CSIRT Regione Abruzzo (CSIRT Abruzzo)

RFC 2350

VERSION 1.0 – 26 Giugno 2026

1. Informazioni sul presente documento

Questo documento contiene una descrizione del CSIRT (Computer Security Incident Response Team) Abruzzo in conformità alla specifica RFC 2350. Fornisce informazioni di base sul CSIRT Italia, descrive le sue responsabilità ei servizi che offre.

1.1 Ultimo aggiornamento

Questa è la versione 1.0, pubblicata l'126/06/2026.

1.2 Elenco di distribuzione per le notifiche

Non esiste alcun canale di distribuzione per notificare le modifiche al presente documento. Le modifiche sono annunciate su:

https://www.regione.abruzzo.it/argomenti/digitale/sicurezza-informatica/csirt-regione-abruzzo .

1.3 Luoghi in cui è possibile trovare questo documento

La versione corrente del documento è disponibile all'indirizzo:

https://www.regione.abruzzo.it/argomenti/digitale/sicurezza-informatica/csirt-regione-abruzzo

Assicurati di utilizzare la versione più recente.

1.4 Identificazione del documento

Titolo "CSIRT Abruzzo_RFC2350"
Versione: 1.0
Dati del documento: 26-06-2026
Scadenza: il presente documento è valido fino a quando non sarà sostituito da una versione successiva.

2. Informazioni di contatto

2.1 Nome del team

CSIRT Abruzzo: Computer Security Incident Response Team - Abruzzo

2.2 Indirizzo

CSIRT Abruzzo c/o
Regione Abruzzo – Via Leonardo da Vinci, 6 - 67100 L’Aquila

2.3 Fuso Orario

Europa Centrale (GMT+1, e GMT+2 dall'ultima domenica di marzo all'ultima domenica di ottobre)

2.4 Numero di telefono

+39 0862 363623

2.5 Numero di fax

Non divulgato

2.6 Altre comunicazioni

I soggetti appartenenti alla Constituency del CSIRT Abruzzo devono comunicare via email all'indirizzo indicato di seguito.

csirt@regione.abruzzo.it

Si tratta di un alias di posta elettronica che inoltra le email agli operatori di turno del CSIRT Abruzzo.

2.7 Membri del team

Il team del CSIRT Abruzzo è composto da Analisti della sicurezza informatica, Analisti delle minacce, formatori tecnici e divulgatori per la sensibilizzazione alle tematiche di cybersecurity e responsabili della risposta agli incidenti.

2.8 Ulteriori Informazioni

Ulteriori informazioni riguardo lo CSIRT Abruzzo possono essere trovate nel sito https://www.regione.abruzzo.it/argomenti/digitale/sicurezza-informatica/csirt-regione-abruzzo

2.9 Contatti

Il metodo consigliato per contattare CSIRT Abruzzo è via email all'indirizzo csirt@regione.abruzzo.it

I messaggi vengono monitorati durante l'orario di apertura che generalmente è il normale orario di lavoro (9:00-17:00, dal lunedì al venerdì, escluse le festività italiane).

Se necessario, qualsiasi caso urgente può essere segnalato telefonicamente al numero +39 0862 363623.

3. Statuto

3.1 Dichiarazione di missione

Il CSIRT Abruzzo , con particolare riferimento alla Constituency formata da Regione Abruzzo supporta le Pubbliche Amministrazioni Locali (PAL) del territorio per le esigenze specifiche di sicurezza e promuove ed agevola l'implementazione sul territorio regionale di regole e modelli organizzativi nazionali in coordinamento continuo con lo CSIRT Italia.

In coerenza con le "Linee Guida per la realizzazione di CSIRT" emanate da ACN, policy ed organizzazione delle attività sono state definite ed implementate al fine di assolvere alla funzione di CSIRT territoriale per la Constituency individuata.

Lo CSIRT Abruzzo intende rispondere all'esigenza di supporto in tema di sicurezza informatica degli enti facenti parte della sua Costituency e non solo. Nella sua "accezione" territoriale, lo CSIRT Abruzzo si intende operativo in strettissimo contatto con lo CSIRT Italia al fine di essere in prima istanza costantemente aggiornato su temi e minacce, e conseguentemente poter svolgere funzione di divulgazione iniziative/indicazioni nazionali.

3.2 Constituency

Il CSIRT Abruzzo offre i propri servizi ad Enti ed Aziende pubbliche ed infrastrutture critiche operanti nel territorio della Regione Abruzzo inclusi:

- Giunta Regionale dell'Abruzzo;
- Enti e Aziende Pubbliche che utilizzano l'infrastruttura tecnologica regionale attraverso il Centro Tecnico Federato della Regione Abruzzo.

3.3 Affiliazione

Il CSIRT Abruzzo è affiliato con CSIRT Italia che fa parte dell'Agenzia per la Cybersicurezza Nazionale (ACN), in cui è istituito anche il Comitato Nazionale per la Gestione della Cybersicurezza (NSC) che supporta il Presidente del Consiglio dei Ministri italiano e il Comitato Interministeriale per la Cybersicurezza (CIC) nelle attività di prevenzione, preparazione, risposta e ripresa relative alla gestione delle crisi nazionali di cybersicurezza.

3.4 Autorità

In considerazione degli obiettivi identificati nel documento di Mandato, delle caratteristiche e delle necessità degli Enti che appartengono alla Constituency, CSIRT Abruzzo opera in un regime di Autorità Condivisa. In virtù di tale regime, CSIRT Abruzzo collabora con i singoli Enti influenzando il processo decisionale circa le azioni che dovrebbero essere intraprese in merito alla sicurezza informatica, senza tuttavia poterle imporre.

4. Policies

I servizi del CSIRT Abruzzo sono progettati per adattarsi ad un ampliamento progressivo della Constituency, prevedendo che nuovi membri possano essere integrati con i processi del CSIRT in maniera scalabile e modulare. Il CSIRT Abruzzo, infatti, adatta i propri servizi al contesto degli Enti e alle prestazioni associate alle tecnologie di sicurezza implementate con l'obiettivo di supportare, reattivamente e proattivamente, la risposta agli incidenti di sicurezza informatica che si verificano all'interno della sua Constituency.
Il CSIRT Abruzzo ritiene fondamentale la cooperazione tecnica e la condivisione delle informazioni con il CSIRT Italia ed altri soggetti rilevanti per raggiungimento dei propri obiettivi definiti nel mandato.
CSIRT Abruzzo assicura che le informazioni relative alle attività proattive e reattive trattate nell'ambito dei propri servizi come nomi e dettagli tecnici, non vengono pubblicate senza accordi formalmente approvati tra le parti. CSIRT Abruzzo per la classificazione delle informazioni e degli asset informatici utilizza, promuove e sensibilizza la Constituency all'utilizzo del TLP, come richiesto da ACN (TLP v2.0 - ACN).

4.1 Tipologia di incidenti e livello di supporto

CSIRT Abruzzo è autorizzato ad affrontare incidenti di sicurezza informatica rilevanti che si verificano, o minacciano di verificarsi, presso la propria Constituency. A seconda della natura dell'incidente di sicurezza, CSIRT Abruzzo implementerà gradualmente i suoi servizi che includono: gestione dello scambio di informazioni e interazioni con stakeholder interni ed esterni; produzione e diffusione di intelligence sulle minacce informatiche tattiche, operative e strategiche, anche per prevenire e contrastare incidenti di sicurezza informatica; allerta e analisi degli artefatti.
Il livello di supporto fornito da CSIRT Abruzzo varierà a seconda del tipo e della gravità dell'incidente o del problema, del suo impatto potenziale o valutato e delle risorse di CSIRT Abruzzo disponibili al momento.

CSIRT Abruzzo si impegna a tenere informata la sua Constituency sulle potenziali vulnerabilità, possibilmente prima che vengano sfruttate attivamente.

4.2 Collaborazioni e condivisione di informazioni

Il CSIRT Abruzzo considera la cooperazione operativa e la condivisione delle informazioni con altri CSIRT e organizzazioni qualificate simili di fondamentale importanza. Pertanto, mentre saranno adottate misure appropriate per proteggere l'identità dei membri della Constituency, il CSIRT Abruzzo condividerà opportunamente le informazioni al fine di supportarli nel risolvere o prevenire incidenti di sicurezza.
Il CSIRT Abruzzo opera nell'ambito degli attuali quadri giuridici italiani ed europei, con particolare riguardo alla gestione e alla divulgazione delle informazioni.

4.3 Comunicazioni e riservatezza

Telefoni ed e-mail non crittografate sono considerati strumenti di comunicazione sufficientemente sicuri per la trasmissione di dati non riservati. Nel caso sia necessario inviare dati sensibili tramite e-mail: i dati sensibili saranno crittografati per la trasmissione.

CSIRT Abruzzo riconosce e adotta il TLP (Information Sharing Traffic Light Protocol TLP v2.0 - ACN).

5. Servizi

CSIRT Abruzzo, nell'ambito delle fasi di identificazione, contenimento, mitigazione, bonifica, recovery e documentazione di incidenti di sicurezza informatica, supporta gli Enti e le Aziende Locali della Constituency erogando le seguenti tipologie di servizi:

- Monitoraggio e analisi degli eventi di sicurezza: raccoglie informazioni utili, monitora gli eventi e li analizza per individuare possibili incidenti e ridurre i falsi allarmi.
- Gestione degli incidenti di sicurezza: supporta l'analisi degli incidenti e delle cause, la raccolta di evidenze, la definizione dei piani di rientro e il coordinamento con i soggetti coinvolti, fino alle azioni di mitigazione e ripristino.
- Gestione delle vulnerabilità: identifica e analizza vulnerabilità (anche non note), condivide informazioni utili e supporta la definizione di azioni di rimedio e messa in sicurezza.
- Aggiornamento del quadro di rischio: analizza dati e segnali rilevanti e condivide indicazioni utili per prevenzione e gestione di minacce e incidenti.
- Formazione e diffusione di conoscenza: promuove consapevolezza sulle minacce informatiche e offre formazione, esercitazioni e supporto tecnico per migliorare infrastrutture, strumenti e servizi di sicurezza.

5.1 Servizi Proattivi

- Technology watch
- Security Audits or Assessments
- Intrusion Detection / Prevention Services

5.2 Servizi Reattivi

- Incident Handling
- Alerts and Warnings

5.3 Security Quality Management

- Security Consulting
- Awareness Building and Education Training

6. Disclamers

Il CSIRT Abruzzo non è responsabile per l'utilizzo improprio degli strumenti messi a disposizione della Constituency nell'ambito dei servizi erogati.