Edizione 1 del 28/02/2022

Redatta da	Leonello Calabresi	**Verificata da**	Leonello Calabresi	**Approvato da**	Antonio Goglia

Informativa Clienti sulle Emergenze

Edizione 1 del 28/02/2022

Redatta da	Leonello Calabresi	**Verificata da**	Leonello Calabresi	**Approvato da**	Antonio Goglia

Edizione 1 del 28/02/2022

Redatta da	Leonello Calabresi	**Verificata da**	Leonello Calabresi	**Approvato da**	Antonio Goglia

Scopo

Lo scopo di questo documento è di illustrare ai clienti come si articola il processo di gestione di incidenti che non ricadono nelle normali operatività dei servizi erogati.

Campo di applicazione

La presente policy si applica agli eventi che possono compromettere la Riservatezza, Integrità e Disponibilità dei dati personali o dei servizi che li gestiscono.

Definizioni

Evento: Qualsiasi occorrenza identificata in un sistema, servizio o rete che indica una possibile violazione della sicurezza o il fallimento di una misura di protezione. Un evento non implica necessariamente un danno; è un'anomalia che richiede monitoraggio.

Incidente della sicurezza delle informazioni: Un evento (o una serie di eventi) che ha un impatto negativo concreto sulla riservatezza, integrità o disponibilità delle informazioni. Un incidente compromette le operazioni e richiede una risposta immediata (Incident Response) per essere contenuto.

Gestione degli incidenti della sicurezza delle informazioni

Il processo di gestione degli incidenti di Advanced Systems S.p.A. è disegnato per gestire qualsiasi tipo di evento che non faccia parte della normale operatività del servizio e che potrebbe causare interruzione o diminuzione della qualità dei servizi erogati; pericoli per la riservatezza, integrità, disponibilità delle informazioni.

Tabella dei contatti per la notifica degli incidenti

Funzione	e-mail
DPO	dpo@advancedsystems.it
CSIRT Aziendale	csirt@advancedsystems.it
Privacy	privacy@advancedsystems.it
Help Desk	entilocali@advancedsystems.it

Gli attori principali nella catena di escalation sono:

- **Operatori dell'help desk**: sono il front-end per il cliente e si occupano dell'assistenza di primo livello.
- **Specialisti IT**: gli specialisti IT sono responsabili della disponibilità e del funzionamento di tutti i sistemi.
- **Specialisti di prodotto**: gli specialisti di prodotto sono i capi progetto. Essi sono responsabili del corretto funzionamento delle applicazioni utilizzate dai clienti. Agiscono come assistenza di secondo livello coadiuvati dai progettisti.

Redatta da	Leonello Calabresi	**Verificata da**	Leonello Calabresi	**Approvato da**	Antonio Goglia

- **Privacy**: è il team che risponde alle comunicazioni in materia di privacy coadiuvato dal DPO.
- **DPO**: è il responsabile per la protezione dei dati personali.
- **CSIRT Aziendale**: è il team di risposta alle emergenze per eventi che possono avere un impatto sulla Riservatezza, Integrità e Disponibilità di dati e servizi.
- **Security Operation Center (SOC)**: il servizio di monitoraggio della sicurezza cyber, operativo H24.

Catena di escalation

La figura seguente mostra la catena di escalation seguita a seguito della notifica di incidente da parte del cliente.

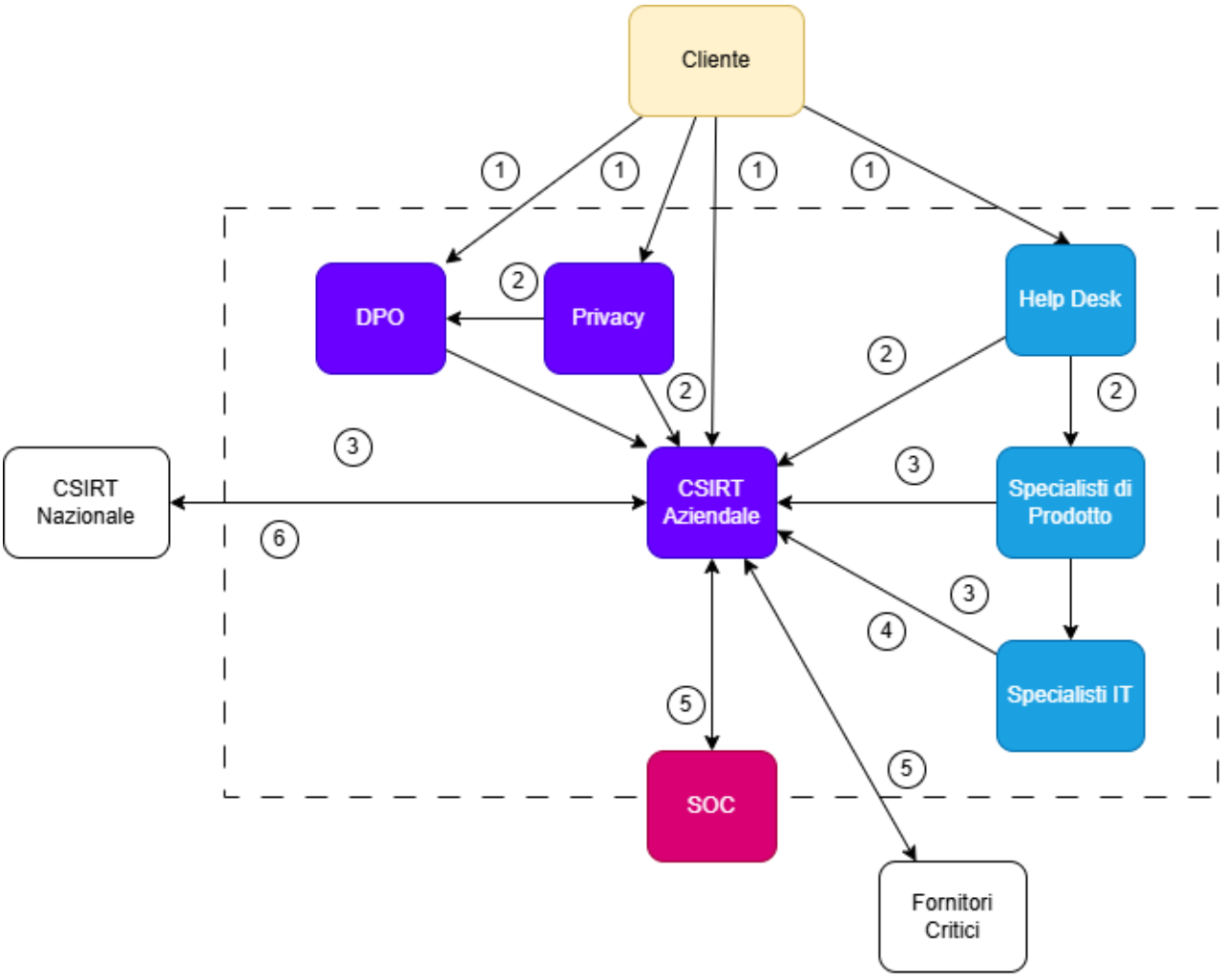

Figura 1 - Catena di escalation

Redatta da	Leonello Calabresi	**Verificata da**	Leonello Calabresi	**Approvato da**	Antonio Goglia

Tutto lo staff di AS ha comunque la responsabilità di notificare ai propri responsabili di area, al management, o al CED situazioni in cui la capacità di AS di operare con continuità e affidabilità le proprie attività sia messa a rischio. Tali comunicazioni dovranno essere propagate fino ad arrivare al Recovery Team che una volta classificato l'incidente porrà in essere il piano di trattamento più adeguato.

Processo

In caso di incidenti relativi alla sicurezza delle informazioni Advanced Systems opera in conformità con le linee guida ISO/IEC 27035-1:2016 e ISO/IEC 27035-2:2016. Il processo di gestione degli incidenti si articola è delineato di seguito.

Tutti gli eventi vengono condivisi con il CSIRT aziendale.

Se l'evento è riferito alla perdita di informazioni, per esempio dati personali che potrebbero essere stati rubati da un archivio cartaceo o elettronico, il responsabile del CED riporterà l'incidente al Data Protection Officer (DPO) e al Management e determinerà l'impatto del data breach facendo riferimento alla procedura **PRSI 160 - Data Breach**.

Notifica

La notifica di un incidente della sicurezza delle informazioni può avenire da parte di entità esterne quali i clienti, utilizzando i canali di comunicazione previsti dalla tabella dei contatti, oppure da parte di personale dello staff di Advanced Systems SpA direttamente al gruppo csirt@advancedsystems.it.

Classificazione

La classificazione della gravità dell'incidente è comunque a sua totale discrezione.

Gravità incidente	Descrizione
Alta	Il grado di compromissione di servizi e/o sistemi è elevato. Si rilevano danni consistenti sugli asset. Il ripristino è di medio o lungo periodo. Si verifica almeno una delle seguenti condizioni. • Indisponibilità del servizio fornito per oltre 24 ore • Perdita di integrità, autenticità o riservatezza dei dati per oltre 100.000 utenti dell'UE (Data Breach)

Redatta da	Leonello Calabresi	**Verificata da**	Leonello Calabresi	**Approvato da**	Antonio Goglia

	• Rischio per la sicurezza e/o l'incolumità pubblica, o in termini di perdite di vite umane
Media	L'incidente non presenta nessuna condizione che porti alla catalogazione "gravità alta". Il grado di compromissione di servizi e/o sistemi è di una certa rilevanza e possono essere rilevati danni sugli asset di una certa consistenza. Il ripristino ha tempi che non compromettono la continuità del servizio L'incidente presenta una tra le seguenti condizioni: • Compromissione di server • Degrado di prestazioni relativo ai servizi offerti dall'ente con conseguente perdita di produttività da parte degli utilizzatori • Attacchi che provocano il funzionamento parziale o intermittente della rete • Impossibilità tecnica di fornire uno o più servizi critici ad un elevato numero di utenti per intervalli di tempo inferiori alle 24 ore • Basso impatto in termini di perdita economica, di immagine e/o reputazione nei confronti degli utenti
Bassa	L'incidente non presenta nessuna condizione che porti alla catalogazione "gravità alta o media". Non vengono compromessi asset o servizi. L'incidente presenta le seguenti condizioni: • Interruzione dell'attività lavorativa di un numero ristretto di dipendenti e per un breve periodo di tempo. • Contaminazioni da virus in un medesimo sito ma comunque identificate dai sistemi anti-malware • Nessuna o limitata perdita di operatività o di business da parte di un ridotto numero di dipendenti.

Tabella 1

Effettuata una prima analisi, ancorché non definitivamente conclusa, il Referente informa tempestivamente il Responsabile per la gestione della sicurezza ICT, che provvede ad attivare l'Incident Recovery Team e, in caso di data breach, informa immediatamente il DPO, e il Legale Rappresentante dell'Azienda.

Trattamento

A seconda della gravità dell'incidente viene attivato uno scenario eseguendo le procedure in esso definite al fine di consentire il contenimento dei danni ed il ritorno alla normale attività.

Tutti gli incidenti di livello **alto** e **medio** che includono una violazione di dati personali vengono riportati al DPO. Tutti gli incidenti di livello basso vengono riportati dal CED al Responsabile della Sicurezza delle Informazioni.

Redatta da	Leonello Calabresi	**Verificata da**	Leonello Calabresi	**Approvato da**	Antonio Goglia

Chiusura

Il Responsabile della Sicurezza delle Informazioni formalmente chiude l'incidente preparando la relazione conclusiva che verrà inviata al cliente. Tale relazione comprende i seguenti elementi: Descrizione dell'evento, Attività di verifica e notifica sull'attacco subito, Azioni intraprese per contenere l'incidente e rimuovere il problema, Azioni di ripristino, Conclusioni.

Conoscenza

Viene effettuato un riesame volto a determinare le cause profonde dell'accadimento, a valutare l'efficacia della risposta, a definire le azioni correttive, ad aggiornare l'analisi del rischio. Viene stilato un report finale che arricchisce la knowledge base aziendale.

Ritorno alle normali operazioni

Il ritorno alle normali operazioni viene comunicato ai dipendenti ed ai clienti a mezzo e-mail e ove necessario telefonicamente.

Archiviazione

Il presente documento viene archiviato dal Responsabile della Qualità e SGSI catalogando per argomento e per attore dell'organizzazione.

Sorveglianza sulle modifiche

La sorveglianza sulle modifiche della presente procedura è del Responsabile della qualità e del SGSI.

Rev	Descrizione delle modifiche apportate	Data di emissione
0	Emissione iniziale	28/02/2022
1	Aggiornata tabella contatti per le emergenze	15/03/2025
2	Aggiornata catena di escalation	17/04/2026