell'organizzazione.

Il CERT è istituito in conformità con la Cyber Strategy Italiana, espressa nel DPCM 27/01/2014 – Strategia Nazionale per la Sicurezza Cibernetica e segue le linee previste dal Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica e dal Quadro Strategico Nazionale per la Sicurezza dello Spazio Cibernetico.

Il CERT Sogei è costituito da risorse Sogei che operano sinergicamente per adempiere agli obiettivi di sicurezza della Constituency e dell'organizzazione stessa, con particolare attenzione al supporto nella gestione degli incidenti e allo svolgimento di attività di Cyber Threat Intelligence. Sono considerati quali incidenti di interesse del CERT quelli disciplinati dal Decreto-legge 21 settembre 2019 n. 105, in quanto rilevanti per i servizi ricompresi nel Perimetro di Sicurezza Nazionale Cibernetica (PSNC), nonché gli incidenti significativi individuati ai sensi del Decreto legislativo 4 settembre 2024 n. 138, in attuazione della Direttiva (UE) 2022/2555 (NIS2).

Nel seguito del presente documento verrà descritta nel dettaglio l'organizzazione del CERT Sogei e illustrato il suo funzionamento.

1.1 VERSIONE

Versione 1.4 del 03 aprile 2026.
Rispetto alla versione precedente (1.3 del 25 gennaio 2023), sono stati effettuati aggiornamenti al personale in organigramma e ai servizi offerti dal CERT.

1.2 DISPONIBILITÀ

La versione corrente del presente documento è disponibile sul sito Internet della Sogei, all'indirizzo
https://www.sogei.it/it/sogei-homepage/azienda/governance/it-governance/sicurezza-e-tutela-dei-dati/computer-emergency-response-team.html

1.3 ACRONIMI

CERT Sogei - Computer Emergency Response Team della Sogei S.p.A.

CSIRT - Computer Security Incident Response Team.

GPG - GNU Privacy Guard. Software libero progettato per sostituire la suite crittografica PGP. È completamente compatibile con gli standard OpenPGP dell'IETF ed è sostenuto dal governo tedesco. GNU Privacy Guard è distribuito sotto la licenza GNU General Public License e fa parte del Progetto GNU.

GNU - GNU (acronimo ricorsivo di "GNU's Not Unix") è un sistema operativo Unix-like creato nel 1984 da Richard Stallman e sviluppato dalla comunità che aderisce al progetto GNU.

MEF - Ministero dell'Economia e delle Finanze.

PSNC - Perimetro di Sicurezza Nazionale Cibernetica, istituito dal Decreto-legge n.105 del 21 settembre 2019 e convertito con Legge n.133 del 18 novembre 2019, ha il fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale.

RFC 2350 – Request for Comments 2350. The University of Auckland - Network Working Group. This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements.

2. CONTATTI UFFICIALI DEL CERT SOGEI

2.1 NOME

Il nome del Team è "CERT Sogei" in conformità a quanto previsto dal Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica e dal Quadro Strategico Nazionale per la Sicurezza dello Spazio Cibernetico.

2.2 INDIRIZZO

CERT Sogei
Sogei SpA - Via Mario Carucci, 99 e 85 Roma – 00143 Italia

2.3 TIME ZONE

EUROPA CENTRALE GMT +1 (dall'ultima domenica di marzo all'ultima domenica di ottobre GMT +2 – ora legale)

2.4 RIFERIMENTI TELEFONICI E FAX

+390650255005 (fisso)

+393204314519 (reperibilità)

2.5 INDIRIZZO DI POSTA ELETTRONICA

<cert@sogei.it> è l'indirizzo ufficiale del CERT Sogei

2.6 INDIRIZZO DI POSTA ELETTRONICA CERTIFICATA

<cert@pec.sogei.it> è l'indirizzo di posta elettronica certificata del CERT Sogei

2.7 ALTRI TIPI DI COMUNICAZIONE

Ulteriori modalità di comunicazione oltre a quelle sopra elencate sono attivabili su richiesta o in caso di necessità.

2.8 CHIAVI PUBBLICHE E MECCANISMI DI CRITTOGRAFIA

Le comunicazioni tra il CERT Sogei e la Constituency possono avvenire anche tramite scambio di documentazione cifrata con GPG.

Il CERT Sogei rende disponibile la propria chiave pubblica ai referenti degli Enti accreditati, al fine di ricevere da queste comunicazioni contenenti informazioni riservate, protette tramite cifratura. Le chiavi pubbliche sono scambiate tramite canali ritenuti affidabili, per esempio la posta elettronica ordinaria utilizzando caselle istituzionali.

I componenti del CERT hanno accesso alla corrispondente chiave privata, con la quale possono decifrare i dati ricevuti.

Le modalità di utilizzo e di scambio di informazioni sono conformi alle politiche di sicurezza Sogei.

2.9 STRUTTURA DEL TEAM

Il CERT Sogei, incardinato nell'ambito della Direzione Tecnologie e Servizi Digitali (DZT), la cui responsabilità è affidata all'Area Cybersecurity (CYS), è una struttura che opera all'interno di Sogei preposta al trattamento degli incidenti di sicurezza informatica.

Il CERT Sogei è strutturato in maniera tale da adempiere a quanto previsto:

- dal Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica;
- dal Quadro Strategico Nazionale per la Sicurezza dello Spazio Cibernetico;
- dallo Statuto del CERT Sogei.

2.10 PUNTI E MODALITÀ DI CONTATTO PER GLI UTENTI

Il metodo preferenziale per contattare il personale del CERT Sogei è via e-mail all'indirizzo:

- cert@sogei.it

e via PEC all'indirizzo:

- cert@pec.sogei.it

Le e-mail inviate a questi indirizzi sono prese in carico dal personale del CERT il prima possibile, compatibilmente con la gravità attribuita alla segnalazione; tuttavia, qualora si ravvisasse un motivo di urgenza nella comunicazione, è opportuno inserire la dizione "URGENTE" nell'intestazione del messaggio.

I gruppi operativi Sogei che hanno in gestione server o ambienti applicativi possono contattare in caso di urgenze il reperibile di turno del CERT, utilizzando il numero telefonico +393204314519.

Gli orari di funzionamento del CERT Sogei sono generalmente ristretti al normale orario di lavoro (09:00- 18:00 dal lunedì al venerdì).

3. STATUTO

3.1 MISSION

La mission del CERT Sogei consiste nel prevenire e supportare la gestione degli incidenti di sicurezza informatica, svolgendo attività di cyber threat intelligence e promuovendo iniziative di sensibilizzazione e formazione sui temi della cybersecurity. All'interno del CERT Sogei, il Responsabile è incaricato di supportare i vertici aziendali e il personale nella comprensione dei rischi e delle minacce informatiche, con particolare riferimento alla protezione del patrimonio informativo aziendale.

3.2 CONSTITUENCY

La Constituency del CERT Sogei comprende l'insieme degli stakeholder interni ed esterni, nonché delle strutture organizzative ricomprese nel perimetro Sogei, nei cui confronti il CERT eroga servizi di prevenzione e supporto alla gestione degli incidenti di sicurezza informatica.

3.3 ACCREDITAMENTI

Il CERT Sogei è ufficialmente accreditato presso:

- il "Centro Nazionale Anticrimine Informatico a Protezione delle Infrastrutture Critiche" (CNAIPIC);
- il CSIRT Italia - Computer Security Incident Response Team italiano;
- il "Dipartimento delle informazioni per la sicurezza" (DIS).

3.4 AUTHORITY

Il CERT Sogei opera sulla base di contratti/accordi stipulati dall'organizzazione con i clienti accreditati.

4. POLICY DEL CERT SOGEI

4.1 TIPOLOGIE DI INCIDENTI E LIVELLI DI SUPPORTO

Il CERT Sogei fornisce supporto in relazione a incidenti di sicurezza informatica che possano compromettere la riservatezza, l'integrità o la disponibilità dei sistemi informativi e dei servizi rientranti nella propria Constituency.

4.2 COOPERAZIONE, INTERAZIONE E SCAMBIO DI INFORMAZIONI

Nel corso delle attività di prevenzione e di supporto alla gestione degli incidenti, il CERT Sogei avrà una particolare attenzione nella gestione delle informazioni riservate di cui verrà eventualmente a conoscenza. In particolare, le seguenti informazioni saranno trattate in modo da mantenere il massimo della riservatezza possibile:

- le informazioni personali degli utenti;
- le informazioni da considerarsi confidenziali per ragioni legali, contrattuali o etiche.

Saranno altresì considerate come particolarmente riservate tutte le informazioni tecniche riferibili:

- a siti o a sistemi gestiti nell'ambito del dominio di competenza;
- ad attacchi o incidenti, tentati o portati a termine nell'ambito del dominio di competenza;
- ad informazioni statistiche, anche anonime, che possano essere ritenute quali fonti di imbarazzo per le strutture del dominio di competenza;
- ad eventi classificabili come Data Breach.

I potenziali destinatari di comunicazioni del CERT Sogei sono:

- la Sogei;
- la Constituency;
- il CERT-MEF;
- il CSIRT Italia - Computer Security Incident Response Team Italiano;
- altri CERT, nazionali o internazionali;

- il "Centro Nazionale Anticrimine Informatico a Protezione delle Infrastrutture Critiche" (CNAIPIC).

4.3 COMUNICAZIONI: RISERVATEZZA E AUTENTICAZIONE

La natura e la riservatezza delle informazioni di pertinenza del CERT sono tali che le normali comunicazioni telefoniche e l'invio di posta elettronica sono considerati quali mezzi idonei per la trasmissione delle stesse.
Nel caso di comunicazioni contenenti informazioni confidenziali o programmi potenzialmente malevoli sarà utilizzata una cifratura semplice (archivio compresso con password) oppure una cifratura tramite GPG.

5. SERVIZI EROGATI DAL CERT SOGEI

5.1 SUPPORTO ALLA GESTIONE DEGLI INCIDENTI DI SICUREZZA INFORMATICA

Il CERT Sogei fornisce supporto alla gestione degli incidenti di sicurezza informatica all'interno della propria organizzazione, assistendo le strutture interne competenti nelle fasi di Triage, Analisi e Classificazione e Comunicazione e Notifica. In particolare, il CERT offre il supporto necessario per analizzare le minacce e garantire che le informazioni rilevanti siano trattate correttamente, rimanendo informato e aggiornato durante l'intero processo di gestione degli incidenti.

Indicazioni di maggiore dettaglio sono rinvenibili nel seguente documento:

- DP-78-Q4-36 - "Gestione incidenti di sicurezza informatica"

5.1.1 TRIAGE

Durante la fase di Triage, il CERT inoltra le segnalazioni afferenti a potenziali incidenti di sicurezza informatica (ad es. provenienti da attività di Cyber Threat Intelligence), classificandole preliminarmente, alle strutture di competenza.

5.1.2 ANALISI E CLASSIFICAZIONE

Durante la fase di Analisi e Classificazione dell'incidente, se necessario, il CERT conduce attività di Cyber Threat Intelligence per supportare la gestione dell'incidente e fornire un quadro più completo riguardo alla natura della minaccia

5.1.3 COMUNICAZIONE E NOTIFICA

Il CERT rimane informato durante tutto l'iter di gestione dell'incidente, coadiuvando eventuali comunicazioni tra gli attori coinvolti. Al termine, provvede all'invio della relazione finale alle parti interessate.

Se necessario, inoltre, il CERT provvede a notificare l'incidente alle autorità competenti e alla Constituency, garantendo che tutte le informazioni siano trasmesse in modo tempestivo e conforme alle normative in vigore e ai processi aziendali.

5.2 SERVIZI PROATTIVI

5.2.1 CYBER THREAT INTELLIGENCE

Nell'ambito delle attività di Cyber Threat Intelligence, i componenti del CERT effettuano, attraverso l'utilizzo di piattaforme di CTI e la consultazione delle fonti aperte, un monitoraggio quotidiano delle minacce attuali e potenziali che potrebbero avere impatto sull'organizzazione e la sua Constituency.

In particolare, il CERT Sogei eroga i seguenti servizi alla propria Constituency:

- *Early Warning*: individuazione e segnalazione tempestiva di vulnerabilità emergenti o critiche, con particolare attenzione ai casi di sfruttamento attivo o ad elevata probabilità di exploit.;
- *Monitoraggio delle Terze Parti*: attività di identificazione di minacce, vulnerabilità o eventi di sicurezza che possano coinvolgere fornitori, partner o soggetti esterni rilevanti per la Constituency;
- *Digital Risk Protection (DRP):* attività finalizzate all'individuazione e al monitoraggio di minacce e attività malevole relative all'esposizione digitale dell'organizzazione.

5.2.2 CYBER AWARENESS

Il CERT Sogei coordina e mantiene alcuni servizi per supportare la Constituency nell'approfondimento di alcuni temi relativi alla sicurezza informatica, tra cui:

- seminari di approfondimento svolti con cadenza periodica;
- pianificazione ed erogazione di campagne di white phishing;
- Cyber Newsletter: diffusione periodica di aggiornamenti e informazioni sulle principali minacce ed evoluzioni nel panorama cyber.

6. MODULI DI COMUNICAZIONE DEGLI INCIDENTI

Il CERT Sogei non fornisce un modulo di comunicazione degli incidenti di sicurezza.

I referenti accreditati della Constituency possono utilizzare le modalità concordate e i riferimenti previsti.

Tutti gli utenti che volessero segnalare un evento di sicurezza possono farlo tramite la casella di posta elettronica del CERT <cert@sogei.it>, indicando quante più informazioni disponibili, tra cui:

- la tipologia dell'evento o incidente (malware, violazione delle policy, compromissione di sistemi o altro);
- l'ora e la data di quando l'evento è accaduto o se è ancora in corso;
- eventuali evidenze disponibili (ad esempio messaggi di posta elettronica o file), che vanno inviati mediante archivio compresso protetto da password e/o con contenuto cifrato.

7. DISCLAIMER

Sebbene nel corso della predisposizione delle segnalazioni di prevenzione e supporto alla gestione degli incidenti e nella realizzazione dei bollettini/avvisi sia presa ogni possibile precauzione, il CERT Sogei non si assume alcuna responsabilità per eventuali errori ed omissioni o per danni che dovessero risultare dall'uso delle informazioni pubblicate.

Inoltre, la presenza di rinvii operati mediante tecniche di ipertesto (link) inseriti all'interno delle informazioni comunicate dal CERT Sogei, rappresenta unicamente uno strumento per facilitare gli eventuali approfondimenti.