CSIRT Regione Umbria (CSIRT Umbria)

RFC 2350

VERSION 1.0 – 19 Marzo 2025

1. Informazioni sul presente documento

Questo documento contiene una descrizione del CSIRT (Computer Security Incident Response Team) Umbria 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'19/03/2025.

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://csirt.regione.umbria.it/.

1.3 Luoghi in cui è possibile trovare questo documento

La versione corrente del documento è disponibile all'indirizzo:

https://csirt.regione.umbria.it/documents/guest/CSIRT%20Umbria_RFC2350.pdf
Assicurati di utilizzare la versione più recente.

1.4 Autenticazione del presente documento

Il presente documento è stato firmato con la chiave PGP/GPG del CSIRT Umbria.

1.5 Identificazione del documento

Titolo "CSIRT Umbria_RFC2350"
Versione: 1.0
Dati del documento: 19-03-2025
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 Umbria: Computer Security Incident Response Team Umbria

2.2 Indirizzo

CSIRT Umbria c/o
Regione Umbria - Corso Vannucci, 96 - 06121 Perugia,

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

+39 848 883366

2.5 Numero di fax

Non divulgato

2.6 Altre comunicazioni

I soggetti appartenenti alla Constituency del CSIRT Umbria devono comunicare con i membri del team tramite il modulo “Segnalazioni” presente nel sito web o via email all'indirizzo indicato di seguito.

2.7 Indirizzo email

csirt@regione.umbria.it. Si tratta di un alias di posta elettronica che inoltra le email agli operatori di turno del CSIRT Umbria.

2.8 Chiavi pubbliche e altre informazioni di crittografia

Il CSIRT Umbria supporta la crittografia PGP/GPG.
La chiave pubblica PGP/GPG è disponibile sul sito ufficiale del CSIRT Umbria

https://csirt.regione.umbria.it/documents/guest/CSIRT%20Regione%20Umbria_0x6D2141CB_public.asc

2.9 Membri del team

Il team del CSIRT Umbria 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.

2.10 Ulteriori Informazioni

Ulteriori informazioni riguardo lo CSIRT Umbria possono essere trovate nel sito **https://csirt.regione.umbria.it**.

2.11 Contatti

Il metodo consigliato per contattare CSIRT Umbria è compilare il modulo https://csirt.regione.umbria.it/servizi/assistenza o, in subordine, via email all'indirizzo csirt@regione.umbria.it (Si prega di utilizzare PGP/GPG se si intende inviare informazioni sensibili).
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 +39 848 883366.

3. Statuto

3.1 Dichiarazione di missione

Il CSIRT-Umbria, con particolare riferimento alla Constituency formata da Regione Umbria ed Aziende sanitarie umbre, 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 Umbria 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 Umbria 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.
Inoltre, in una realtà regionale dalle dimensioni obiettivamente contenute come quella Umbra, lo CSIRT Umbria risulta essere profondamente e sostanzialmente integrato con il SOC Regionale, al fine di assicurare una capacità di risposta che si prevede abbia necessità di un continuo e proficuo interscambio tra le attività operative proprie del SOC e quelle di supporto, analisi e di indirizzo strategico che caratterizzano lo CSIRT.

3.2 Constituency

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

- Giunta Regionale dell'Umbria;
- Aziende Sanitarie/Ospedaliere Umbre;
- Enti che utilizzano l'infrastruttura tecnologica regionale umbra.

3.3 Affiliazione

Il CSIRT Umbria 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 Umbria opera in un regime di Autorità Condivisa. In virtù di tale regime, CSIRT Umbria 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.
In tal senso, il CSIRT Umbria espleta il suo mandato nell'abito della Constituency con il riconoscimento della propria funzione da parte di:

- Servizio Sistema informativo regionale, infrastrutture digitali e cybersecurity della Regione Umbria.

4. Policies

I servizi del CSIRT Umbria 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 Umbria, 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 Umbria 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 Umbria 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 Umbria 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 Umbria 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 Umbria 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 Umbria varierà a seconda del tipo e della gravità dell'incidente o del problema, del suo impatto potenziale o valutato e delle risorse di CSIRT Umbria disponibili al momento.
CSIRT Umbria 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 Umbria 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 Umbria condividerà opportunamente le informazioni al fine di supportarli nel risolvere o prevenire incidenti di sicurezza.
Il CSIRT Umbria 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, dovrà essere utilizzato PGP/GPG (vedi precedente paragrafo 2.8). I trasferimenti di file debbono essere trattati con le stesse regole descritte per le e-mail: i dati sensibili saranno crittografati per la trasmissione. CSIRT Umbria riconosce e adotta il TLP (Information Sharing Traffic Light Protocol TLP v2.0 - ACN).

5. Servizi

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

- supporto all'analisi delle cause dell'incidente;
- coordinamento dei team convolti nella risposta all'incidente;
- supporto alla classificazione dell'incidente ed alla disseminazione nella Constituency degli IoC;
- gestione delle attività di escalation verso CSIRT Italia ed altre autorità competenti.

CSIRT Umbria inoltre eroga le seguenti tipologie di servizi come meglio descritto nel sito (Servizi – CSIRT Umbria):

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. Incident Reporting Forms

La condivisione dei report associati ad incidenti presi in carico dai SOC regionale all'interno della Constituency deve avvenire come descritto al paragrafo 4.2 utilizzando la classificazione TLP. Le richieste di servizio e di supporto per la risposta agli incidenti devono essere inviate utilizzando il modulo https://csirt.regione.umbria.it/servizi/assistenza o, in subordine, via e-mail all'indirizzo csirt@regione.umbria.it (Si prega di utilizzare PGP/GPG se si intende inviare informazioni sensibili).

7. Disclamers

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