Modello di Organizzazione, Gestione e Controllo ai sensi del D.Lgs 231/2001 adottato da

Associazione Irrigazione Est Sesia

(in seguito, per brevità, “Est Sesia” o “AIES” o “l’Associazione” o l’“Ente”)

Parte Speciale R02

Delitti informatici e trattamento illecito di dati

(art. 24-bis del D.Lgs 231/2001)

Finalità

La presente Parte Speciale ha la finalità di definire i protocolli specifici di comportamento e di controllo che tutti i soggetti coinvolti nell'ambito delle attività "sensibili", elencate nei successivi paragrafi, dovranno seguire al fine di prevenire la commissione dei reati previsti dal Decreto e di assicurare condizioni di correttezza e trasparenza nella conduzione delle attività aziendali.

Attività sensibili potenzialmente rilevanti

Le attività sensibili individuate che sono state ritenute come potenzialmente rilevanti in considerazione dei "Delitti informatici e trattamento illecito di dati" sono le seguenti:

1. (GSI01) accesso ai sistemi informatici aziendali o di terze parti, che contengono: (i) informazioni bancarie; (ii) dati di fatturazione o di credito; (iii) dati relativi a pagamenti; (iv) altra documentazione in formato digitale;
2. (GSI02) gestione degli strumenti informatici in dotazione agli utenti (con particolare riguardo alla gestione dei profili di accesso alle apparecchiature informatiche, alla rete ed ai sistemi e all'installazione del software e gestione delle applicazioni esistenti);
3. (GSI03) gestione della sicurezza informatica, dell'infrastruttura informatica e degli strumenti di connettività aziendale (gestione dei back up, gestione del data center environment, ripristino da fallimenti delle operazioni, acquisto di strumenti hardware e software).

GSI01 - Accesso ai sistemi informatici aziendali o di terze parti, che contengono: (i) informazioni bancarie; (ii) dati di fatturazione o di credito; (iii) dati relativi a pagamenti; (iv) altra documentazione in formato digitale

Il processo di gestione e assegnazione degli account e degli accessi logici ai sistemi informativi aziendali è formalizzato nelle procedure di seguito elencate e nel "Regolamento interno per l'utilizzo degli strumenti informatici, della posta elettronica e di Internet", che disciplina i comportamenti da adottare nell'ambito dell'accesso ai sistemi informatici e a cui si fa espresso e diretto richiamo nella presente Parte Speciale.

In generale, è previsto un formale sistema di autorizzazioni volto a consentire l'accesso al sistema amministrativo-contabile esclusivamente ai soggetti che per la propria mansione necessitano di tali accessi. Sono inoltre presenti log di registrazione delle attività effettuate da ciascun utente.

Protocolli di comportamento e controllo

Di seguito sono indicati i protocolli definiti relativamente all'attività sensibile individuata.

- AIES si è dotata di un regolamento volto a disciplinare l'utilizzo degli strumenti informatici, della posta elettronica e di Internet "regolamento interno per l'utilizzo degli strumenti informatici, della posta elettronica e di internet" reso noto a tutti i Dipendenti tramite circolare n. 9 dell'11 ottobre 2021, il cui dettato qui si riassume.
- Ogni richiesta di creazione di utenza, modifica della stessa o sua eliminazione deve essere soggetta ad apposito iter di approvazione e, comunque, devono essere abilitate le funzionalità strettamente necessarie all'esecuzione della mansione associata.
- In sede di creazione/modifica/eliminazione di un'utenza, il GOI provvede a:
  - verificare che la richiesta provenga da soggetto formalmente identificato (e.g. Responsabile diretto) e che sia stata formalmente autorizzata;
  - verificare che la profilazione dell'utenza sia conforme alla mansione ricoperta dal destinatario dell'utenza;
  - attribuire un codice identificativo univoco (user-id) all'utenza ai fini dell'accesso ad applicazioni ed alla rete internet.
- Il GOI è inoltre responsabile della definizione di criteri e modalità per la creazione delle password di accesso alle reti aziendali, alle applicazioni e indicazione delle scadenze delle stesse.
- Il personale di AIES è responsabile della corretta gestione della propria user-id e della password, sia in termini di divulgazione delle stesse che in termini di aggiornamento e rispetto di tutte le regole definite dal GOI.
- Periodicamente, GOI provvede a verificare che non siano presenti utenze "obsolete" (e.g. a fronte di dimissioni/licenziamenti) e, nel caso si attiva per la loro eliminazione o disabilitazione.

- Tutte le attività effettuate dagli utenti e dagli Amministratori di Sistema sono tracciate in appositi file di log, di cui sono garantite l'integrità e l'immodificabilità.
- Gli utenti già profilati che intendano connettersi da remoto alla rete interna sono in grado di farlo mediante connessione in VPN; laddove tecnicamente possibile, l'accesso in VPN avviene mediante meccanismi di autenticazione basati su strong authentication definiti da parte di GOI.
- Al fine di minimizzare il rischio di accesso non autorizzato alle risorse di rete, la connessione alla rete WLAN è consentita unicamente ai soggetti autorizzati, previa autenticazione mediante l'impiego di un protocollo di sicurezza autorizzato, sicuro e affidabile.

GSI02 - Gestione degli strumenti informatici in dotazione agli utenti (con particolare riguardo alla gestione dei profili di accesso alle apparecchiature informatiche, alla rete ed ai sistemi e all'installazione del software e gestione delle applicazioni esistenti)

Il processo di gestione e assegnazione degli account e degli accessi logici ai sistemi informativi aziendali è formalizzato nelle procedure operative di seguito elencate e nel "Regolamento interno per l'utilizzo degli strumenti informatici, della posta elettronica e di Internet", che disciplina i comportamenti da adottare nell'ambito dell'accesso ai sistemi informatici e a cui si fa espresso e diretto richiamo nella presente Parte Speciale.

Protocolli di comportamento e controllo

Si fa riferimento alle procedure allegate:

- Procedura_Registrazione_Deregistrazione_Accessi Est Sesia;
- Procedura_Registrazione_Accessi Rete;
- Procedura_Provisioning_Accessi App;
- Procedura_Assegnazione Asset.

Di seguito sono riassunti i protocolli definiti relativamente all'attività sensibile individuata.

- È responsabilità di GOI garantire una corretta gestione delle modalità di accesso (sia fisico sia informatico) di utenti interni all'azienda e gli obblighi dei medesimi nell'utilizzo dei sistemi informatici, delle modalità di accesso (sia fisico sia informatico) di utenti esterni all'azienda e gli obblighi dei medesimi nell'utilizzo dei sistemi informatici.
- GOI è responsabile della gestione dei rapporti con i terzi (Responsabile CED) in caso di accesso, gestione, comunicazione, fornitura di prodotti/servizi per l'elaborazione dei dati e informazioni da parte degli stessi terzi. In tale ambito GOI è inoltre incaricato di monitorare l'operato del terzo e di garantire il rispetto del corretto trattamento dei dati da questo acquisiti.
  I soggetti terzi che devono accedere alla rete aziendale e/o solo a determinati server, per interventi di assistenza e supporto tecnico, sono nominati "Responsabile del trattamento" con apposita lettera di nomina firmata da entrambe le parti, Est Sesia e fornitore di servizi, in fase di sottoscrizione del contratto e vengono catalogati nel Sistema di accesso "Guacamole" che è utilizzato come strumento di accesso remoto con autenticazione criptata su protocollo HTTPS. Le password di accesso vengono create e assegnate dai GOI in fase di attribuzione utenza.
  La password può essere modificata dal possessore delle credenziali di accesso.
- In generale, il personale di Est Sesia è diffidato a effettuare copie non specificatamente autorizzate di dati sensibili e di software protetti da licenza. (Ripreso da GSI03)
- GOI ha implementato una struttura informativa e di controllo IT volta a monitorare e limitare l'accesso alle informazioni, ai sistemi informativi, alla rete, ai sistemi operativi ed alle applicazioni; in particolare, GOI ha definito quanto segue:
  - obbligo di autenticazione individuale degli utenti tramite codice identificativo dell'utente e password o altro sistema di autenticazione sicura;
  - assegnazione agli utenti di profili di accesso specifici e selettivi a funzioni e dati che lo richiedono;
  - accesso ai servizi di rete esclusivamente da parte degli utenti che sono stati specificatamente autorizzati e le restrizioni della capacità degli utenti di connettersi alla rete

- obbligo di custodia dei dispositivi di memorizzazione (ad esempio chiavi USB, CD, hard disk esterni) e l'adozione di regole di clear screen per gli elaboratori utilizzati;
- regole di assegnazione e gestione degli apparati abilitanti l'accesso personale ai sistemi e alle applicazioni (ad esempio, dispositivi di autenticazione o di firma).

Con riferimento alle regole adottate da Est Sesia per l'attribuzione e relativa gestione delle utilities (sia informatiche che non), si rimanda a quanto disciplinato all'interno dell'attività sensibile "Assegnazione e gestione dei beni strumentali e delle utilità aziendali (es. personal computer, carte di credito, cellulari, autovetture, ecc.)", a cui si fa espresso riferimento.

GSI03 - Gestione della sicurezza informatica, dell'infrastruttura informatica e degli strumenti di connettività aziendale (gestione dei back up, gestione del data center environment, ripristino da fallimenti delle operazioni, acquisto di strumenti hardware e software)

Al fine di garantire un agevole e strutturato sistema di gestione della sicurezza informatica, AIES si è dotata, per il tramite del proprio GSI, di un sistema di ticketing in grado di supportare la gestione degli "incidenti di sicurezza informatica". Tale sistema di ticketing provvede a classificare, prioritizzare e a protocollare gli errori riscontrati, anche al fine di garantire tracciabilità degli interventi e degli incidenti riscontrati.

Inoltre, al fine di garantire la business continuity, il GSI ha implementato logiche di back-up delle informazioni e delle scritture obbligatorie, che in particolare:

- mantiene le copie di back-up in luoghi sufficientemente distanti al fine di prevenire il rischio di perdita derivante da calamità o altri rischi "territoriali";
- effettua test sul ripristino delle scritture contabili obbligatorie;
- esegue un'attività di monitoraggio sull'esito dei backup e, qualora vi fossero riscontrate anomalie, vengono prese in carico e risolte tempestivamente.

All'atto della configurazione di un nuovo terminale (o altra apparecchiatura hardware), GOI provvede ad installare antivirus e firewall. Periodicamente viene richiesto ai dipendenti utilizzatori del terminale/hardware di effettuare gli aggiornamenti alla versione di antivirus e firewall più aggiornati. Gli eventuali "mancati" aggiornamenti vengono monitorati da parte di GOI che eventualmente attua i dovuti correttivi.

Al fine di garantire l'impossibilità di accesso ad informazioni riservate e/o intrusioni non autorizzate, la rete aziendale risulta essere segregata in due ambienti distinti e non connessi tra loro: un ambiente è riservato ai dipendenti dell'Associazione ed alle apparecchiature abilitate; un antro ambiente è invece reso disponibile ai soggetti esterni. Inoltre, per le sedi decentrate (e comunque anche per l'esecuzione di attività in modalità "smart-working") l'accesso alla rete aziendale (e relativa compartimentazione) è attuabile per il tramite di VPN.

Con particolare riferimento invece all'introduzione all'interno del sistema dell'Associazione di hardware e software "nuovi", si segnala che in generale AIES procede, nei casi di sostituzione delle postazioni obsolete che non richiedono particolari caratteristiche hardware, allo scouting di soluzioni "ricondizionate" e, comunque, prima del loro inserimento, il prodotto viene testato e verificato da parte del GOI, al fine di precludere ogni eventuale rischio per AIES. Inoltre, in caso di asset informatici ad alto valore, l'inserimento avviene sempre per il tramite di gara di acquisto che vede il coinvolgimento di GOI per l'esecuzione dei controlli di adeguatezza previsti.

Protocolli di comportamento e controllo

Di seguito sono indicati i protocolli definiti relativamente all'attività sensibile individuata.

- In caso di smarrimento di hardware di proprietà di Est Sesia, il dipendente assegnatario di tale hardware deve effettuare segnalazione a GOI, il quale si deve attivare per limitare le eventuali perdite di informazioni o la possibilità di intrusione non autorizzata per il tramite di tale hardware.
- In generale, il personale di Est Sesia è diffidato a effettuare copie non specificatamente autorizzate di dati sensibili e di software protetti da licenza.
- GOI ha provveduto ad implementare un inventario dei software, delle banche dati e dei contenuti protetti dal diritto d'autore (o copyright), comprensivo delle informazioni sulle relative licenze d'uso, al fine di attuare attività di monitoraggio sul rispetto delle condizioni contrattuali.

- GSI ha implementato logiche di back-up al fine di garantire l'accessibilità ed il ripristino dei dati chiave in caso di disastro o di incidente informatico; in particolare:
  - le copie di back-up sono mantenute in luoghi sufficientemente distanti al fine di prevenire il rischio di perdita derivante da calamità o altri rischi "territoriali";
  - periodicamente vengono effettui test sul ripristino delle scritture contabili obbligatorie;
  - è presente un'attività di monitoraggio sull'esito dei backup e, qualora vi fossero riscontrate anomalie, vengono prese in carico e risolte tempestivamente da parte di GOI o di consulente informatico incaricato.
- GOI è responsabile del monitoraggio del corretto funzionamento di antivirus (a livello di installazione e rilascio di eventuali aggiornamenti) al fine di prevenire eventuali incidenti informatici. I firewall sono gestiti e configurati su richiesta dal CSI per la rete internet e di gestione domini e da Vodafone per la rete MPLS.
- In sede di acquisto di hardware e software, Est Sesia deve rispettare quanto previsto nell'ambito del processo "Gestione degli acquisti di beni, servizi e consulenze", con la particolarità che deve essere contemplato il coinvolgimento di GOI per il rilascio di un parere esplicito preliminarmente all'esecuzione dell'acquisto.