DATACONSEC

DATA PROTECTION - CONSULTING - SECURITY

NIS 2
Prossime scadenze e adempimenti

Webinar, 11 febbraio 2026

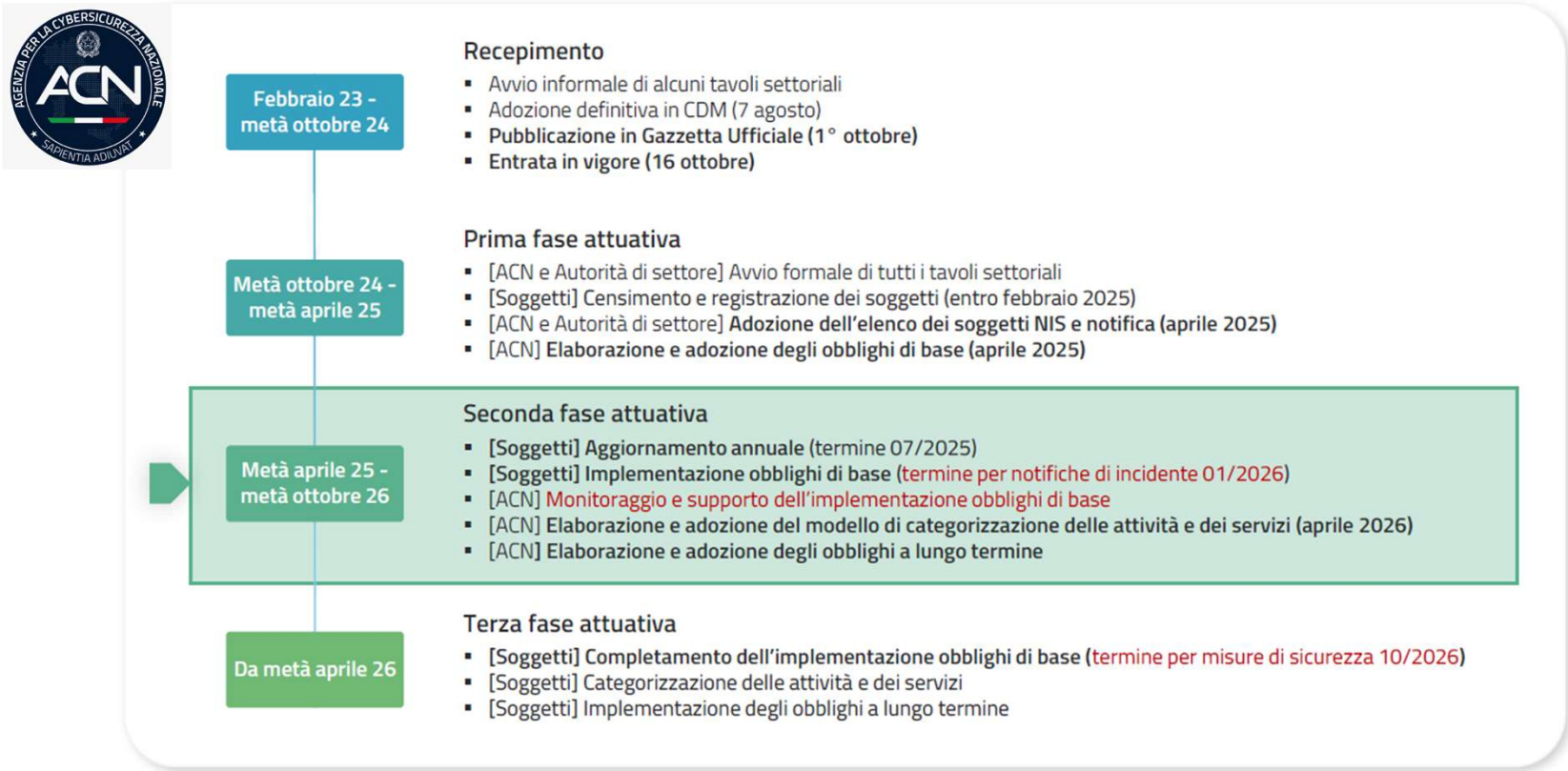
Agenda

- Recepimento e attuazione e prossime scadenze
- Applicazione della normativa – Le specifiche di base e alcuni approfondimenti
- Applicazione della normativa – Il piano di gestione degli incidenti e le notifiche
- Simulazione di una notifica di incidente di sicurezza
- Q&A

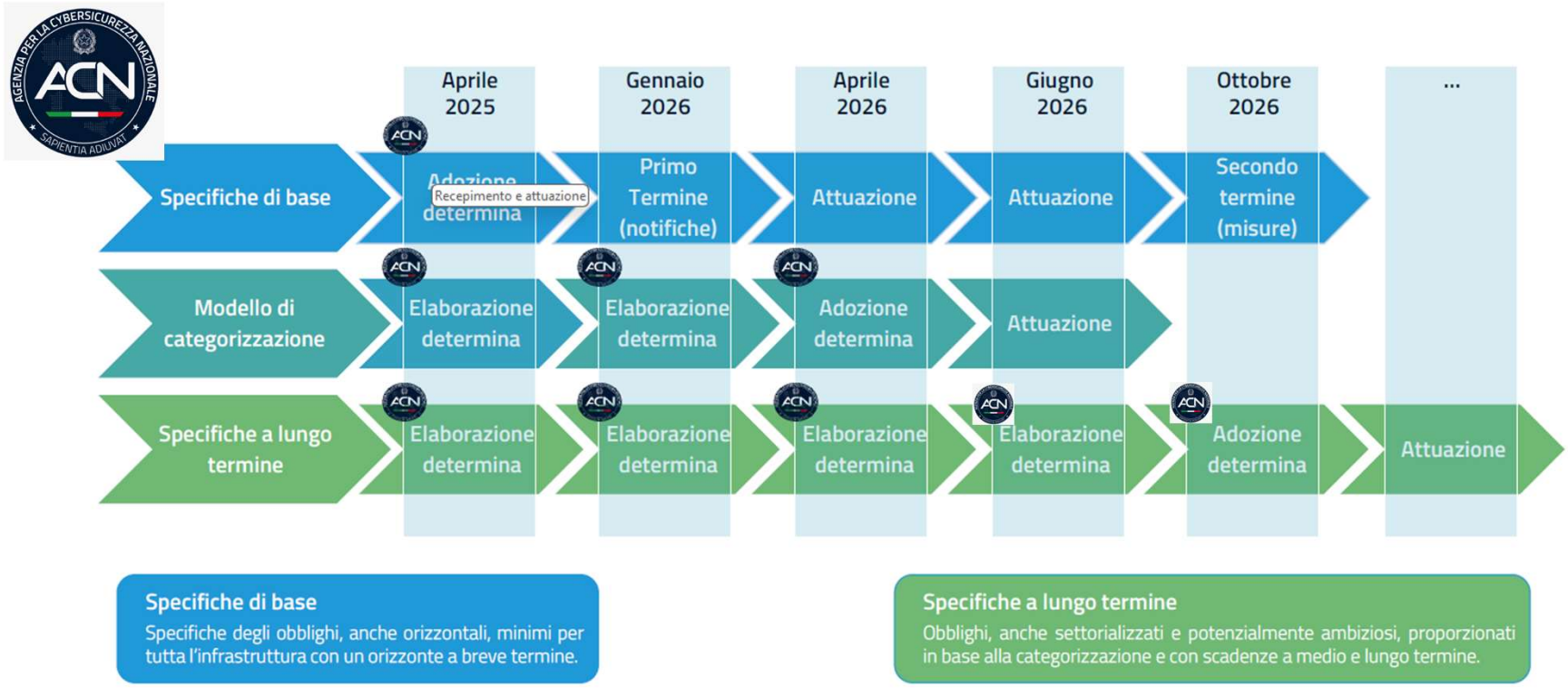
Agenda

- ➢ **Recepimento e attuazione e prossime scadenze**
- ❑ Applicazione della normativa – Le specifiche di base e alcuni approfondimenti
- ❑ Applicazione della normativa – Il piano di gestione degli incidenti e le notifiche
- ❑ Simulazione di una notifica di incidente di sicurezza
- ❑ Q&A

Recepimento e attuazione 1/2



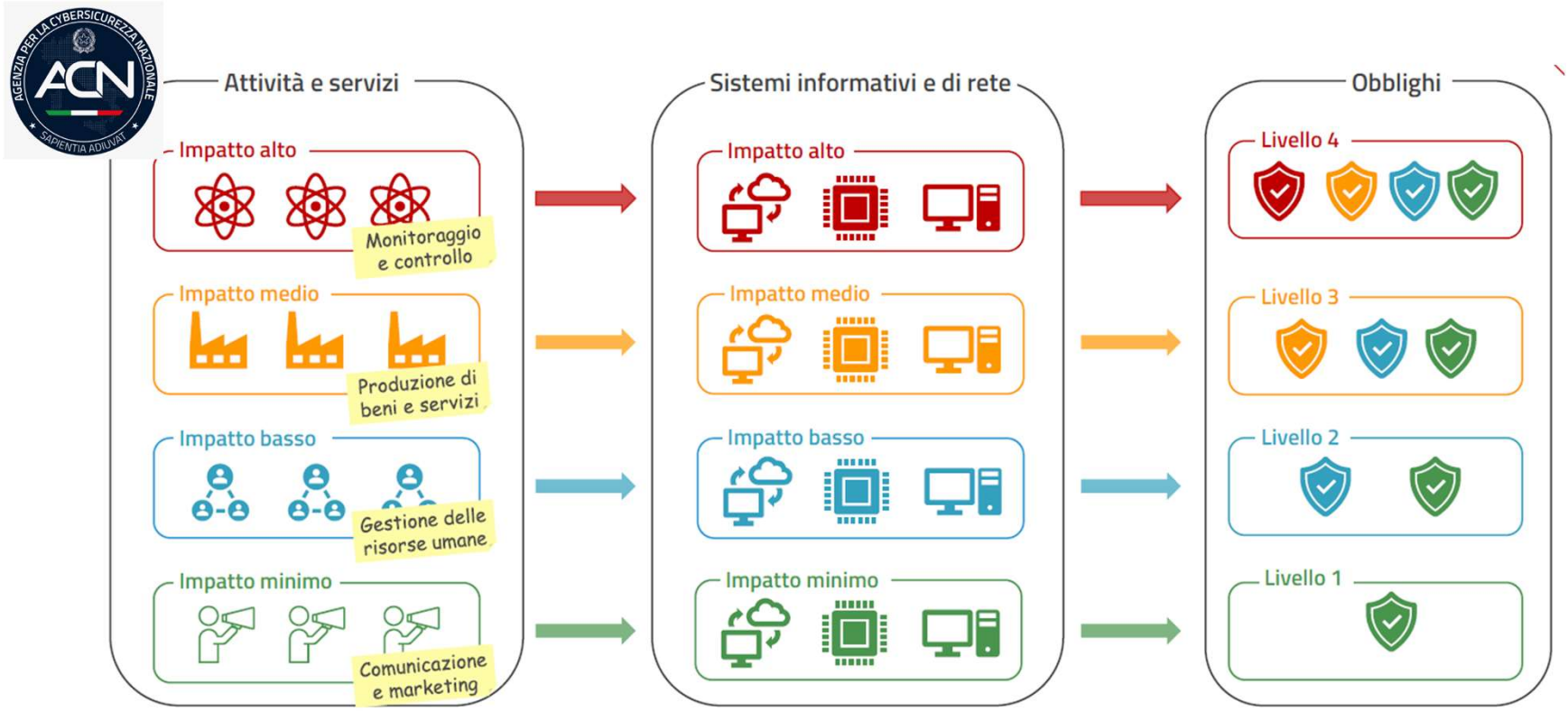
Recepimento e attuazione 2/2



Specifiche di base
Specifiche degli obblighi, anche orizzontali, minimi per tutta l'infrastruttura con un orizzonte a breve termine.

Specifiche a lungo termine
Obblighi, anche settorializzati e potenzialmente ambiziosi, proporzionati in base alla categorizzazione e con scadenze a medio e lungo termine.

Recepimento e attuazione – Proporzionalità degli obblighi



Prossime scadenze

Agenda

- Recepimento e attuazione e prossime scadenze
- **Applicazione della normativa – Le specifiche di base e alcuni approfondimenti**
- Applicazione della normativa – Il piano di gestione degli incidenti e le notifiche
- Simulazione di una notifica di incidente di sicurezza
- Q&A

Le misure di sicurezza di base per i soggetti essenziali e importanti 1/3

D. Lgs. 138/2024 (Decreto NIS)

Art. 23
Organi di amministrazione e direttivi

Art. 24
Obblighi in materia di misure di gestione dei rischi per la sicurezza informatica

Art. 26
Obblighi in materia di notifica di incidente

Determinazione ACN 379907 del 18 dicembre 2025

Allegato 1
Misure di sicurezza di base – soggetti importanti

Allegato 2
Misure di sicurezza di base – soggetti essenziali

Allegato 3
Incidenti significativi di base – soggetti importanti

Allegato 4
Incidenti significativi di base – soggetti essenziali

Le responsabilità degli organi amministrativi e direttivi

Con la locuzione "**organi di amministrazione**" e "**organi direttivi**" ci si riferisce a quegli organi che detengono il **potere di direzione del Soggetto NIS**, incluso, ove presente, il Consiglio di amministrazione (art. 1, lett. e), Determinazione ACN del 10 aprile 2025, n. 136117).

Art. 23 Decreto NIS

Approvano le modalità di **implementazione** delle **misure di gestione dei rischi** per la sicurezza informatica, adottate dal Soggetto NIS

Sovrintendono all'**implementazione** degli **obblighi in materia di gestione del rischio** per la sicurezza informatica e di **notifica degli incidenti**, oltre che di **comunicazione di informazioni specifiche** all'Autorità competente NIS (ACN)

Sono **responsabili delle violazioni del Decreto NIS** (es: mancata osservanza degli obblighi in materia di gestione del rischio di sicurezza informativa; mancate registrazioni o comunicazioni; inottemranza alle disposizioni della Autorità competente o mancata collaborazione con Autorità e CSIRT; ecc.)

Sono tenuti a **seguire una formazione** in materia di sicurezza informatica

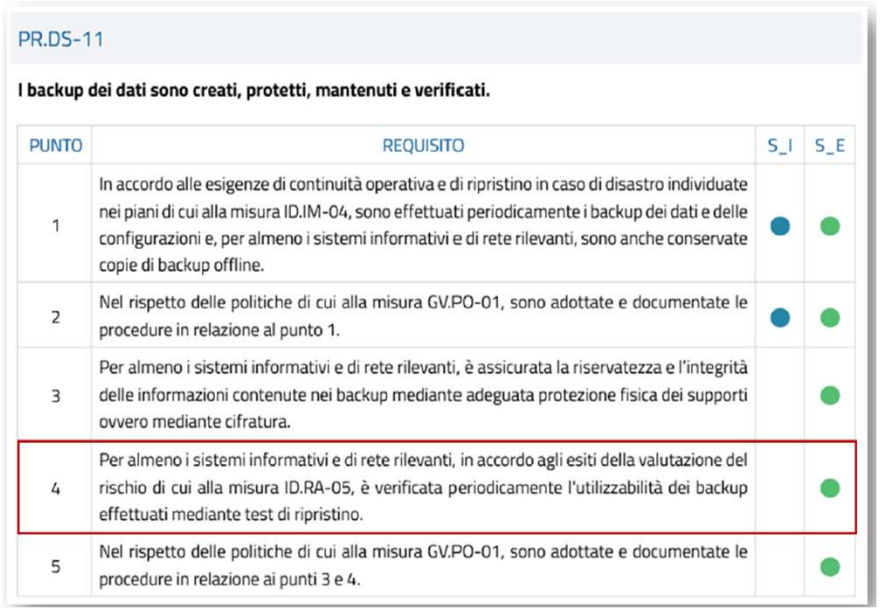
Promuovono l'offerta periodica di una **formazione in materia di sicurezza informatica** ai dipendenti

Sono **informati** su base periodica o, se opportuno, tempestivamente **degli incidenti e delle notifiche effettuate**

Le misure di sicurezza

Obblighi in materia di misure di gestione dei rischi per la sicurezza informatica (art. 24, Decreto NIS)				
Politiche di analisi dei rischi e di sicurezza dei sistemi informativi	Gestione degli incidenti	Continuità operativa, inclusa la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi	Sicurezza catena approvvigionamento, compresi aspetti relativi alla sicurezza dei rapporti con fornitori e fornitori di servizi	Sicurezza catena approvvigionamento, compresi aspetti relativi alla sicurezza dei rapporti con fornitori e fornitori di servizi
Politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi di cybersicurezza	Pratiche di igiene informatica di base e formazione in materia di cybersicurezza	Politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura	Sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli assetti	Uso di soluzione di autenticazione a più fattori o di autenticazione continua e di sistemi di comunicazione protetti

Le misure di sicurezza di base (Det. ACN 379907/2025)



PR.DS-11

I backup dei dati sono creati, protetti, mantenuti e verificati.

PUNTO	REQUISITO	S_I	S_E
1	In accordo alle esigenze di continuità operativa e di ripristino in caso di disastro individuate nei piani di cui alla misura ID.IM-04, sono effettuati periodicamente i backup dei dati e delle configurazioni e, per almeno i sistemi informativi e di rete rilevanti, sono anche conservate copie di backup offline.	●	●
2	Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione al punto 1.	●	●
3	Per almeno i sistemi informativi e di rete rilevanti, è assicurata la riservatezza e l'integrità delle informazioni contenute nei backup mediante adeguata protezione fisica dei supporti ovvero mediante cifratura.		●
4	Per almeno i sistemi informativi e di rete rilevanti, in accordo agli esiti della valutazione del rischio di cui alla misura ID.RA-05, è verificata periodicamente l'utilizzabilità dei backup effettuati mediante test di ripristino.		●
5	Nel rispetto delle politiche di cui alla misura GV.PO-01, sono adottate e documentate le procedure in relazione ai punti 3 e 4.		●

Linee Guida NIS – Specifiche di base – Guida alla lettura (settembre 2025) [https://www.acn.gov.it/portale/documents/d/guest/guida-alla-lettura-specifiche-di-base]

Incidenti significativi di base

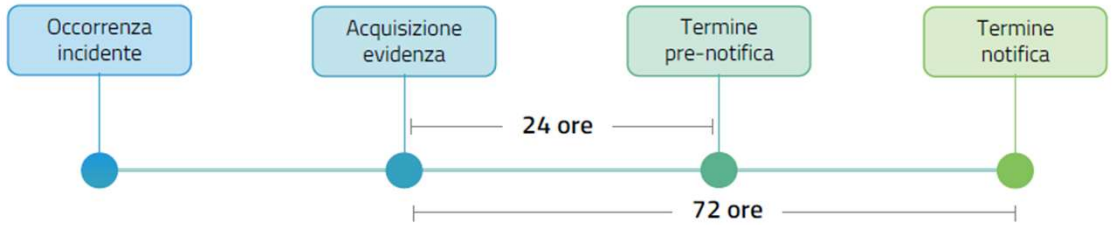
IS-1	Il soggetto NIS ha evidenza della perdita di riservatezza, verso l'esterno, di dati digitali di sua proprietà o sui quali esercita il controllo, anche parziale.
IS-2	Il soggetto NIS ha evidenza della perdita di integrità, con impatto verso l'esterno, di dati di sua proprietà o sui quali esercita il controllo, anche parziale.
IS-3	Il soggetto NIS ha evidenza della violazione dei livelli di servizio attesi dei suoi servizi e/o delle sue attività, sulla base dei livelli di servizio atteso (SL) definiti ai sensi della misura DE.CM-01.
IS-4	Il soggetto NIS ha evidenza, anche sulla base di parametri quali-quantitativi definiti ai sensi della misura DE.CM-01, dell'accesso, non autorizzato o con abuso dei privilegi concessi, a dati digitali di sua proprietà o sui quali esercita il controllo, anche parziale.

Soggetti importanti ed essenziali

Solo soggetti essenziali

Evidenza dell'incidente

Ai fini dell'adempimento dell'obbligo di notifica degli incidenti ciò che rileva è che il soggetto abbia evidenza del verificarsi di una delle tipologie di incidente indicate. L'acquisizione dell'evidenza definisce il momento dal quale decorre il termine per l'obbligo di notifica.



Linee Guida NIS – Specifiche di base – Guida alla lettura (settembre 2025) [https://www.acn.gov.it/portale/documents/d/guest/definizione-del-processo-di-gestione-degli-incidenti-di-sicurezza-informatica]

Agenda

- Recepimento e attuazione e prossime scadenze
- Applicazione della normativa – Le specifiche di base e alcuni approfondimenti
- **Applicazione della normativa – Il piano di gestione degli incidenti e le notifiche**
- Simulazione di una notifica di incidente di sicurezza
- Q&A

Gestione e segnalazione degli incidenti – Cos'è un incidente di *sicurezza informatica significativo*?

Incidente

Un evento che **compromette** la **disponibilità**, l'**autenticità**, l'**integrità** o la **riservatezza** di **dati** conservati, trasmessi o elaborati o dei **servizi offerti dai sistemi informativi e di rete** o accessibili attraverso di essi

Quasi-incidente (*near-miss*)

Un evento che **avrebbe potuto configurare un incidente** senza che quest'ultimo si sia verificato, ivi incluso il caso in cui un incidente sia stato **efficacemente evitato**.

Incidente di sicurezza su vasta scala

Un incidente che causa un livello di perturbazione superiore alla capacità di uno Stato membro di rispondervi o che ha un **impatto significativo su almeno due Stati membri**.

I soggetti essenziali e importanti notificano, senza ingiustificato ritardo al **CSIRT Italia** ogni **incidente** che ha un **impatto significativo** sulla fornitura dei loro servizi, secondo modalità e tempistiche precise.

Un incidente è considerato **significativo** se:

- ha causato o è in grado di causare una **grave perturbazione operativa dei servizi** o **perdite finanziarie** per il soggetto interessato;
- ha avuto ripercussioni o è idoneo a provocare **ripercussioni su altre persone fisiche o giuridiche** causando **perdite materiali e immateriali** considerevoli.

Modello del processo di gestione degli incidenti

Gestione degli incidenti – Preparazione-Governo

In questa sotto-fase, il soggetto definisce il quadro strategico e organizzativo per la gestione degli incidenti, provvedendo, in particolare, all'elaborazione delle **politiche di sicurezza informatica** e all'assegnazione dei **ruoli e delle responsabilità** per le attività del processo di gestione degli incidenti.

Misure di sicurezza

- ✓ **GV.PO-01**: La politica per la gestione del rischio di cybersecurity è stabilita in base al contesto organizzativo, alla strategia di cybersecurity e alle priorità, ed è comunicata e applicata.
- ✓ **GV.PO-02**: La politica per la gestione del rischio di cybersecurity è revisionata, aggiornata, comunicata e applicata per riflettere i cambiamenti nei requisiti, nelle minacce, nella tecnologia e nella missione dell'organizzazione.
- ✓ **GV.RR-02**: I ruoli, le responsabilità e i correlati poteri relativi alla gestione del rischio di cybersecurity sono stabiliti, comunicati, compresi e applicati.
- ✓ **GV.SC-02**: I ruoli e le responsabilità in materia di cybersecurity per fornitori, clienti e partner sono stabiliti, comunicati e coordinati internamente ed esternamente.

Gestione degli incidenti – Preparazione-Identificazione

In questa sotto-fase è acquisita una conoscenza del contesto operativo al fine di pianificare in modo efficace la risposta agli incidenti. Le attività di *identificazione* riguardano, ad esempio, l'inventario dei sistemi informativi e di rete e l'individuazione di minacce e vulnerabilità.

Misure di sicurezza

- ✓ **ID.AM-01**: Sono mantenuti gli inventari dell'hardware gestito dall'organizzazione..
- ✓ **ID.AM-02**: Sono mantenuti gli inventari del software, dei servizi e dei sistemi gestiti dall'organizzazione..
- ✓ **ID.AM-03**: Sono mantenute le rappresentazioni delle comunicazioni di rete e dei flussi di dati di rete interni ed esterni, autorizzati dall'organizzazione.
- ✓ **ID.AM-04**: È mantenuto un inventario aggiornato dei servizi informatici erogati dai fornitori, ivi inclusi i servizi cloud.

Gestione degli incidenti – Preparazione-Protezione

In questa sotto-fase sono stabilite le misure di protezione volte a ridurre la probabilità e limitare l'impatto degli incidenti. Ridurre la probabilità, e dunque il numero, di incidenti consente di dedicare maggiori risorse alla risposta degli incidenti più critici e complessi, mentre limitare l'impatto dell'incidente rende generalmente meno complesse le attività di contenimento ed eradicazione, oltre a mitigare le conseguenze dell'attacco, in termini non solo di sistemi informativi e di rete compromessi, ma anche operativi, economici e reputazionali.

Misure di sicurezza

- ✓ **PR.DS-11**: I backup dei dati sono creati, protetti, mantenuti e verificati.
- ✓ **PR.PS-04**: I registri di log sono generati e resi disponibili per il monitoraggio continuo..
- ✓ **PR.IR-01**: Le reti e gli ambienti sono protetti dall'accesso logico e dall'uso non autorizzati.
- ✓ **PR-IR-03:** Sono implementati meccanismi per soddisfare i requisiti di resilienza in situazioni normali e avverse.
- ✓ **PR.AT-01**:Il personale è sensibilizzato e formato in modo da possedere le conoscenze e le competenze per svolgere compiti di carattere generale tenendo conto dei rischi di cybersecurity.
- ✓ **PR-AT-02**: Il personale è sensibilizzato e formato in modo da possedere le conoscenze e le competenze per svolgere compiti di carattere generale tenendo conto dei rischi di cybersecurity.

Gestione degli incidenti – Rilevamento

La fase di rilevamento è finalizzata a individuare e analizzare gli **eventi rilevanti per la sicurezza informatica** con l'obiettivo di individuare tempestivamente il verificarsi di un incidente e limitarne l'impatto e l'estensione.

Gli *eventi rilevanti per la sicurezza informatica* sono eventi di natura intenzionale o accidentale che compromettono o potrebbero compromettere la sicurezza dei sistemi informativi e di rete e che necessitano pertanto di un'analisi (triage) al fine di verificare se si tratta di un incidente.

Nel caso in cui l'analisi di un evento rilevante per la sicurezza informatica abbia effettivamente determinato che è relativo a un incidente, viene dichiarato l'incidente e si passa alla successiva fase di risposta.

Misure di sicurezza

- ✓ **DE.CM-01**: Le reti e i servizi di rete sono monitorati per individuare eventi potenzialmente avversi.
- ✓ **DE.CM-09**: L'hardware e il software di elaborazione, gli ambienti di runtime e i loro dati sono monitorati per individuare eventi potenzialmente avversi.

Gestione degli incidenti – Risposta

La fase di risposta inizia nel momento in cui è stato dichiarato l'incidente e rappresenta la fase centrale del processo di gestione degli incidenti ed è costituita dalla seguenti sotto-fasi:

- **segnalazione**: si procede a notificare l'incidente alle autorità competenti e a comunicarlo alle parti, interne ed esterne, interessate;
- **investigazione**: viene esaminato in modo approfondito l'incidente con l'obiettivo di ricostruire possibilmente l'intera sequenza degli eventi occorsi (cosiddetta cyber kill chain), individuare la causa dell'incidente e valutare l'estensione della compromissione.
- **contenimento**: viene circoscritto il perimetro dell'attacco in modo da limitare l'impatto dell'incidente ed evitarne l'estensione ad altri sistemi informativi e di rete;
- **eradicazione**: viene rimossa ogni capacità di controllo e persistenza nella rete da parte dell'attaccante.

Misure di sicurezza

- ✓ **RS.MA-01:** Il piano di risposta agli incidenti è eseguito in coordinamento con le terze parti interessate una volta dichiarato un incidente.

Gestione degli incidenti – Ripristino

La fase di ripristino è finalizzata a riportare i sistemi informativi allo stato antecedente all'incidente, assicurandosi che tutto funzioni regolarmente e riguarda, ad esempio, la creazione di golden/clean image, la reinstallazione dei i sistemi a partire dalle golden/clean image, il ricollegamento in rete dei sistemi informativi e di rete bonificati, il monitoraggio dei sistemi per verificare l'efficacia delle attività.

Misure di sicurezza

- ✓ **RC.RP-01:** La parte del piano di risposta agli incidenti relativa al rispristino viene eseguita una volta avviata dal processo di risposta agli incidenti.
- ✓ **RC.CO-03**: Le attività di ripristino e i progressi nel ripristino delle capacità operative sono comunicati agli stakeholder interni ed esterni designati.

Gestione degli incidenti – Miglioramento

La fase di miglioramento si estende per l'intero ciclo di vita del processo ed è finalizzata a potenziare la capacità di gestione degli incidenti e riguarda principalmente attività come l'analisi post-incidente al fine di individuare eventuali carenze e valutare l'efficacia della risposta.

A tal fine sono organizzate le cosiddette riunioni di lesson learned in cui si ha l'opportunità di trarre insegnamenti, alla luce di quanto emerso durante la gestione dell'incidente, dalle azioni intraprese e dalla loro efficacia e di individuare gli interventi correttivi e di potenziamento

Misure di sicurezza

- ✓ **ID.IM-01:** Sono identificati miglioramenti in esito alle valutazioni.
- ✓ **ID-IM-04:** I piani di risposta agli incidenti e gli altri piani di cybersecurity che impattano le operazioni sono stabiliti, comunicati, mantenuti e migliorati.

Gestione e segnalazione degli incidenti – Esempio di piano di gestione degli incidenti informatici

1. **Fasi e procedure di gestione degli incidenti**:
   - **a) segnalazione/rilevazione** dell'evento e relativa tracciatura (data e ora dell'evento e della segnalazione; elenco degli asset coinvolti; servizi impattati; descrizione del problema);
   - **b) analisi e classificazione** dell'evento a seconda del livello di rilevanza, secondo metriche definite;
   - c) identificazione e adozione delle **strategie di contenimento ritenute più efficaci**, finalizzate a minimizzare ogni ulteriore conseguenza e ad evitare un peggioramento della situazione;
   - **d) ripristino**, in particolare con riguardo al ripristino del normale funzionamento dei sistemi informativi e di rete coinvolti dall'incidente di sicurezza;
   - ***e) lesson learned*** e valutazione dell'eventuale revisione di politiche, procedure, processi, strumenti, modalità, compresa l'analisi del rischio
2. Fasi e procedure per la **notifica dell'incidente alle autorità** competenti e per la **predisposizione e trasmissione delle correlate relazioni**, secondo le modalità e le tempistiche individuate dalle normative vigenti, in particolare il Decreto NIS
3. **Ruoli e responsabilità nella gestione degli incidenti**, comprese quelle degli organi di amministrazione e gestione della Società (CdA)
4. **Informazioni di contatto** per la segnalazione degli incidenti, interne e, ove necessario, esterne
5. Modalità previste per la **comunicazione interna** relativamente agli incidenti, anche con riguardo al coinvolgimento degli organi di amministrazione e direttivi
6. Procedure per **comunicare senza ingiustificato ritardo**, anche quando intimato dall'autorità competente:
   - a) ai **destinatari dei servizi**, gli **incidenti significativi** che possono ripercuotersi negativamente sulla fornitura degli stessi;
   - b) ai **destinatari dei servizi** potenzialmente interessati da una **minaccia informatica significativa**, le misure o azioni correttive o di mitigazione che questi possono adottare in risposta a detta minaccia;
   - c) al pubblico, gli incidenti occorsi
7. **Reportistica** da utilizzare per la **documentazione dell'incidente**, tenuto anche conto dei modelli eventualmente messi a disposizione dall'autorità competente.

Notifiche a CSIRT degli incidenti di sicurezza informatica – Tempistiche e caratteristiche

a senza ingiustificato ritardo, e comunque **entro 24 ore** da quando sono venuti a conoscenza dell'incidente significativo, una **pre-notifica** che, ove possibile, indichi se l'incidente significativo possa ritenersi il risultato di **atti illegittimi o malevoli** o può avere un **impatto transfrontaliero**

b senza ingiustificato ritardo, e comunque **entro 72 ore** da quando sono venuti a conoscenza dell'incidente significativo, una **notifica dell'incidente** che, ove possibile, **aggiorni le informazioni** di cui alla lettera a) e indichi una **valutazione iniziale** dell'incidente significativo, comprensiva della sua **gravità** e del suo **impatto**, nonché, ove disponibili, gli **indicatori di compromissione**

c su **richiesta del CSIRT Italia**, una **relazione intermedia** sui pertinenti aggiornamenti della situazione

d una **relazione finale entro un mese** dalla trasmissione della notifica di cui alla lettera b), che comprenda:

- una **descrizione dettagliata** dell'incidente, inclusi la sua gravità e il suo impatto;
- il **tipo di minaccia** o la causa originale (***root cause***) che ha probabilmente innescato l'incidente;
- le **misure di attenuazione** adottate e in corso;
- ove noto, l'**impatto transfrontaliero** dell'incidente.

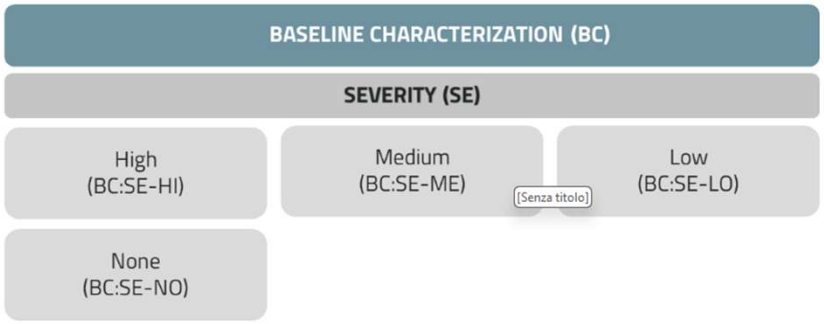
e in caso di **incidente in corso** al momento della trasmissione della relazione finale di cui alla lettera d), una **relazione mensile sui progressi** e una **relazione finale entro un mese dalla conclusione** della gestione dell'incidente.

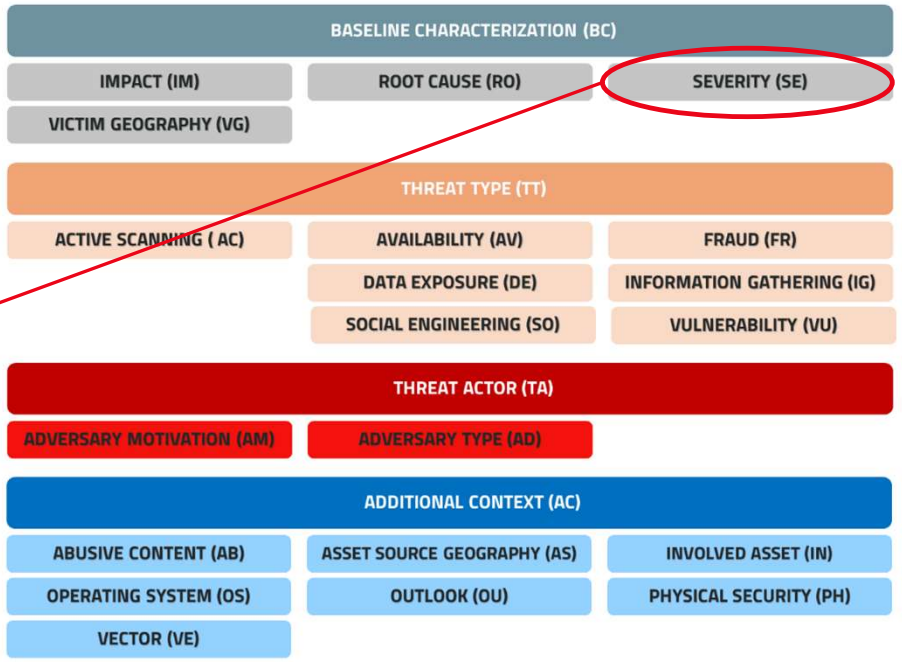
In aggiunta all'obbligo di notifica degli incidenti significativi, possono essere trasmesse, **su base volontaria**, notifiche **al CSIRT Italia** da parte dei:

a) soggetti essenziali e soggetti importanti, per quanto riguarda gli **incidenti diversi da quelli significativi**, le **minacce informatiche** e i **quasi-incidenti**;
b) soggetti **diversi**, **indipendentemente dal fatto che ricadano o meno nell'ambito di applicazione del Decreto NIS**, per quanto riguarda gli incidenti che hanno un impatto significativo sulla fornitura dei loro servizi, le minacce informatiche e i quasi-incidenti.

Focus – Analisi e classificazione degli eventi

https://www.acn.gov.it/portale/documents/20119/552690/ACN_Tassonomia_Cyber_CLEAR.pdf/9595cc35-1c0b-4007-07b2-8f0468e5b82e?t=1731598519616





Le modalità di intervento del CSIRT Italia in caso di notifica di incidenti di sicurezza informatica

Riscontri, consulenza e supporto tecnico

Senza ingiustificato ritardo e ove possibile **entro 24 ore dal ricevimento della pre-notifica**, il CSIRT Italia fornisce una **risposta al soggetto notificante**, comprensiva di un riscontro iniziale sull'incidente significativo e, su richiesta del soggetto, **orientamenti** o **consulenza** sull'attuazione di **possibili misure tecniche di mitigazione**. Su richiesta del soggetto notificante, il CSIRT Italia fornisce **ulteriore supporto tecnico**.

Orientamenti su segnalazioni alle istituzioni

Qualora si sospetti che l'incidente significativo abbia **carattere criminale**, il CSIRT Italia fornisce al soggetto notificante anche orientamenti sulla **segnalazione dell'incidente significativo**, all'organo centrale del **Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione** (Autorità di contrasto).

Indicazioni su ulteriori comunicazioni

Sentito il CSIRT Italia, se ritenuto opportuno e qualora possibile, i **soggetti essenziali** e i **soggetti importanti comunicano**, senza ingiustificato ritardo, **ai destinatari dei loro servizi** gli **incidenti significativi** che possono **ripercuotersi negativamente sulla fornitura di tali servizi**.

I **soggetti essenziali** e i **soggetti importanti**, se ritenuto opportuno e **qualora possibile**, sentito il CSIRT Italia, **comunicano** senza ingiustificato ritardo, ai **destinatari dei loro servizi** che sono potenzialm**ente interessati da una minaccia informatica significativa**, **misure o azioni correttive o di mitigazione** che tali destinatari possono adottare in risposta a tale minaccia. Inoltre, sentito il CSIRT Italia, se ritenuto opportuno, i soggetti essenziali e i soggetti importanti comunicano ai medesimi destinatari **anche la natura di tale minaccia** informatica significativa.

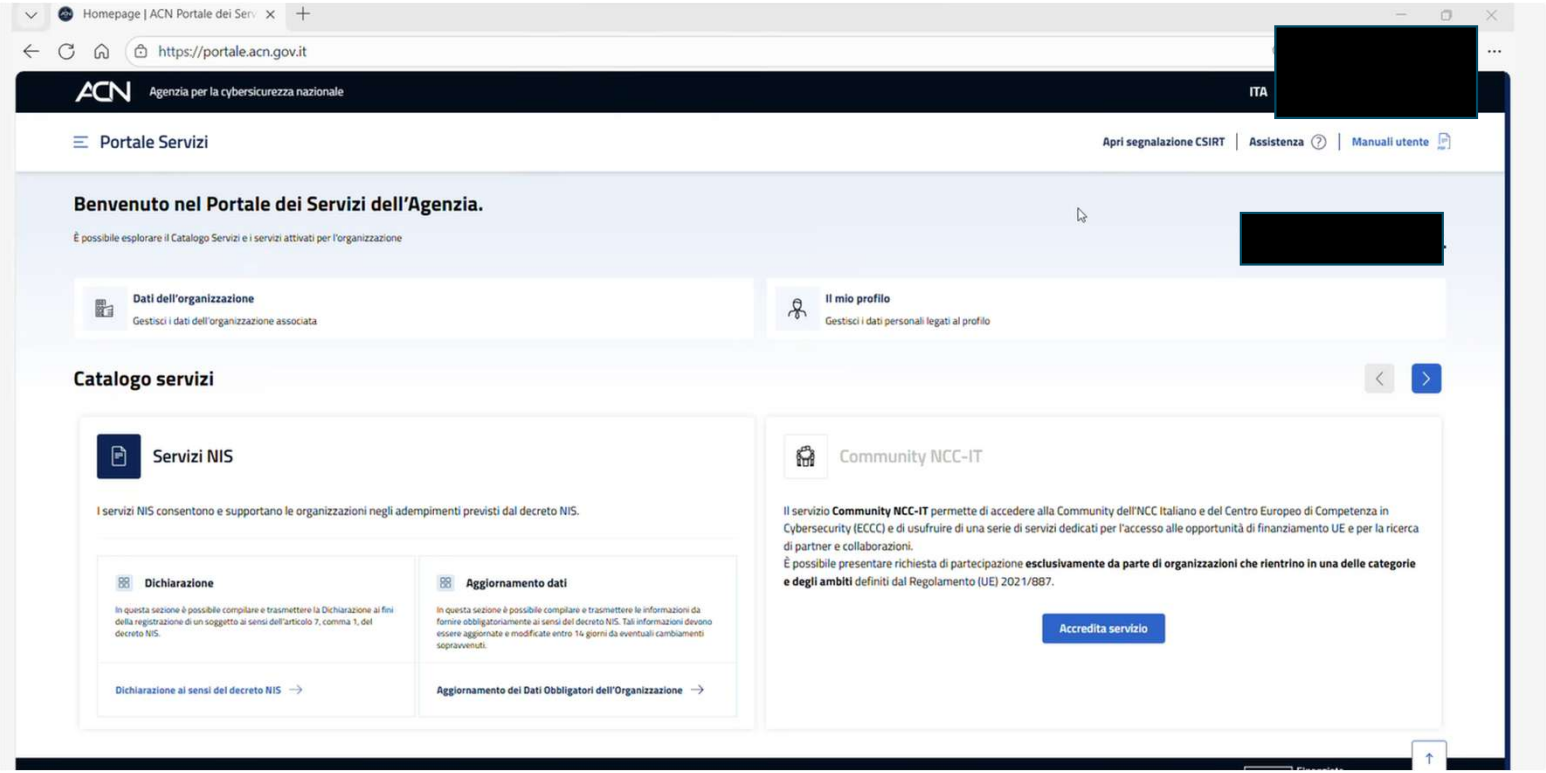
Gestione delle segnalazioni volontarie

Il CSIRT Italia:
a) tratta le notifiche volontarie applicando la **procedura ordinaria**;
b) tratta le **notifiche di incidenti significativi prioritariamente** rispetto alle notifiche volontarie;
c) tratta le **notifiche volontarie** soltanto qualora ciò **non costituisca un onere sproporzionato** o **eccessivo**.

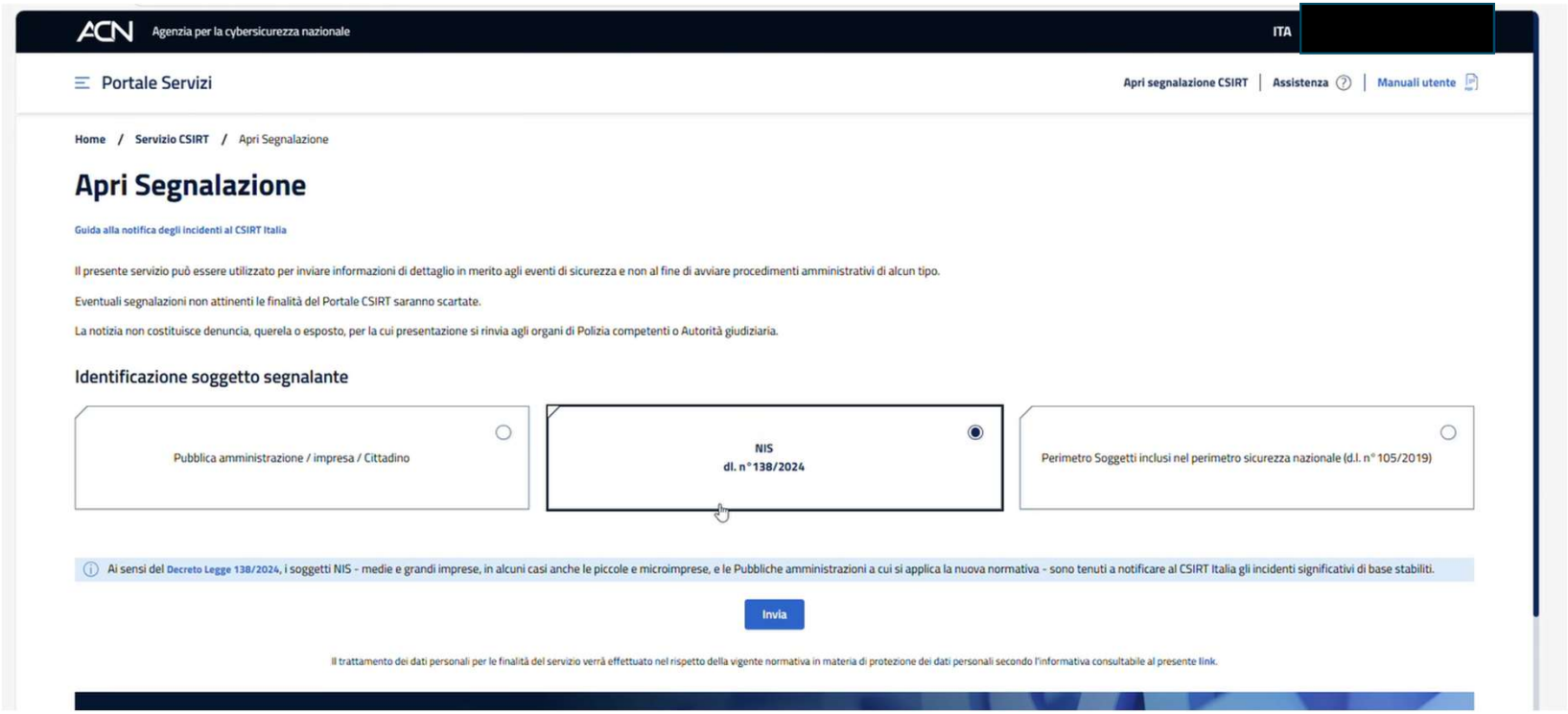
Agenda

- Recepimento e attuazione e prossime scadenze
- Applicazione della normativa – Le specifiche di base e alcuni approfondimenti
- Applicazione della normativa – Il piano di gestione degli incidenti e le notifiche
- **Simulazione di una notifica di incidente di sicurezza**
- Q&A

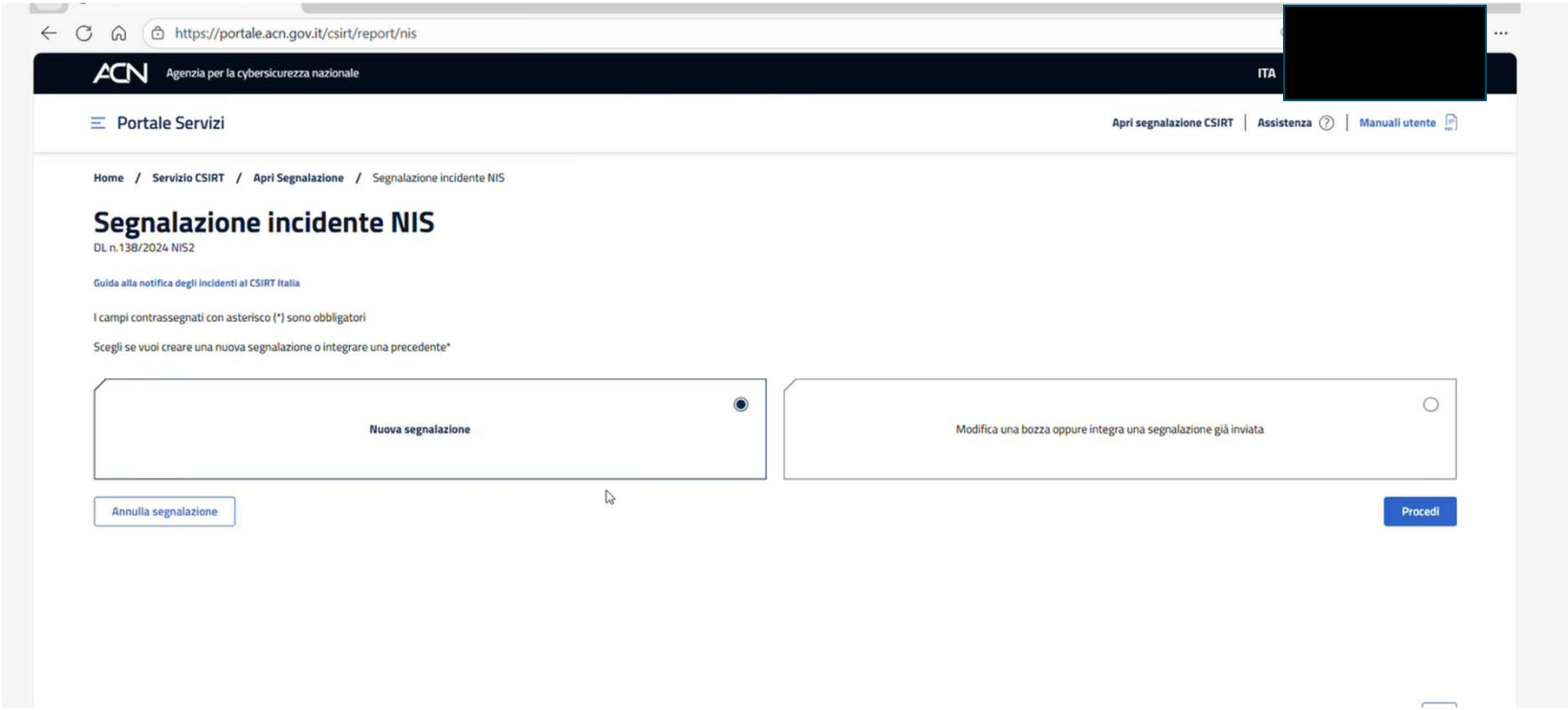
Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione 1/37



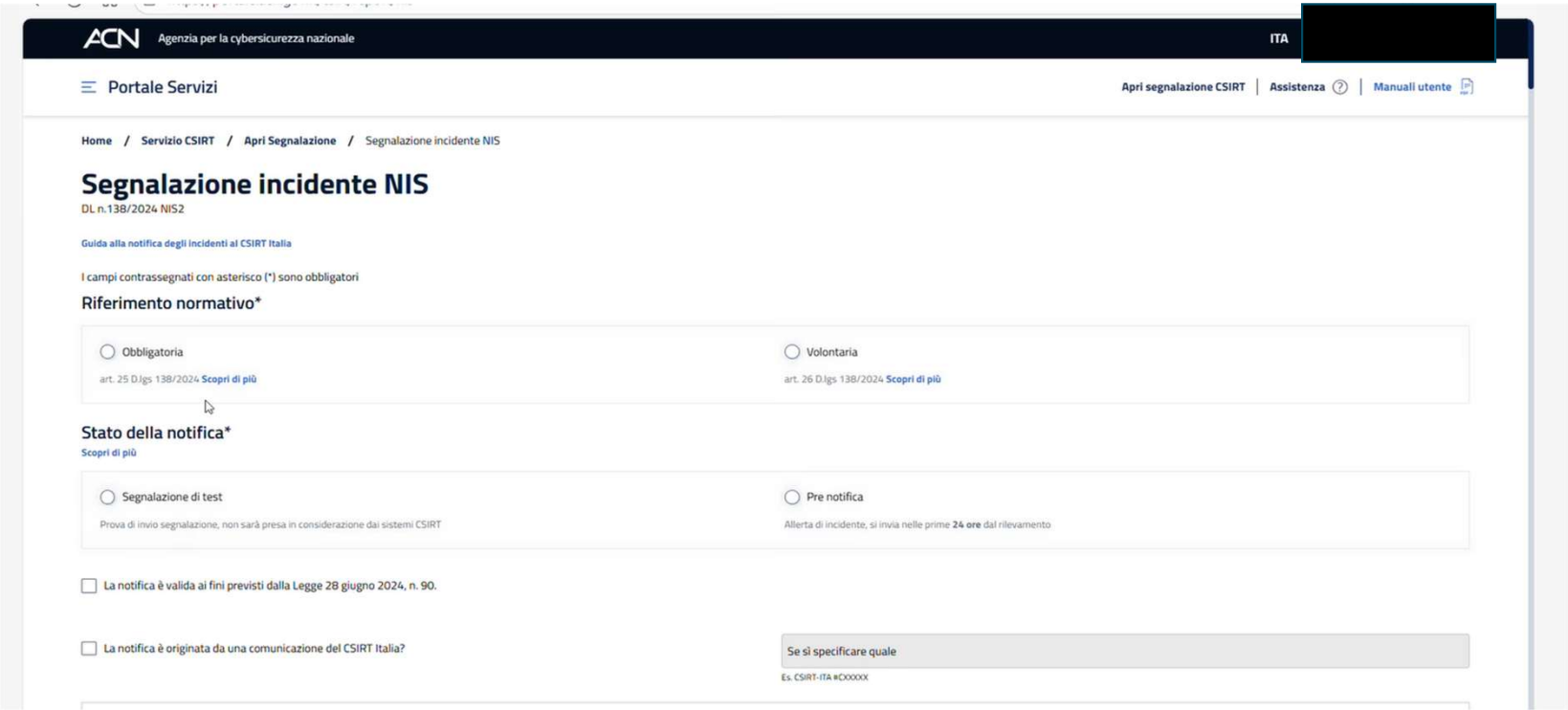
Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione



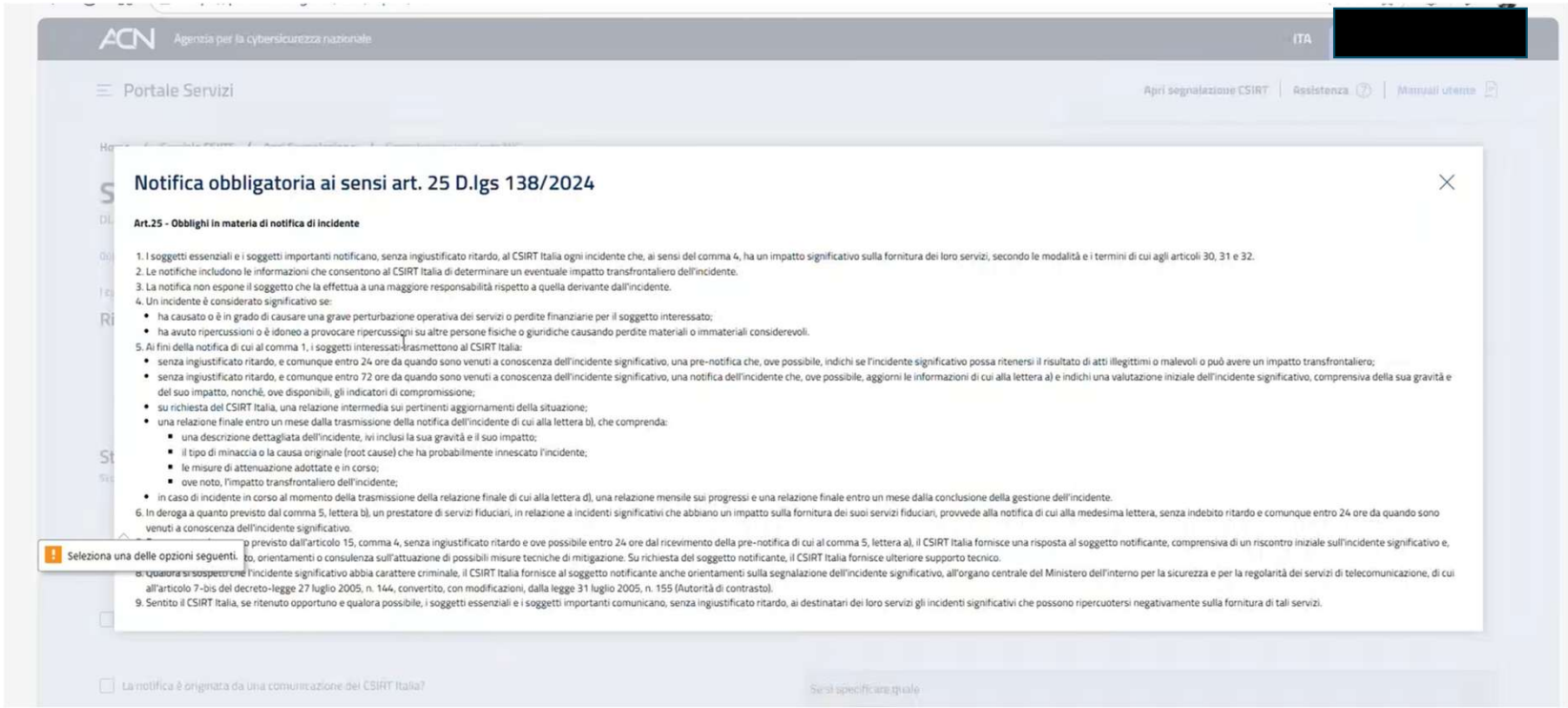
Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione 3/37



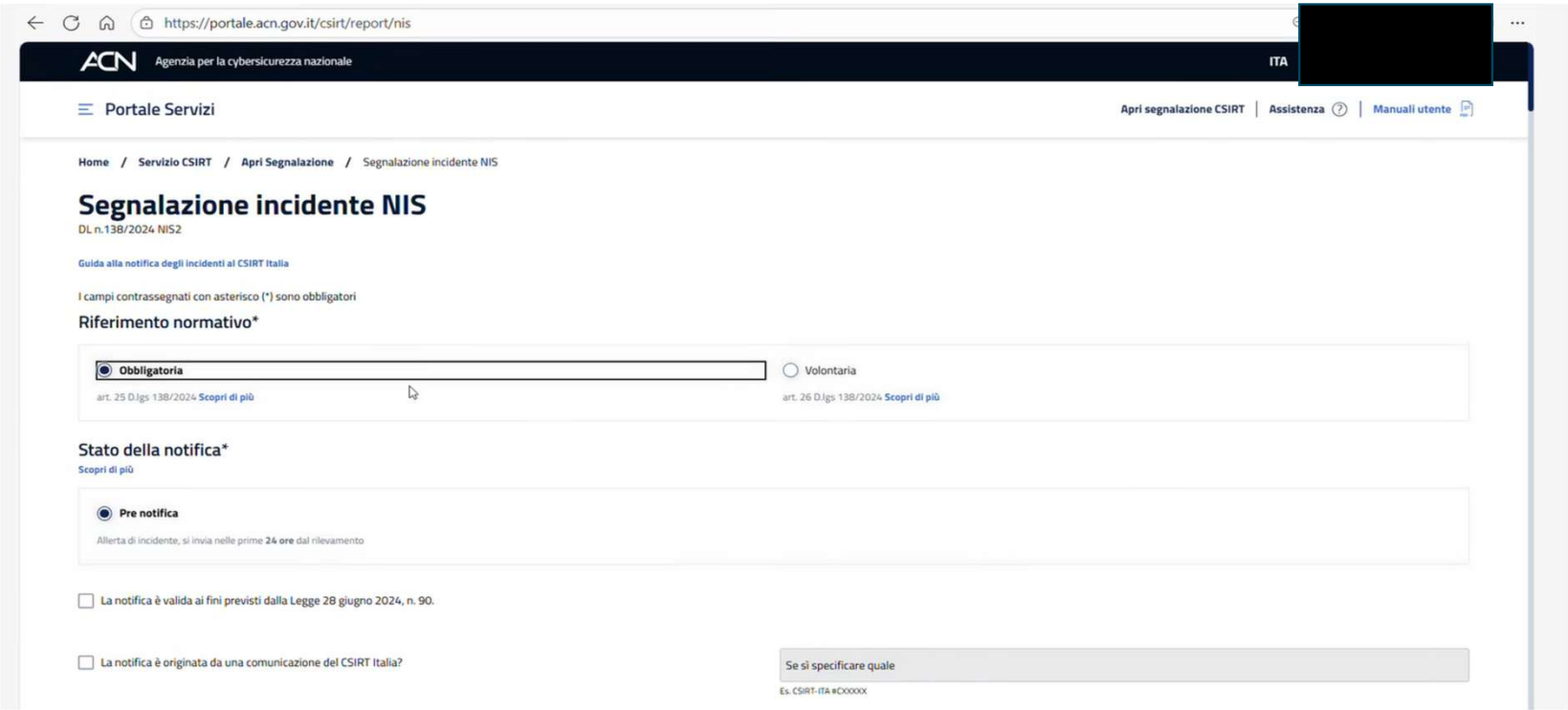
Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione 4/37



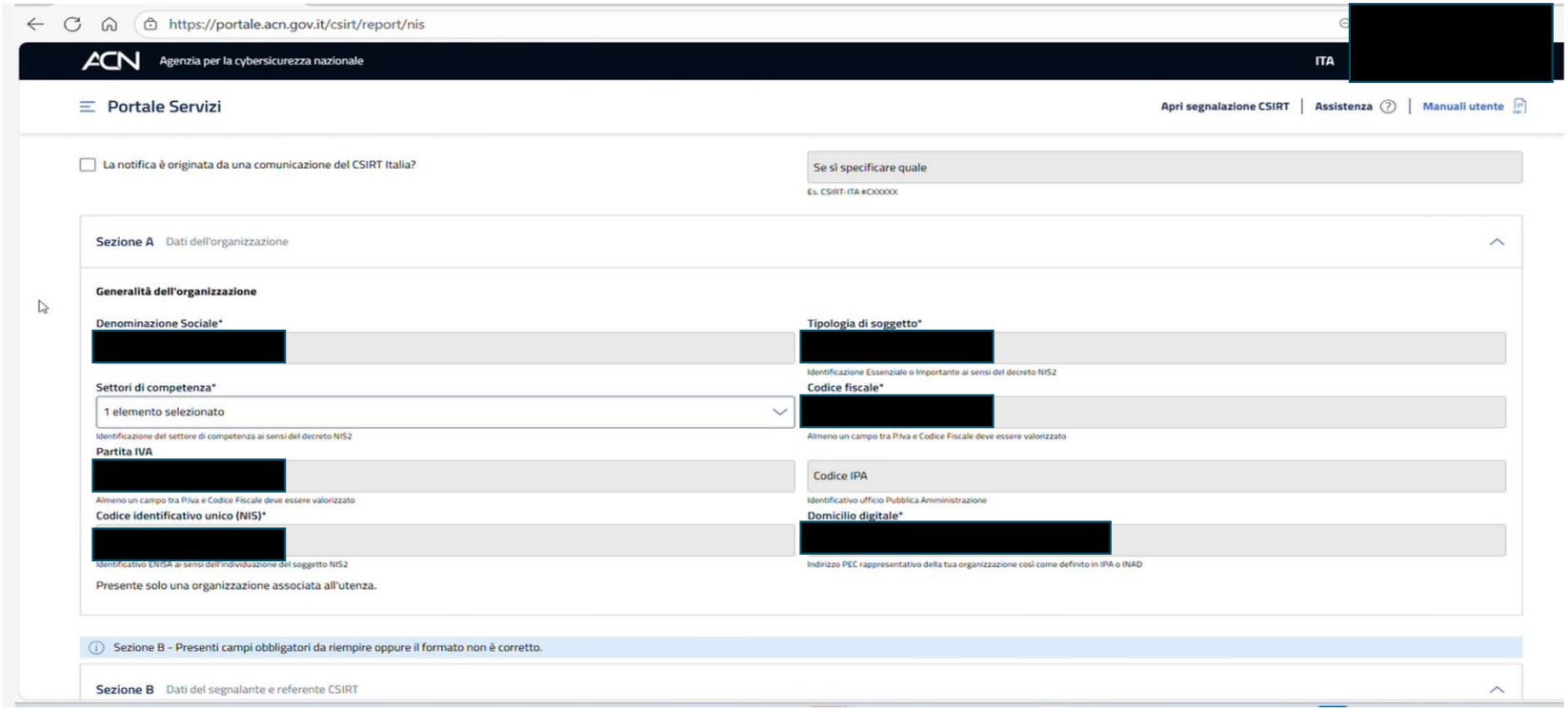
Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione



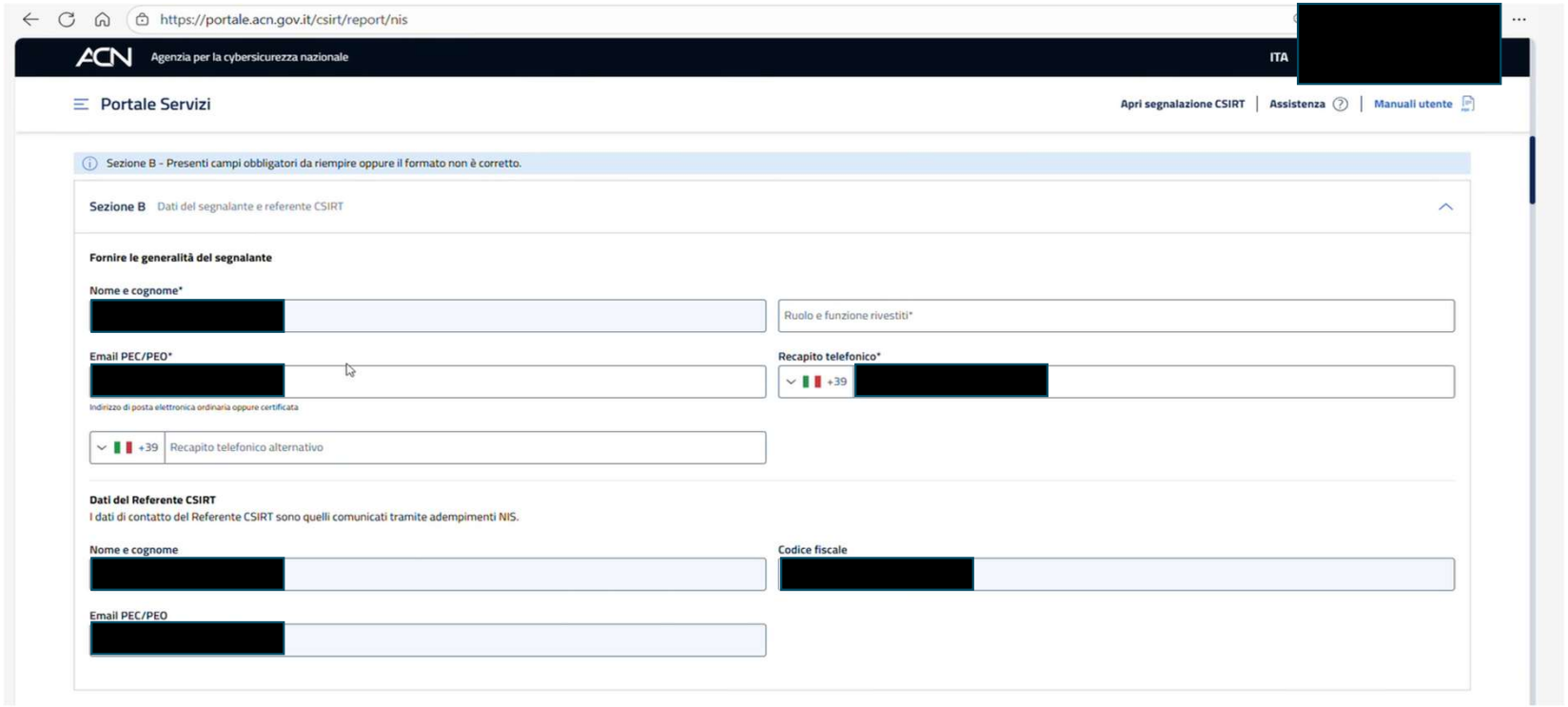
Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione



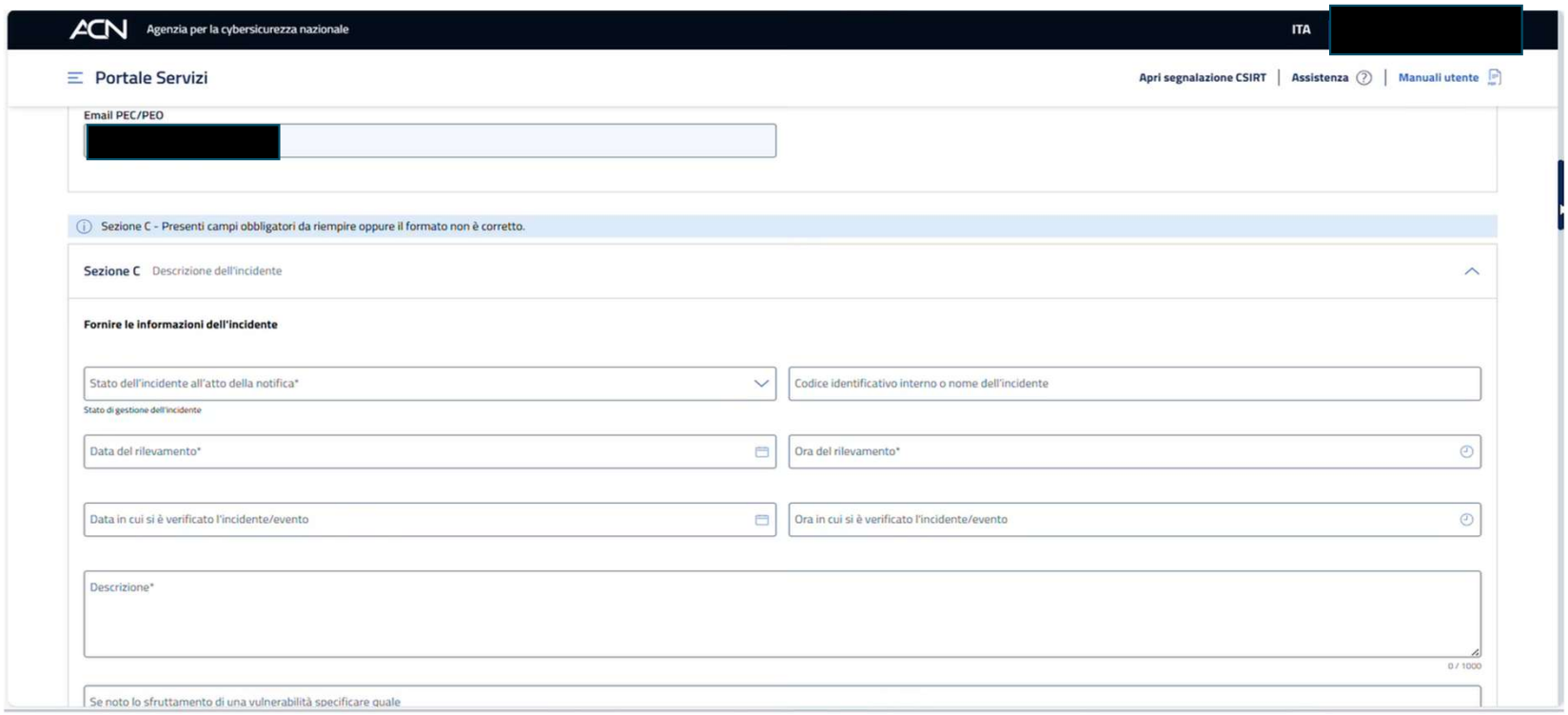
Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione 7/37



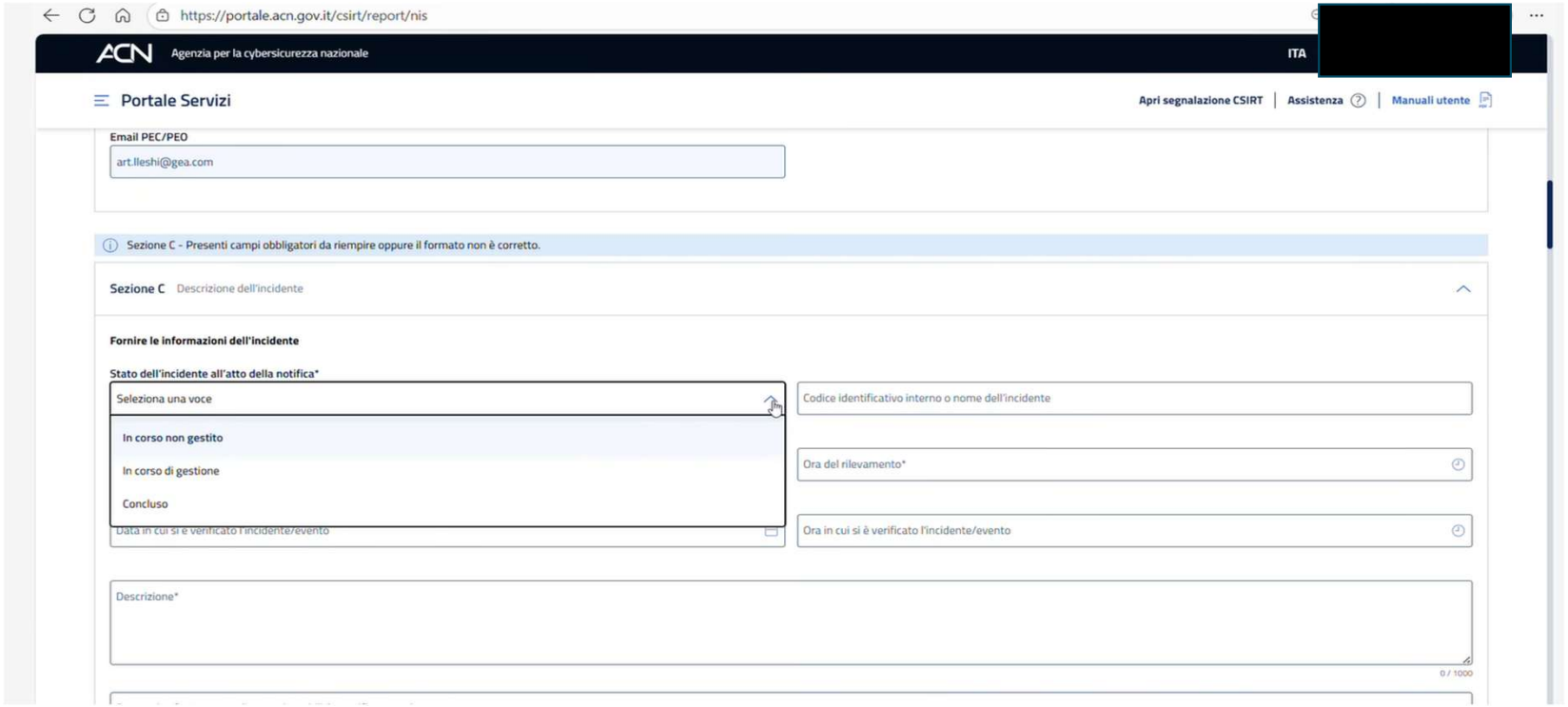
Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione 8/37



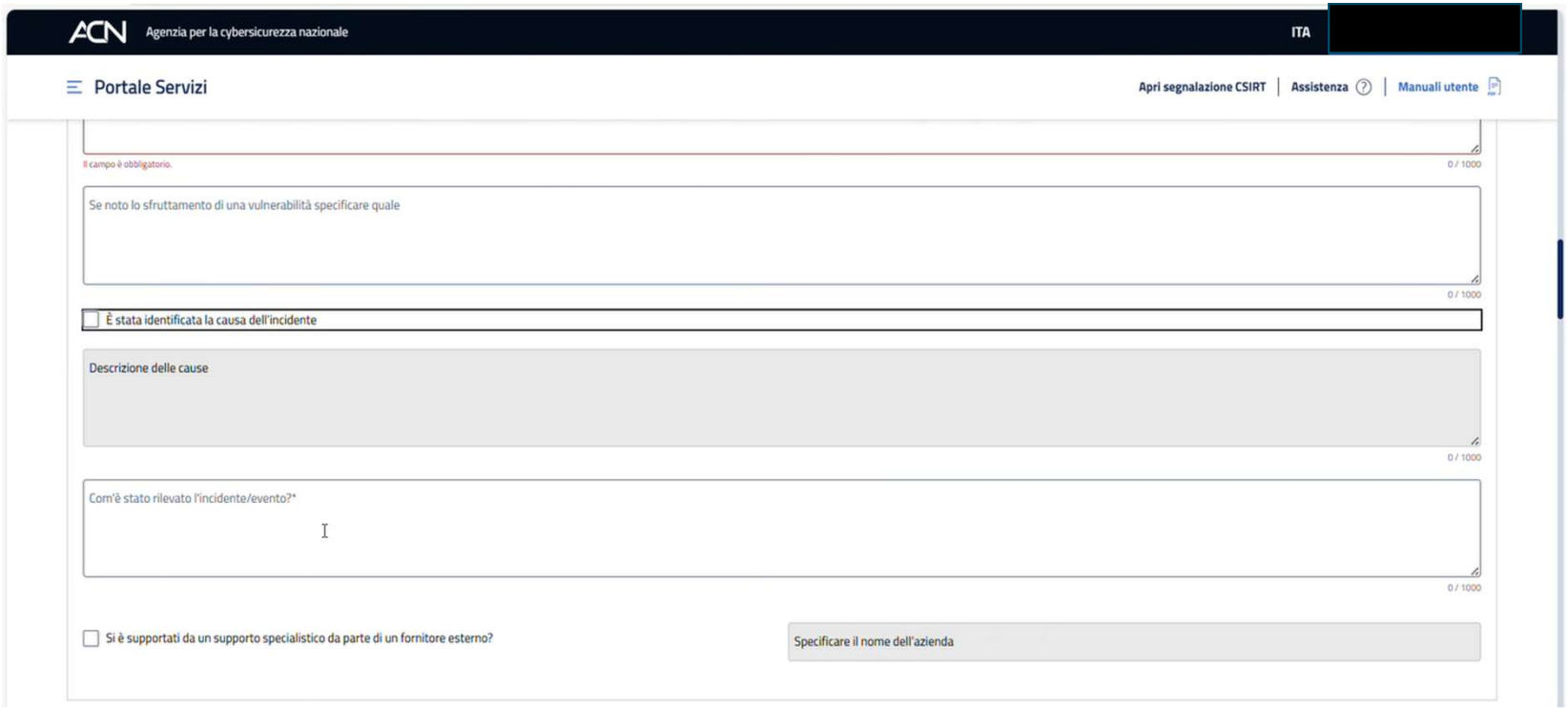
Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione 9/37



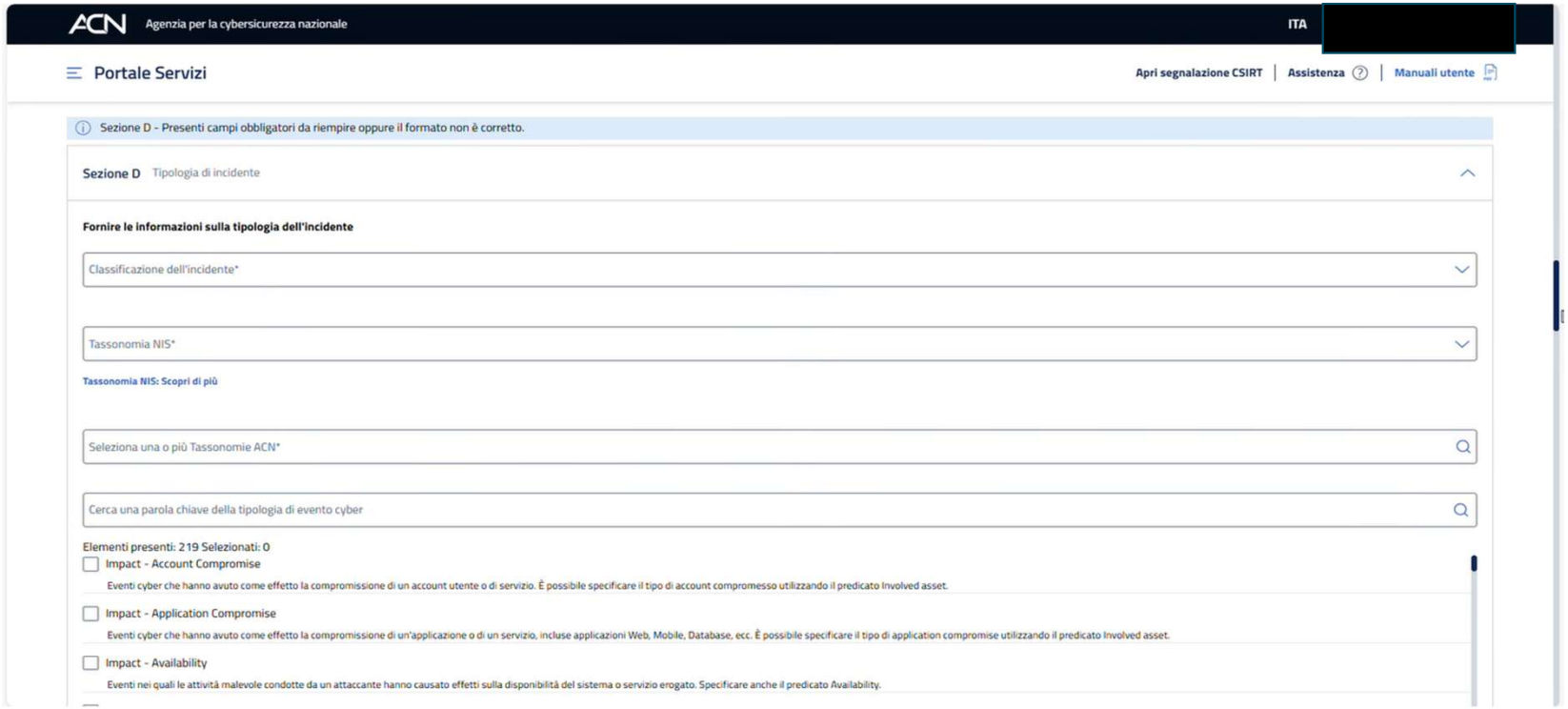
Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione



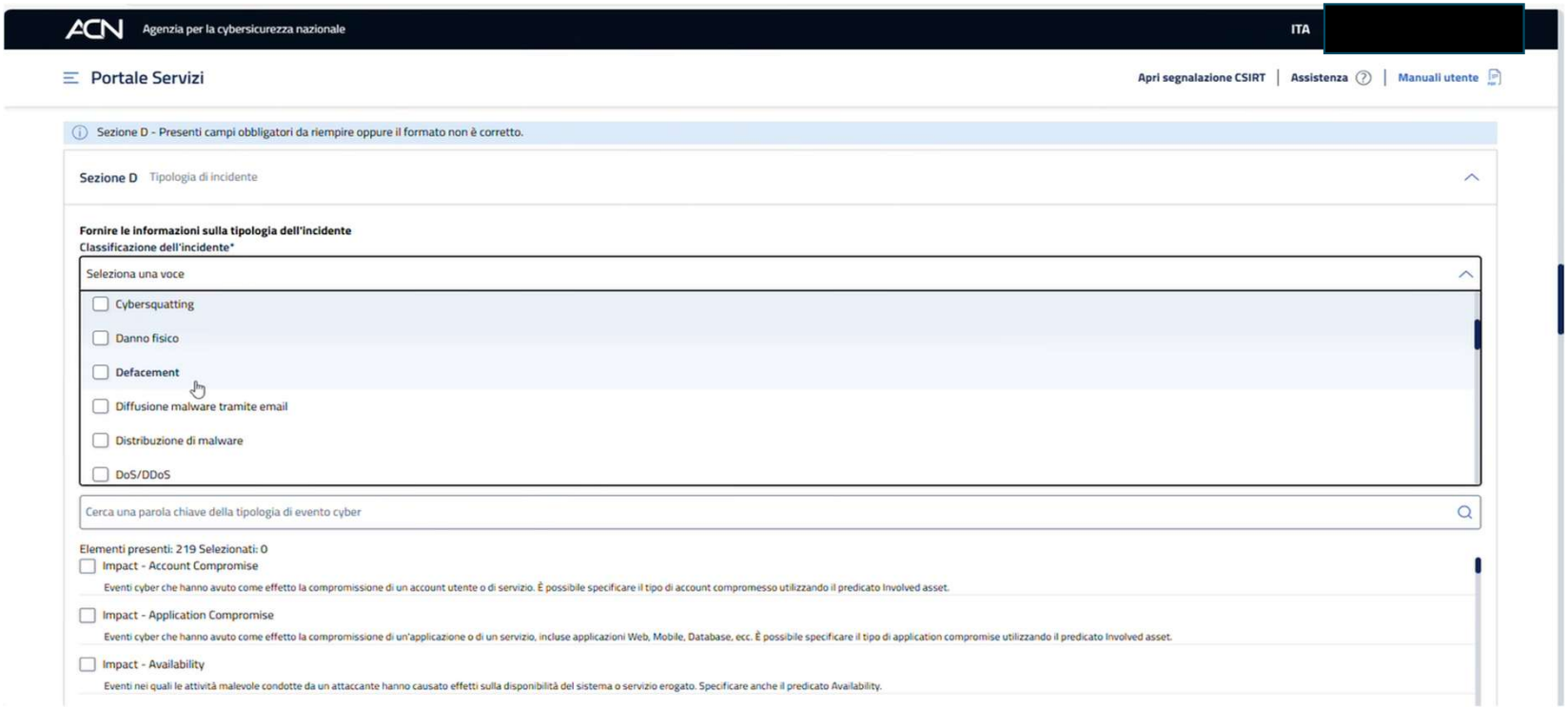
Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione 11/37



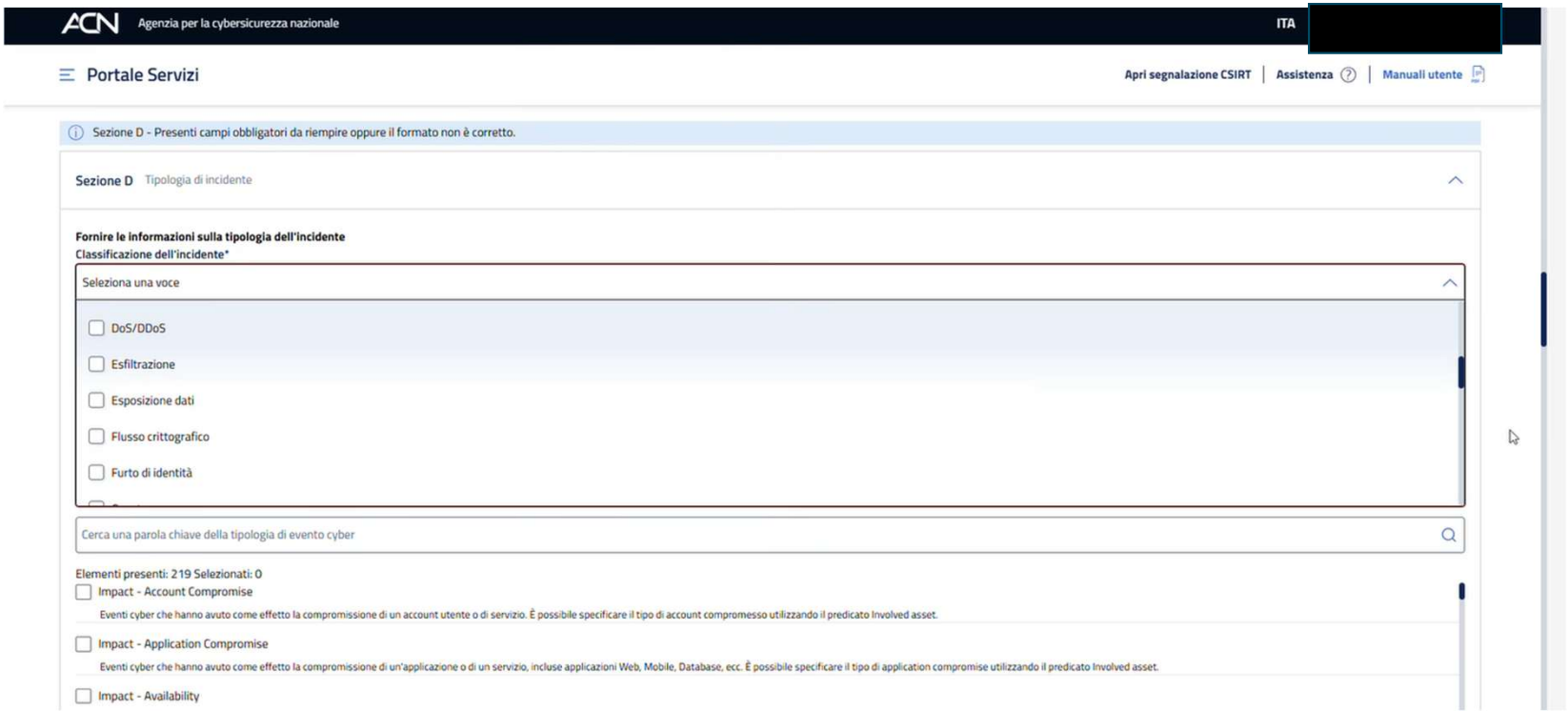
Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione



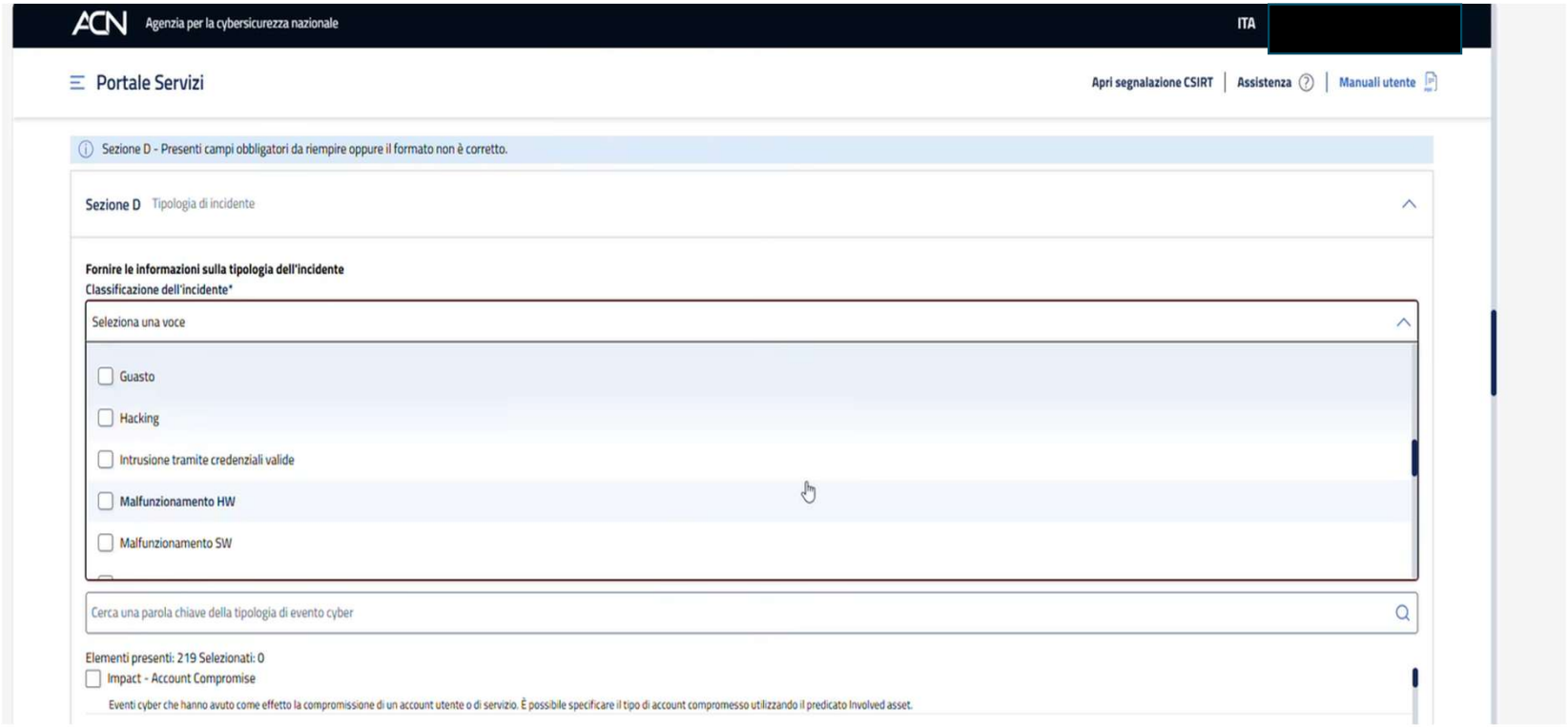
Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione



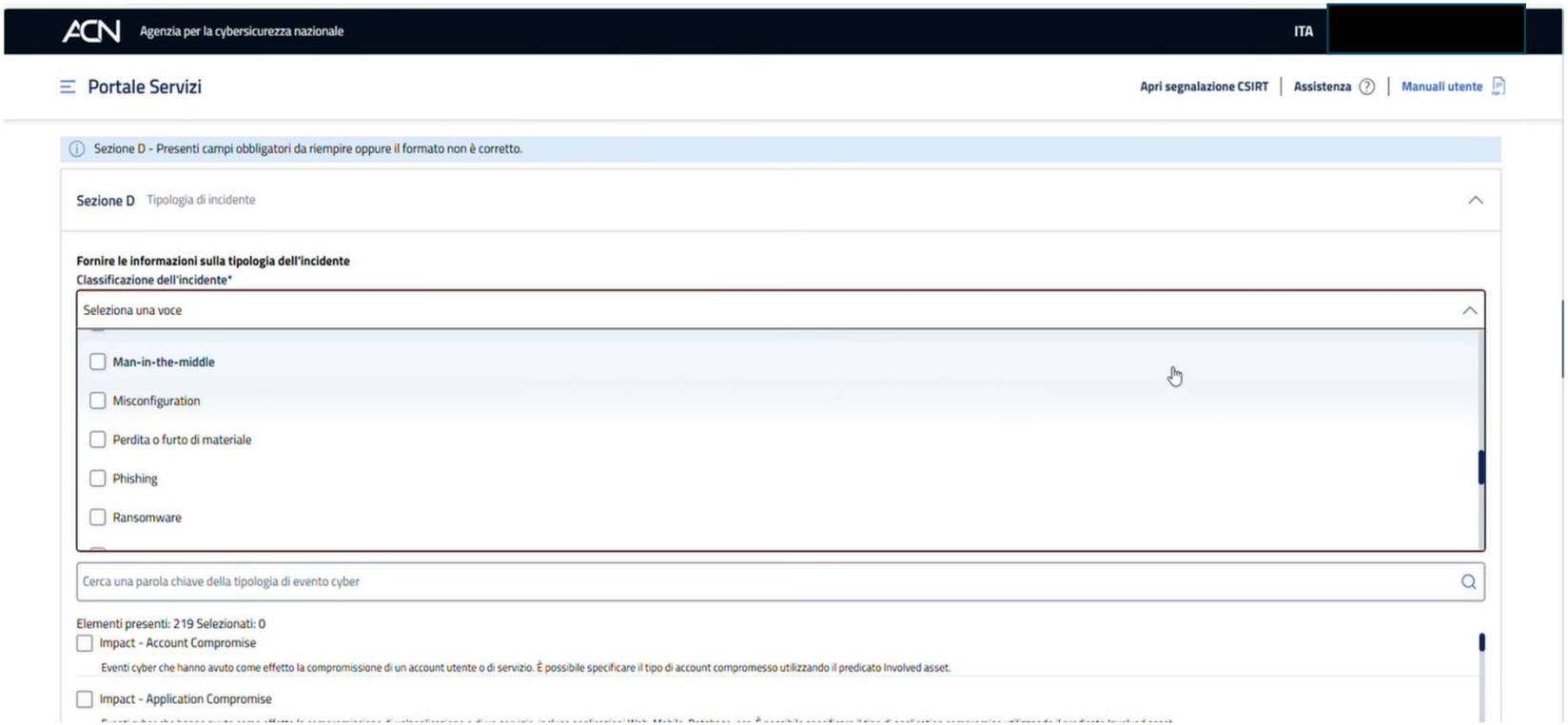
Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione



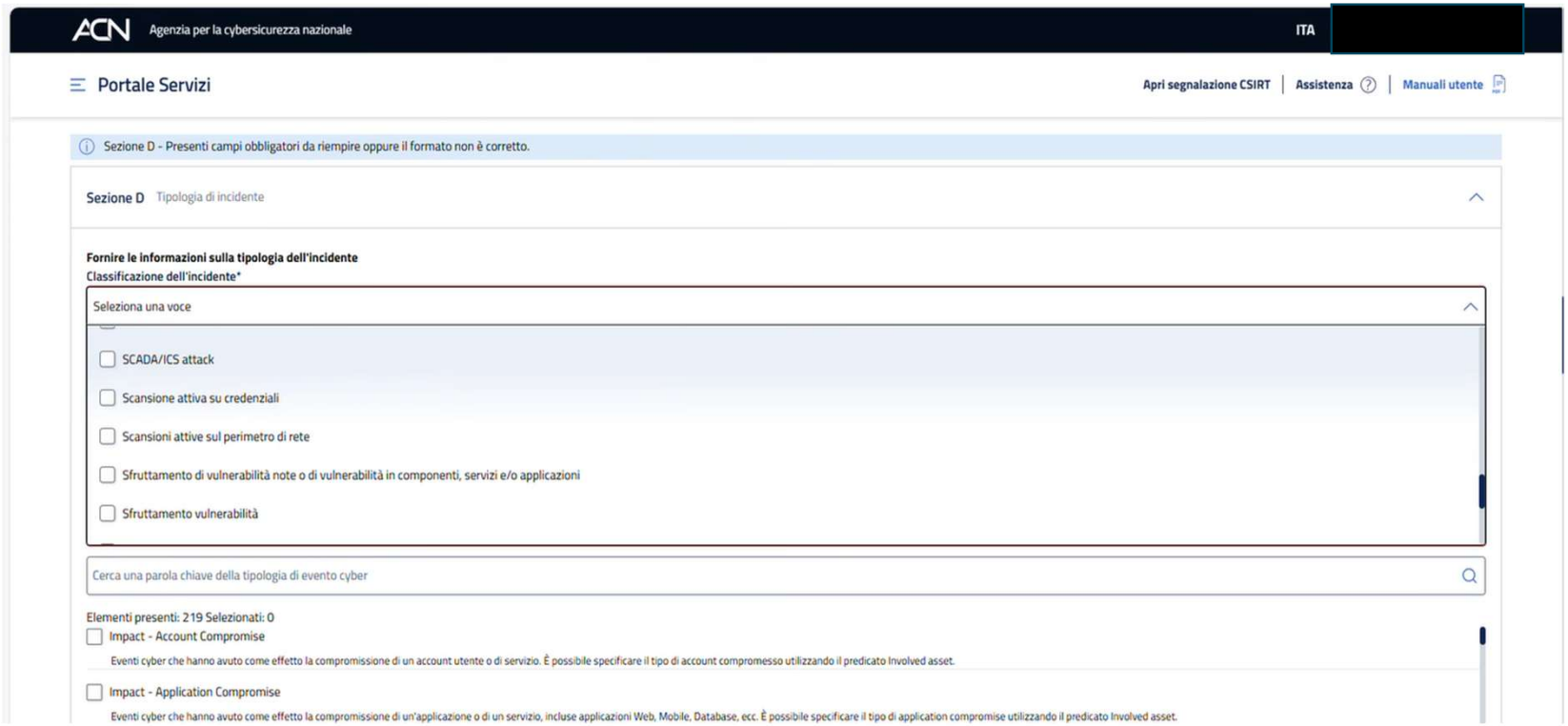
Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione



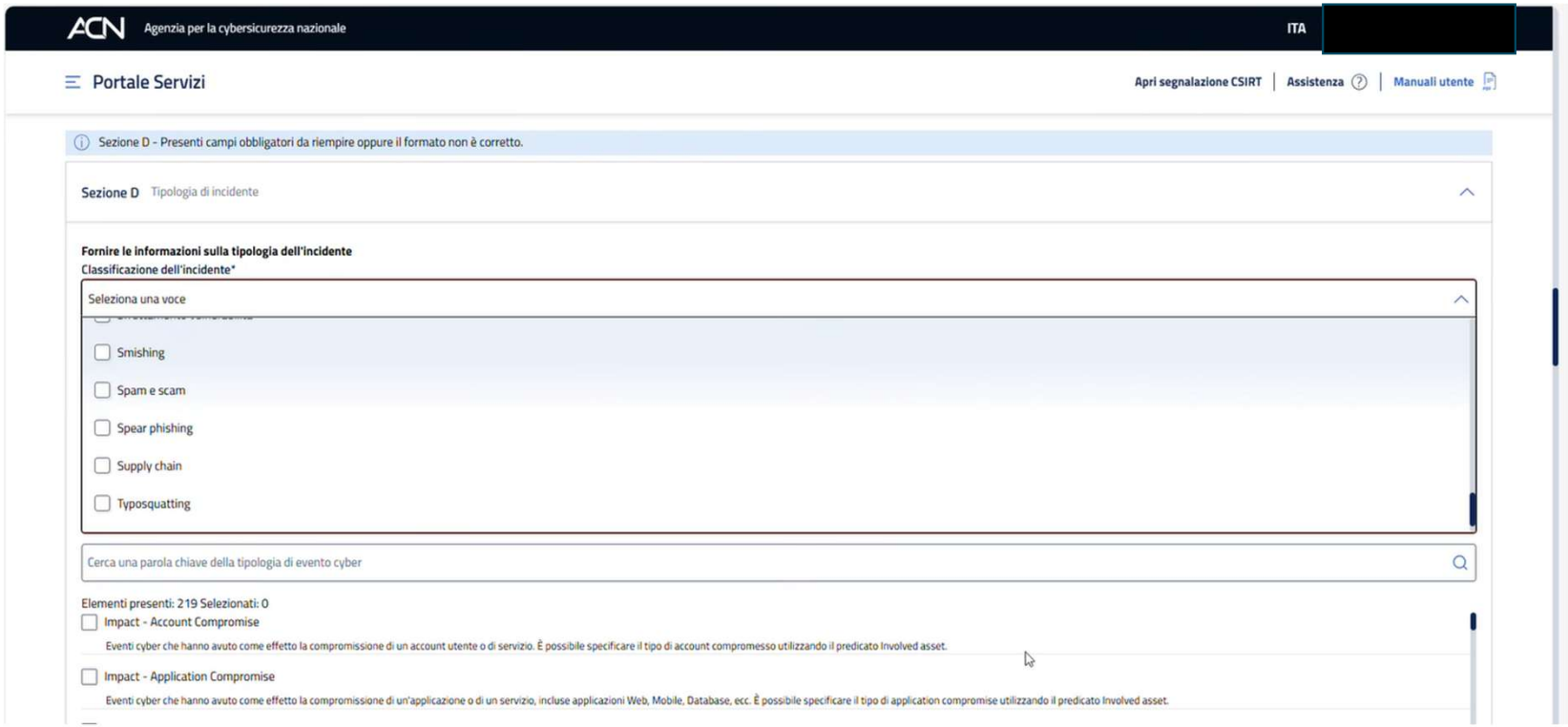
Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione



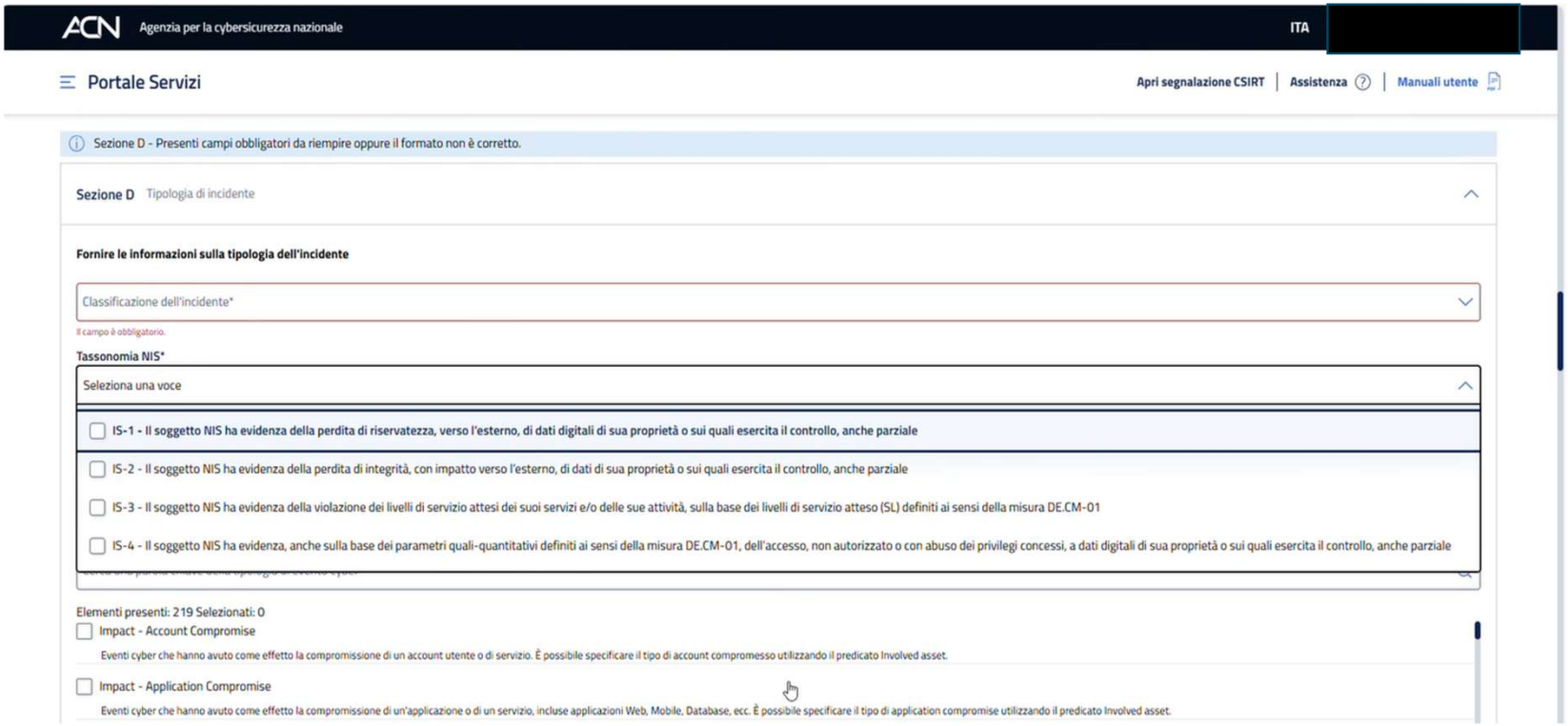
Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione



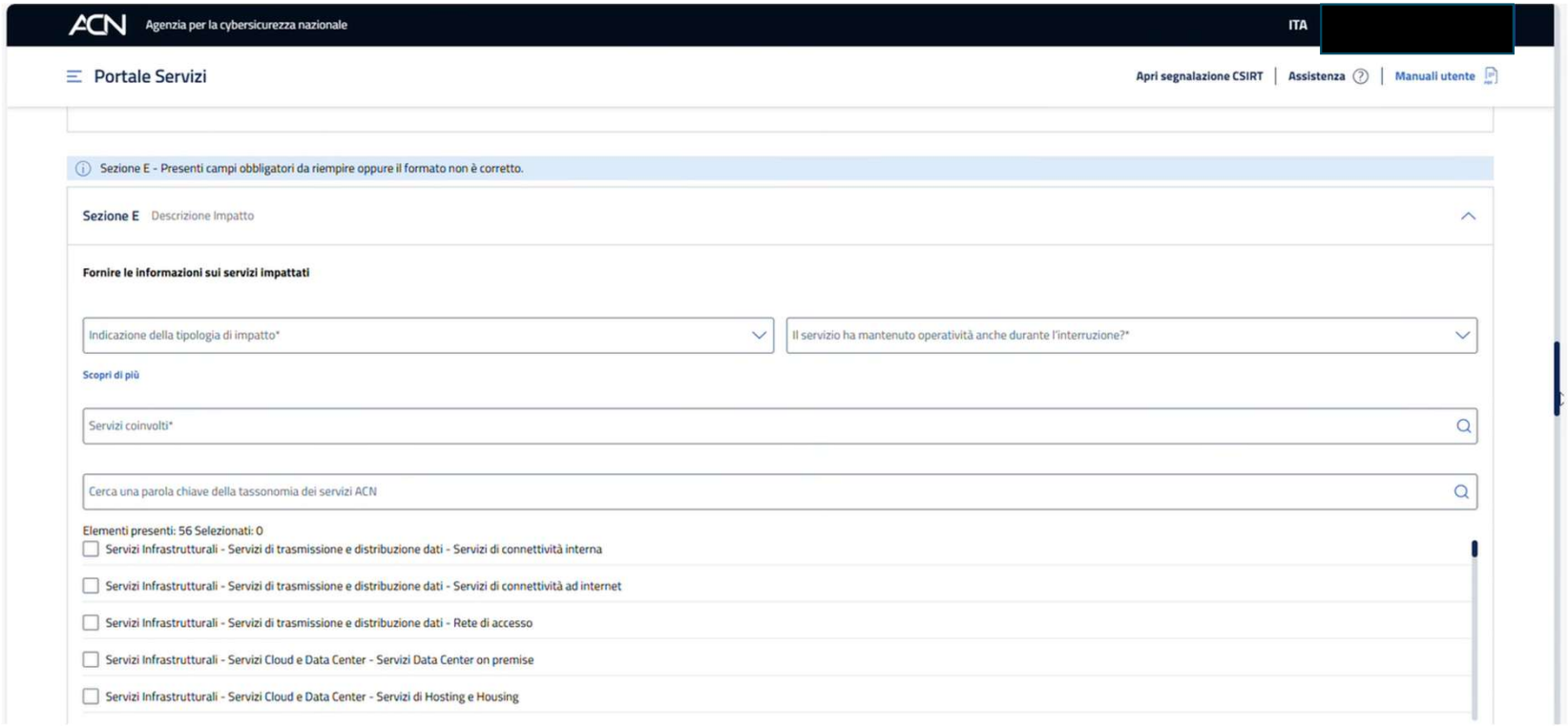
Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione



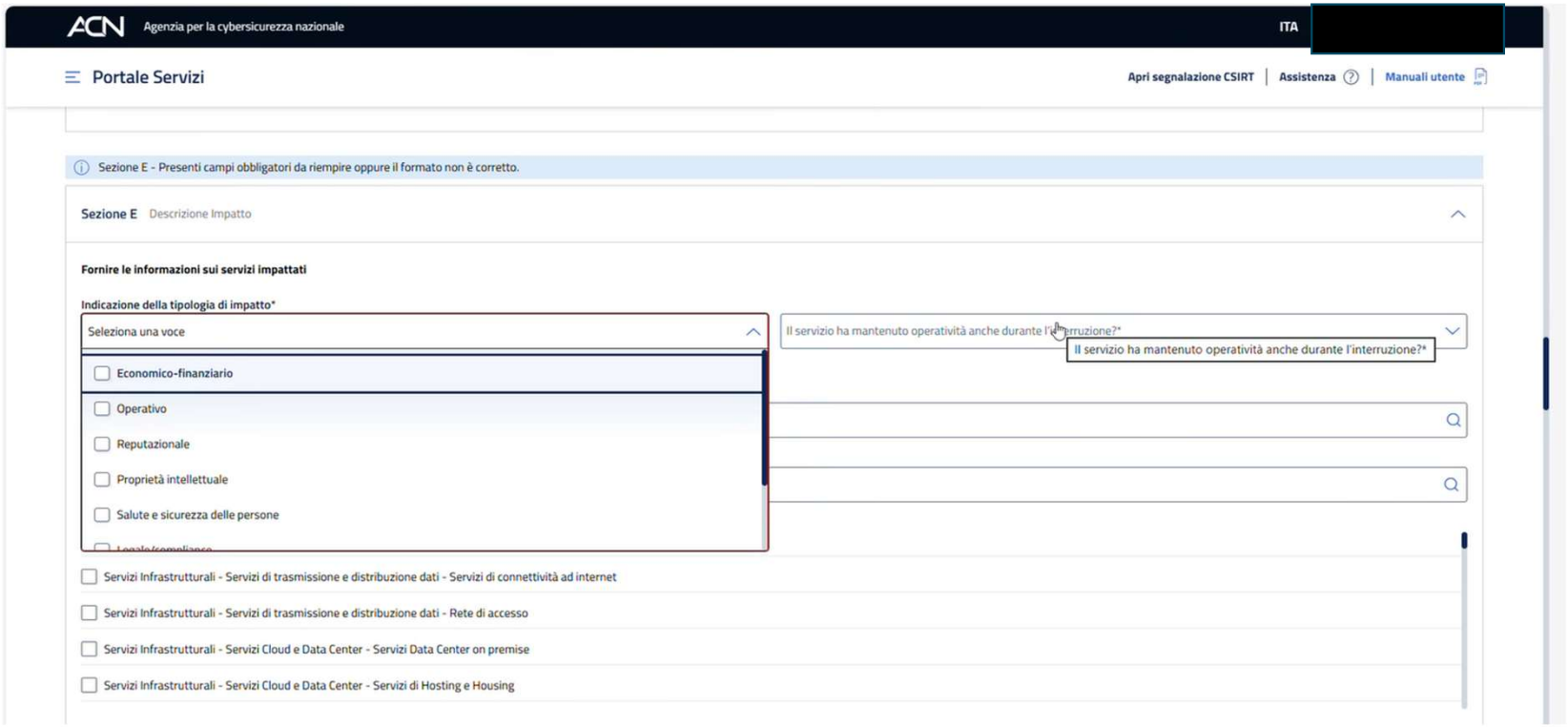
Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione



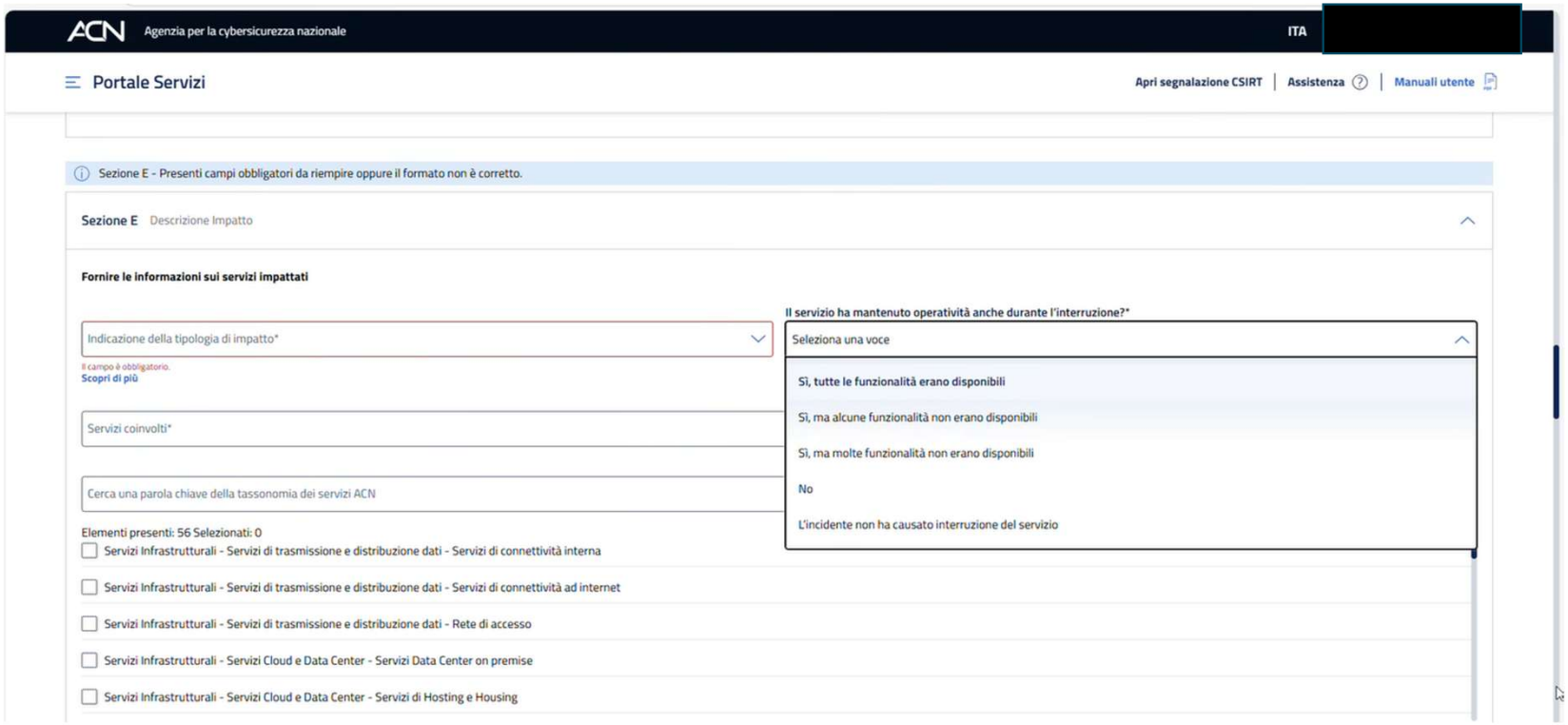
Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione



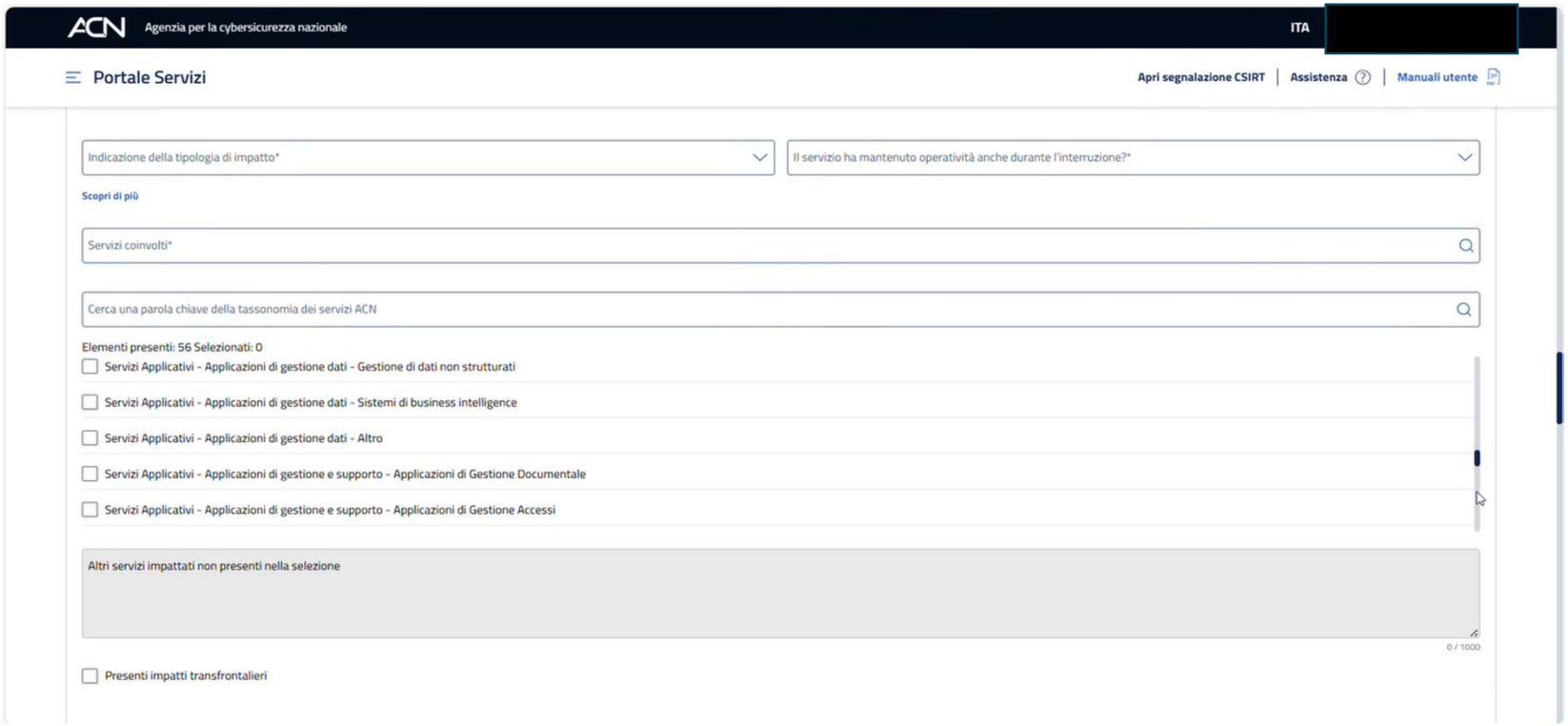
Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione



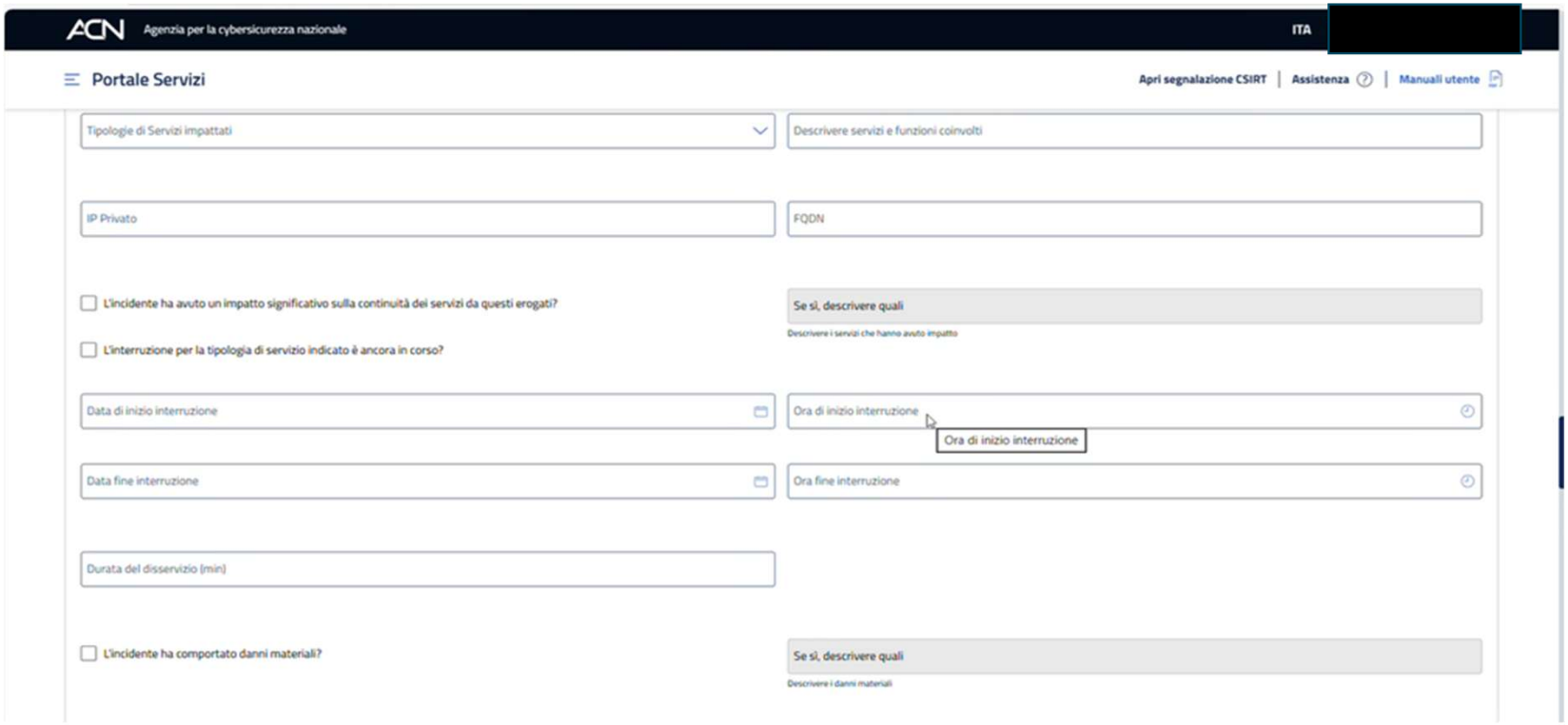
Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione



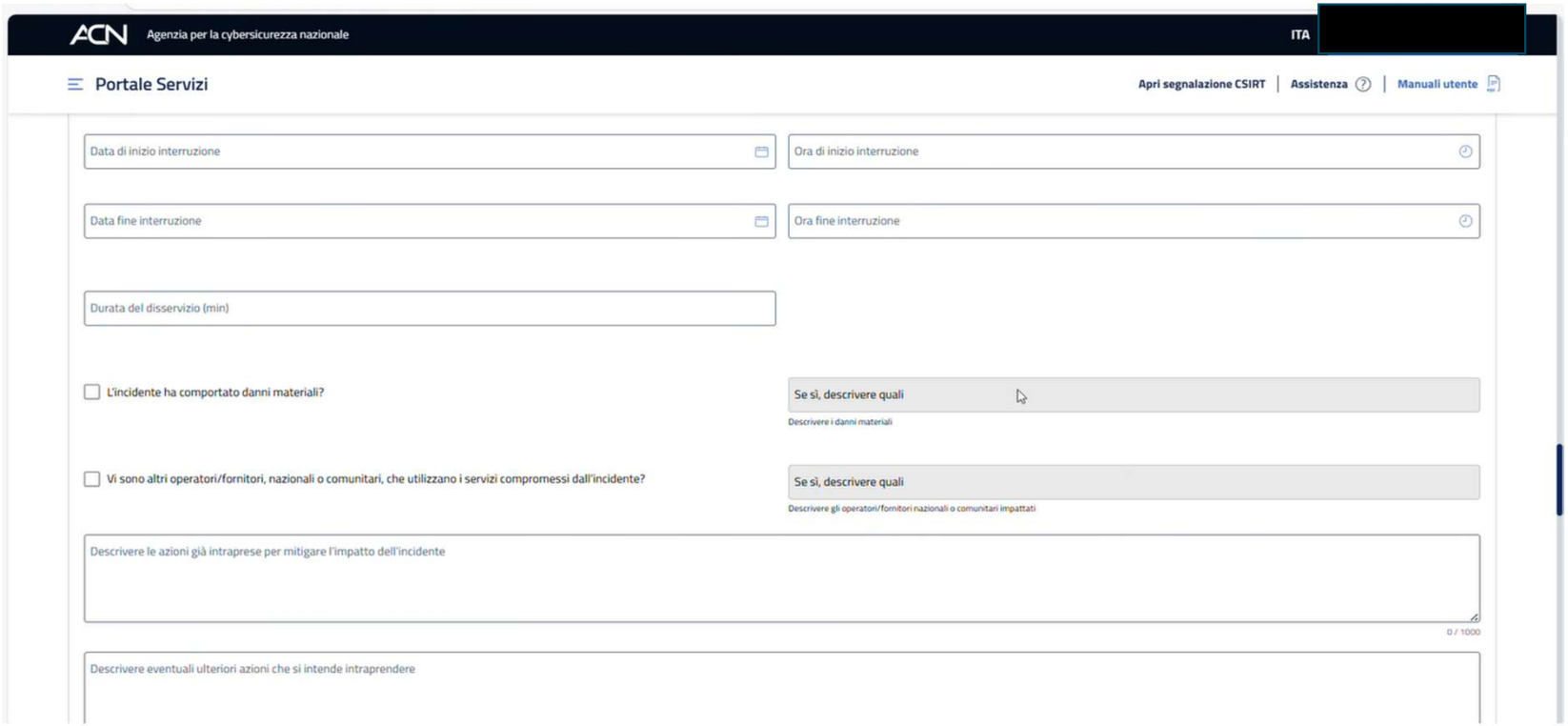
Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione



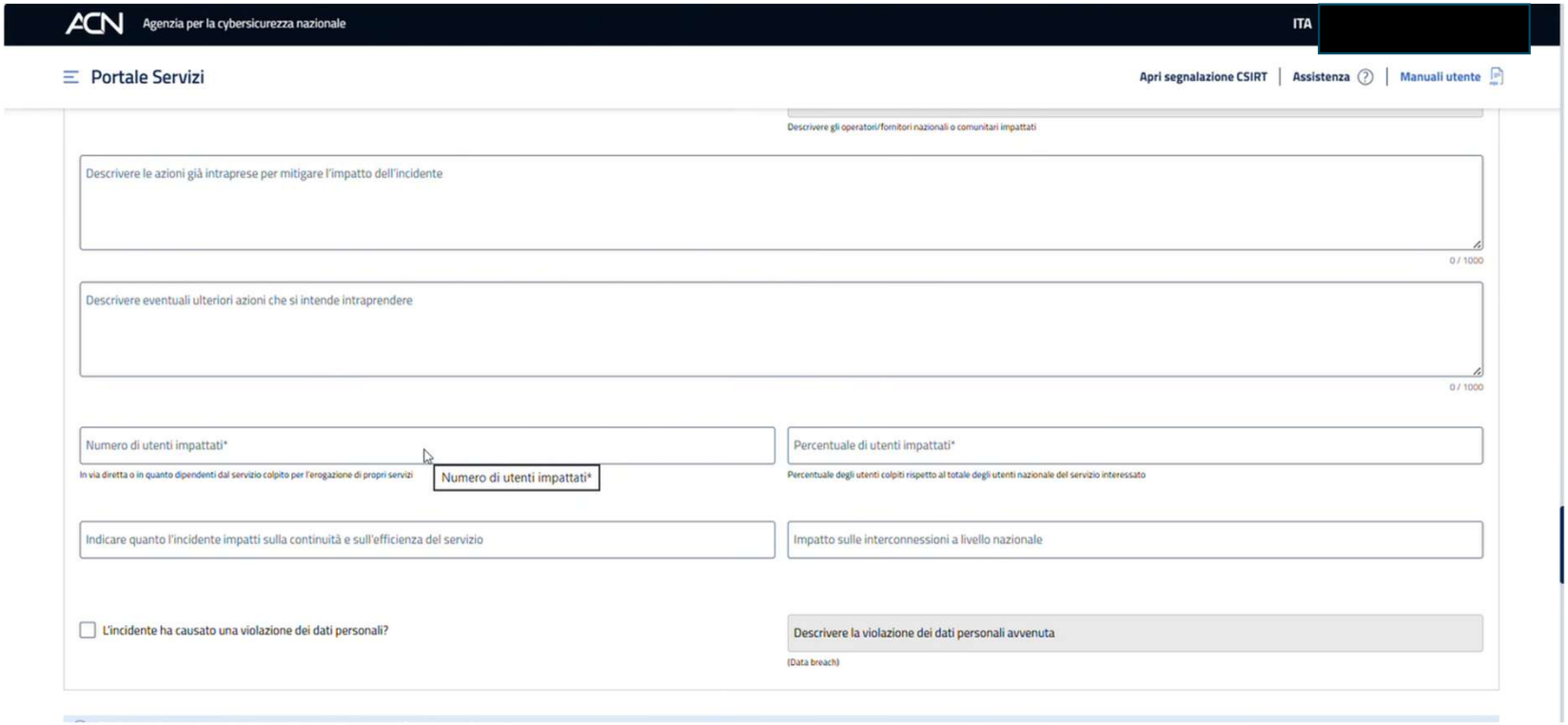
Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione



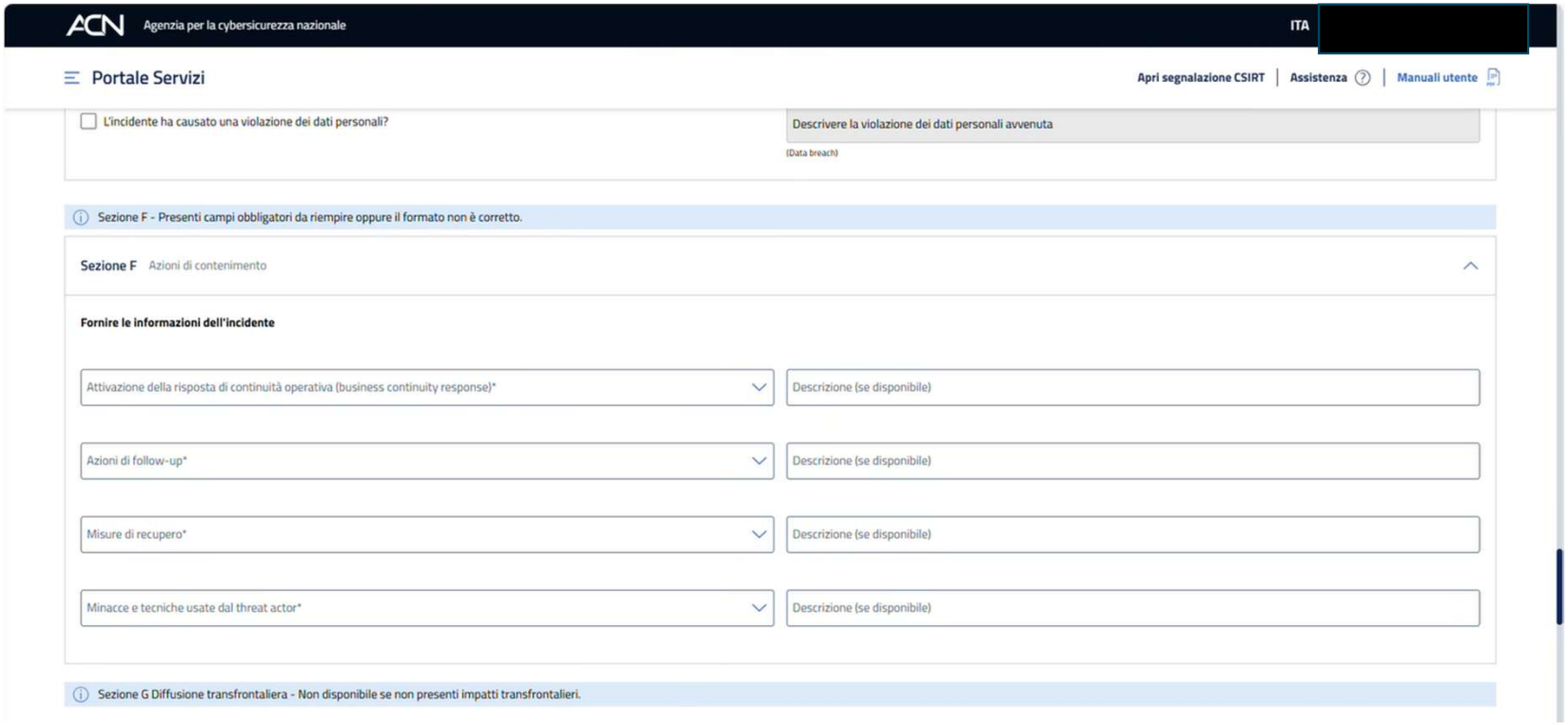
Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione



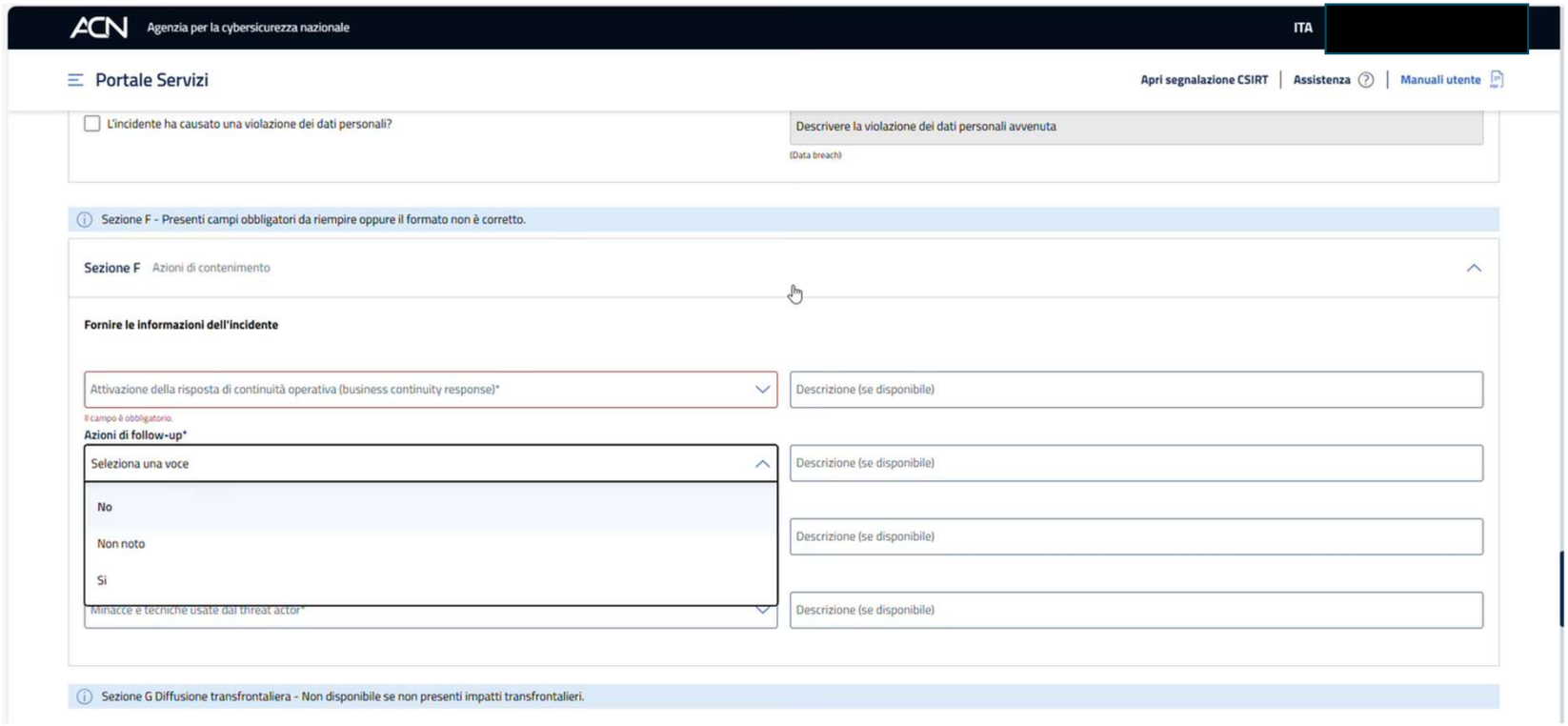
Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione



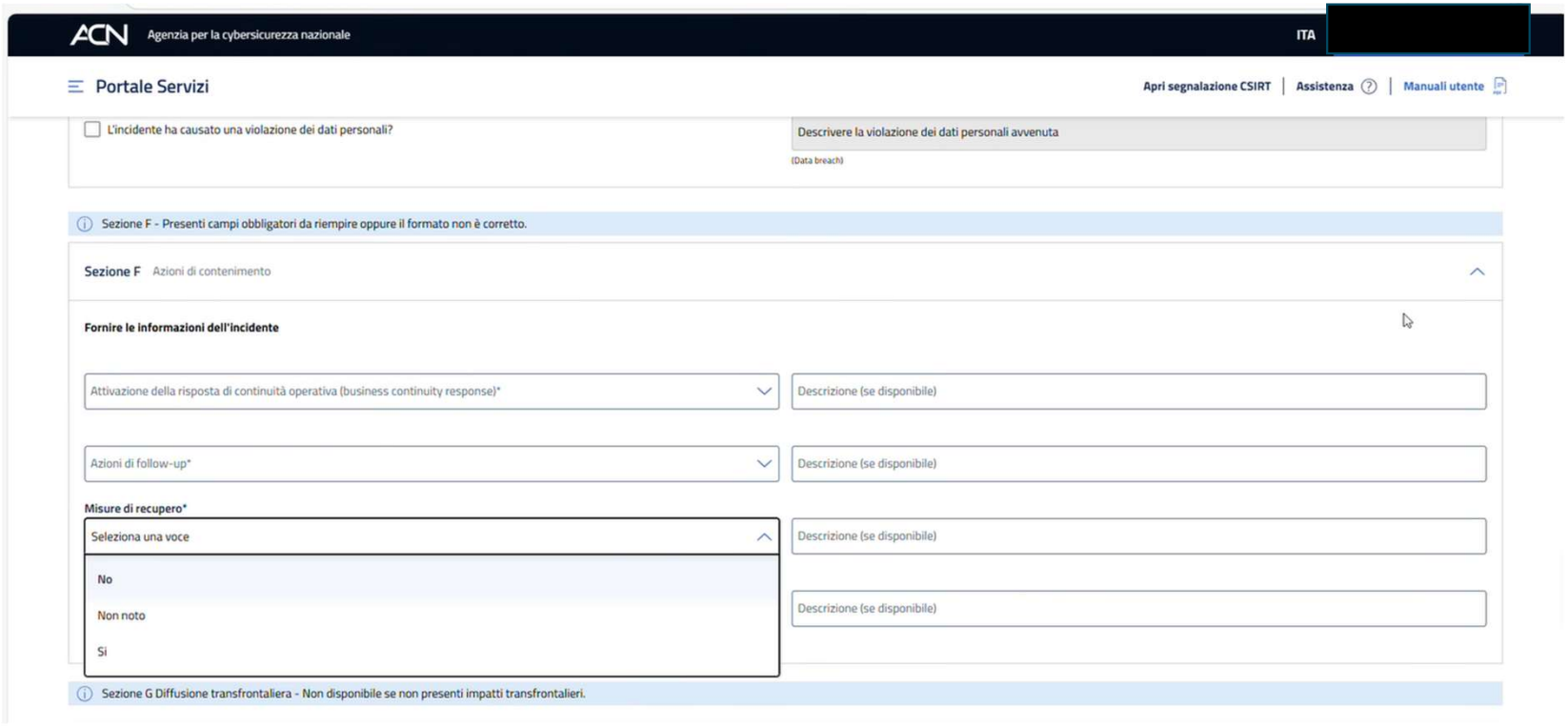
Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione



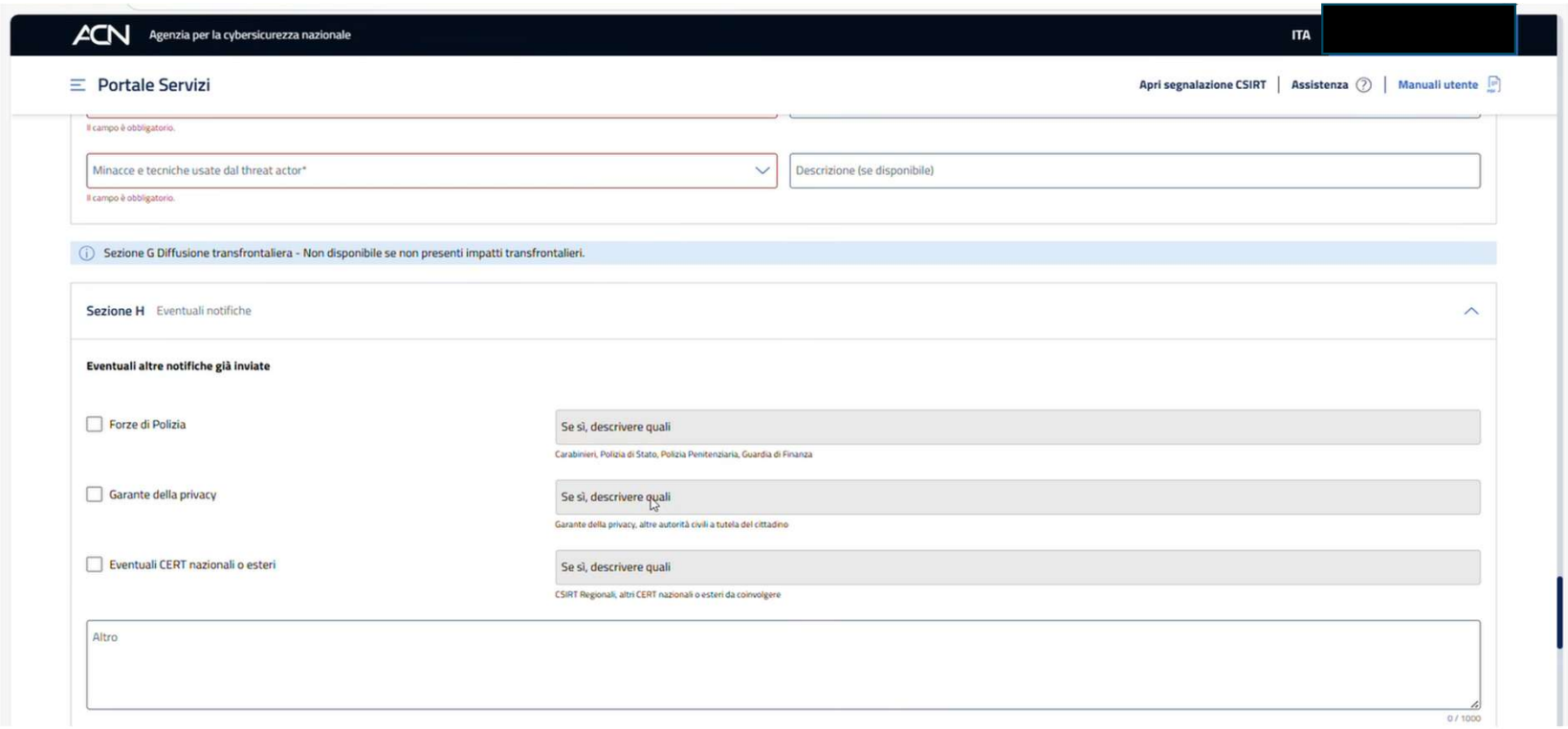
Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione



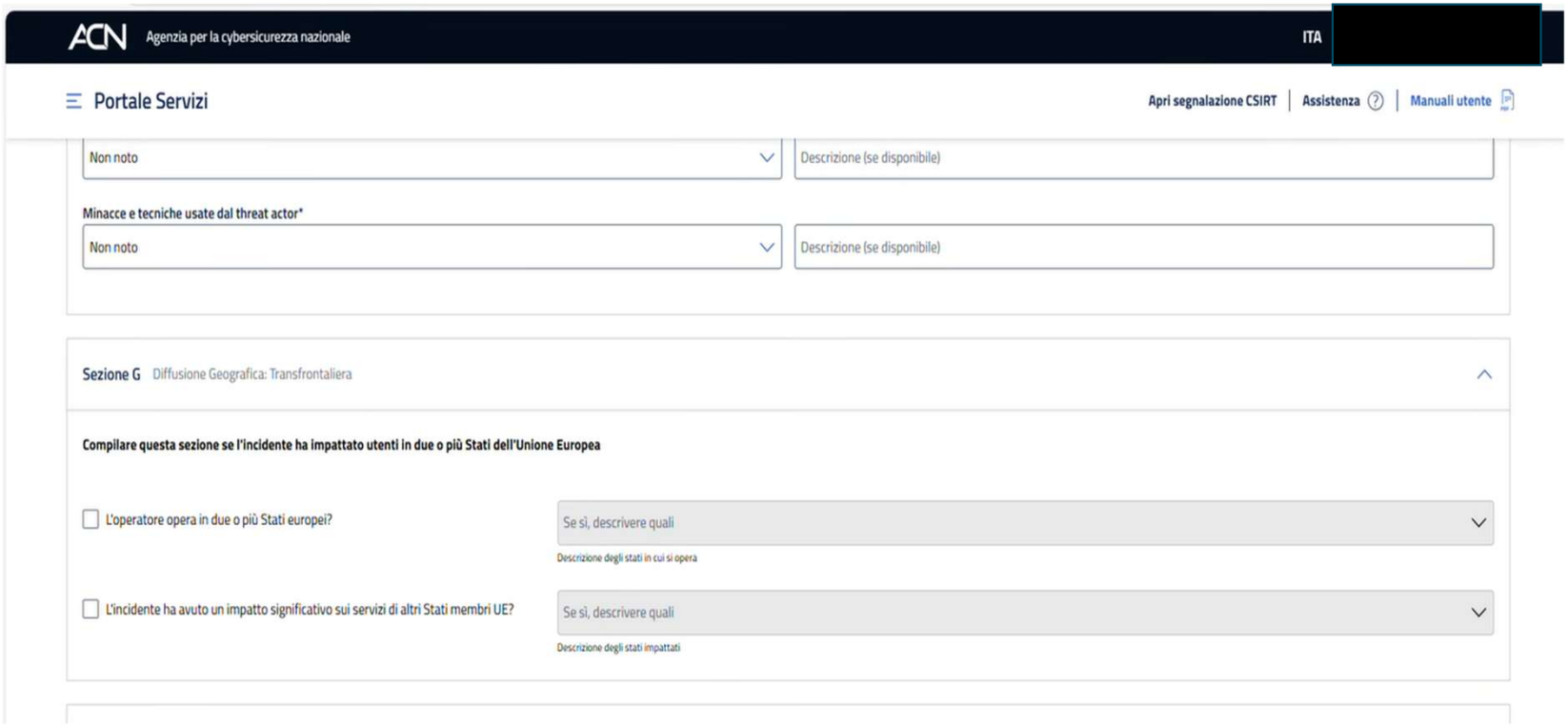
Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione



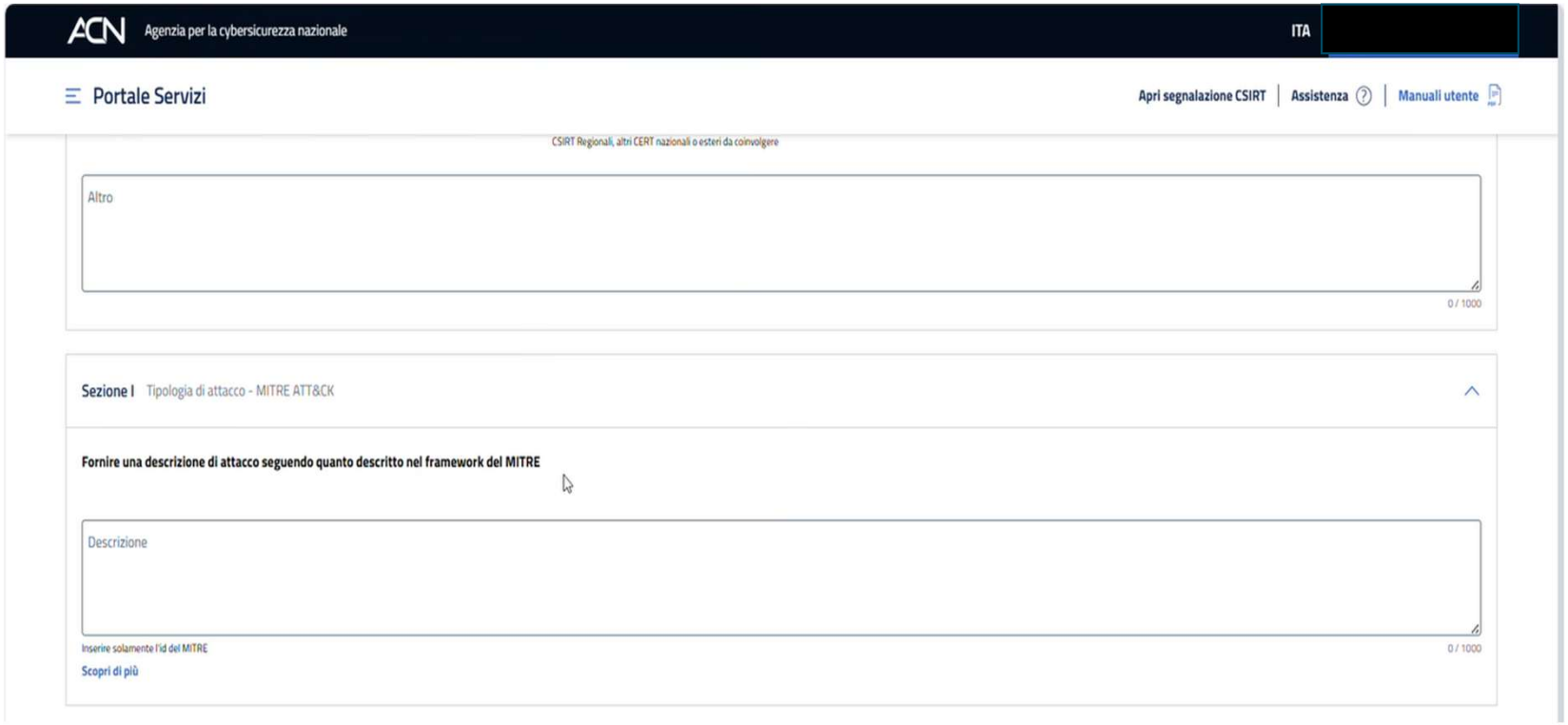
Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione



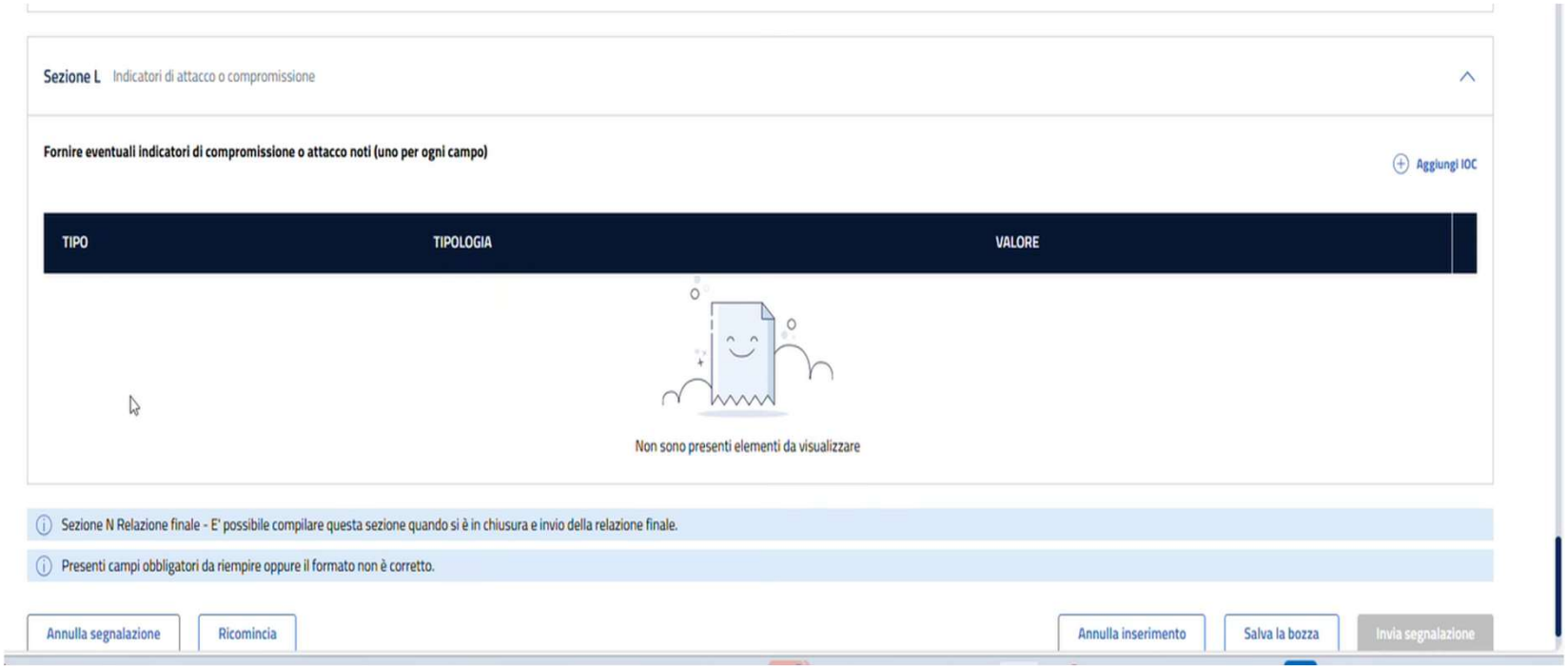
Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione



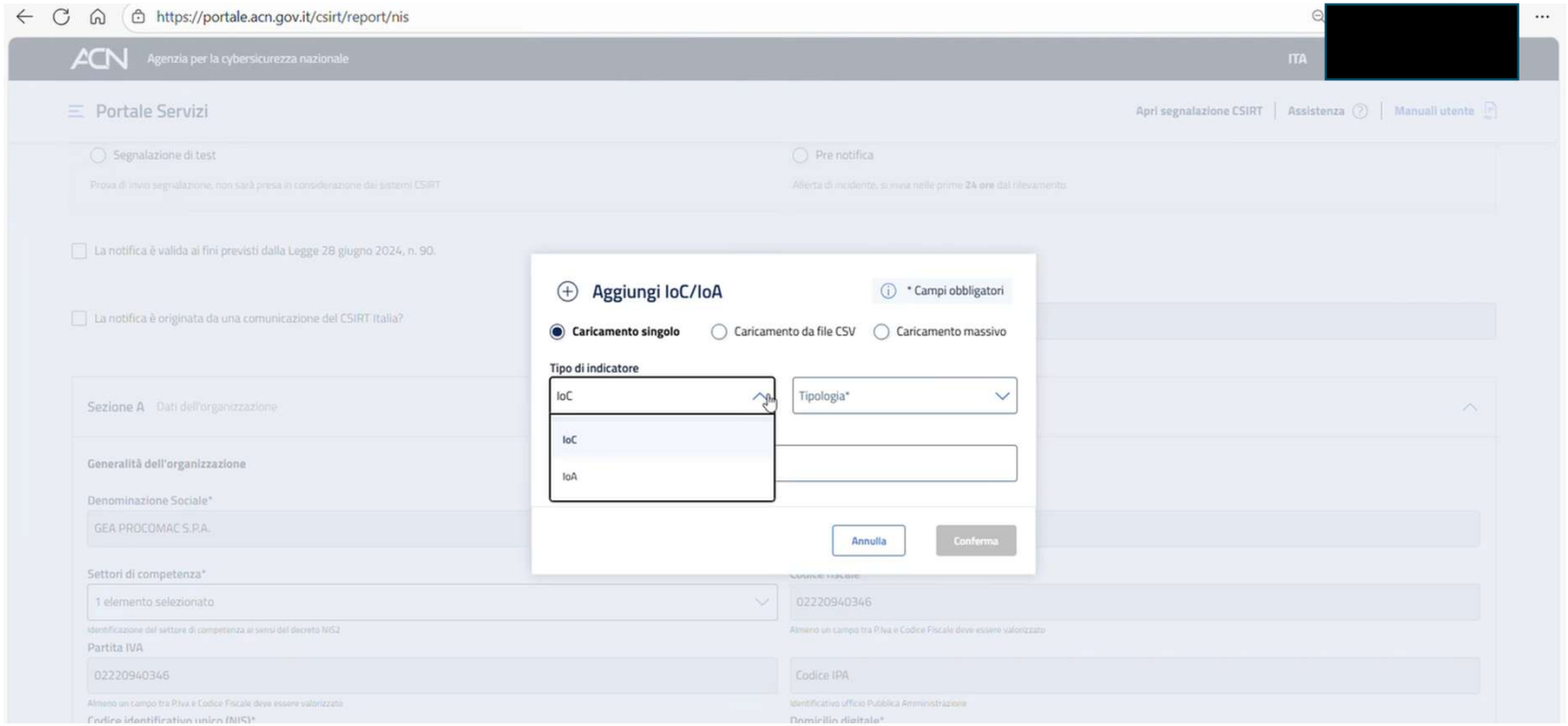
Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione



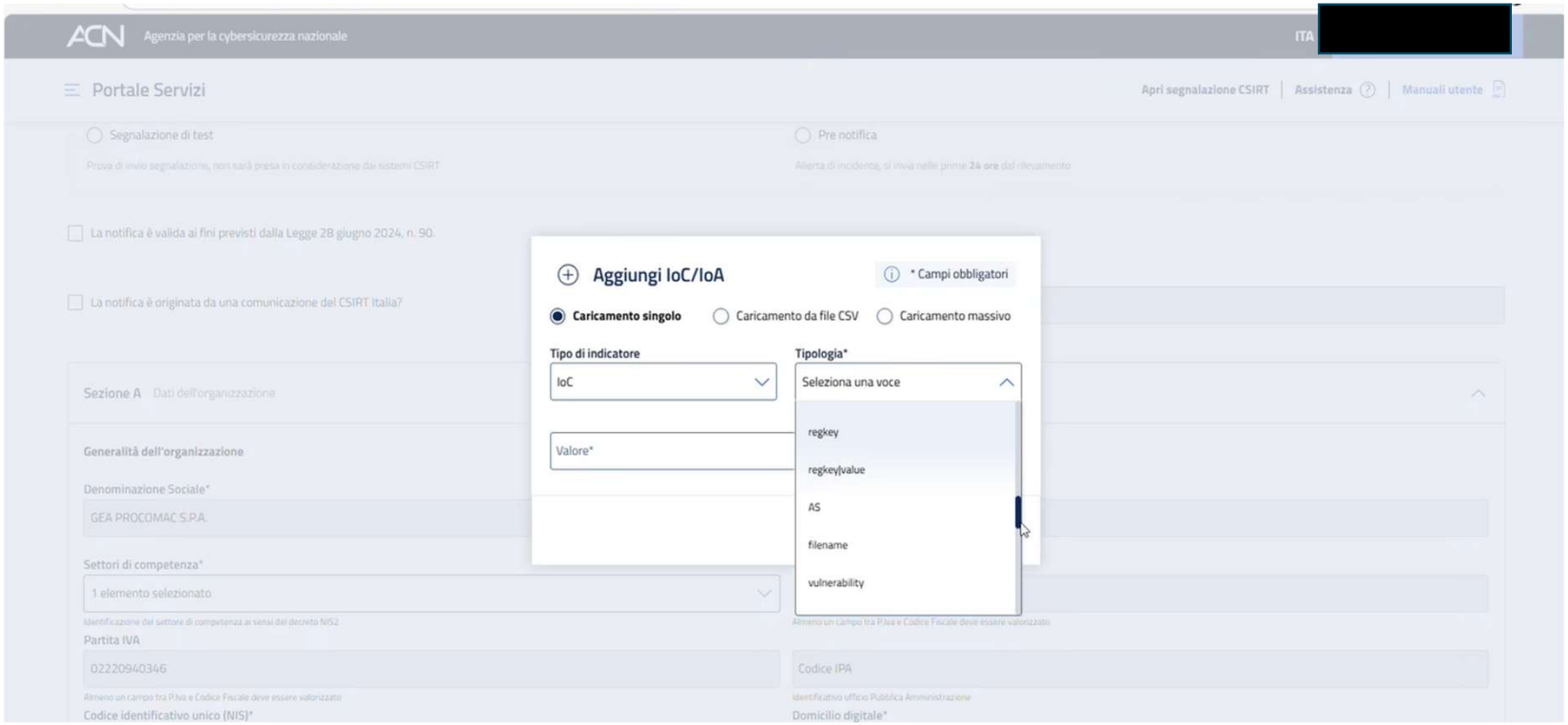
Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione



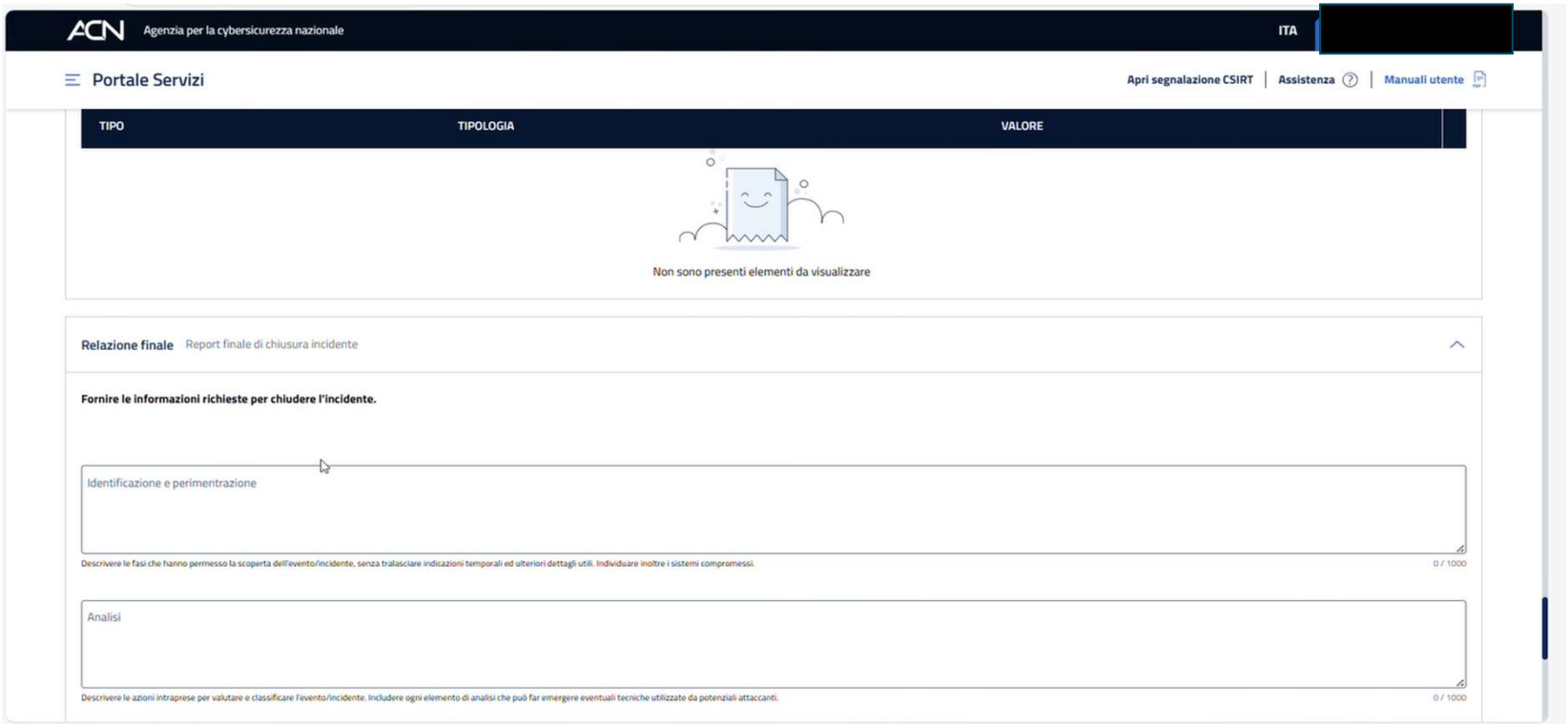
Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione



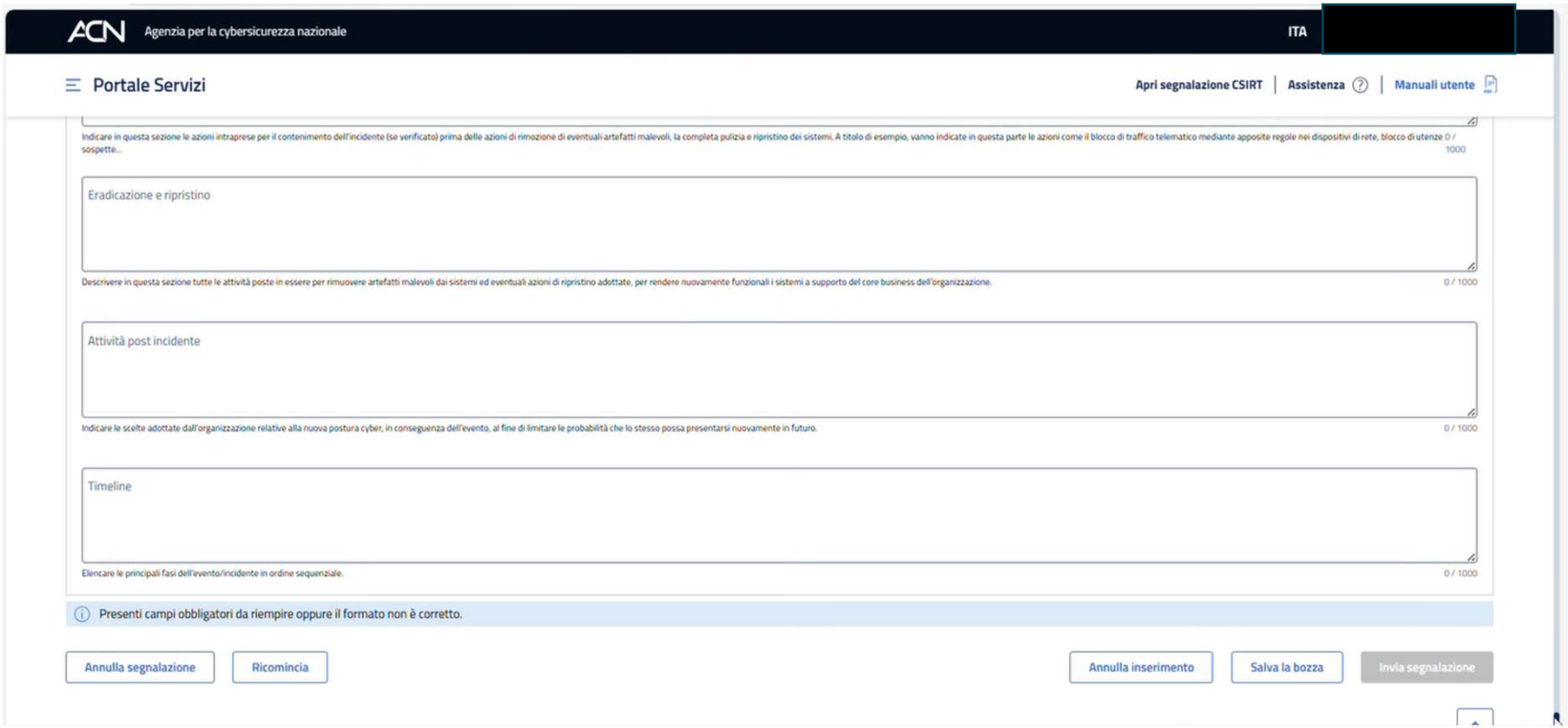
Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione



Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione



Notifiche a CSIRT degli incidenti di sicurezza informatica – Una simulazione



Agenda

- Recepimento e attuazione e prossime scadenze
- Applicazione della normativa – Le specifiche di base e alcuni approfondimenti
- Applicazione della normativa – Il piano di gestione degli incidenti e le notifiche
- Simulazione di una notifica di incidente di sicurezza
- **Q&A**

Q&A

Grazie per l’attenzione!

DataConSec

DATA PROTECTION - CONSULTING - SECURITY

V.le Fratti, 56 Parma - Italia
Tel. e Fax: +39 0521 77 12 98
e-mail: info@dataconsec.com
amministrazione@pec.dataconsec.com
web: www.dataconsec.com