

Cybersecurity & Data Protection

Newsletter mensile: Gennaio 2026



Questo mese parliamo di...

INCIDENT MANAGEMENT: IDENTIFICAZIONE E SEGNALAZIONE



L'**Incident Management** consente di gestire in modo organizzato gli eventi imprevisti che possono compromettere i dati o la sicurezza informatica dell'Agenzia. ARPAC ha adottato una procedura dedicata per garantire una risposta tempestiva, ridurre i danni, proteggere i dati personali e assicurare la continuità dei servizi.

IDENTIFICAZIONE DI UN POSSIBILE INCIDENTE*



In presenza di un'anomalia, di un malf funzionamento sospetto o di un evento potenzialmente rischioso, è essenziale **agire con tempestività**. Anche in caso di semplice dubbio, è sempre raccomandato procedere con una **segnalazione**.



COMPORTAMENTI ANOMALI

Comportamenti anomali del sistema informatico, blocchi improvvisi o malfunzionamenti che impediscono le normali attività



PHISHING

Ricezione di messaggi e-mail sospette, contenenti allegati o link potenzialmente malevoli, indirizzati a caselle istituzionali o personali



MALWARE

Prestazioni e attività insolite come rallentamenti improvvisi del computer o programmi installati senza il consenso dell'utente

*gli incidenti riportati costituiscono solo un sottoinsieme dei possibili casi che possono rappresentare una minaccia e che vanno prontamente segnalati

RILEVO UN EVENTO SOSPETTO: COSA FARE



Una **gestione efficace** degli incidenti di sicurezza richiede il **coinvolgimento attivo e consapevole** di tutto il personale

BUONE PRATICHE

- Si suggerisce di **raccogliere le principali informazioni utili alla segnalazione**, così da facilitarne la gestione
- È opportuno **inviare la segnalazione tramite i canali messi a disposizione dall' Agenzia**
- Si consiglia di **seguire le raccomandazioni fornite dal personale specializzato**, evitando di agire in autonomia.



SEGNALAZIONE POSSIBILE INCIDENTE



La **segnalazione** tempestiva di un evento di sicurezza **permette di rilevare e gestire gli incidenti e attacchi informatici** garantendo la resilienza dell'Agenzia attraverso l'adozione di adeguate azioni correttive e assicurando la conformità alla normativa vigente (NIS2).

A seguito dell'identificazione è necessario segnalare tempestivamente l'evento alla **U.O. Sistemi Informativi e Informatici**, tramite i seguenti canali:



securityalert@arpacampania.it



0812326343