POLITICA PER LA QUALITÀ, PER LA SALUTE E LA SICUREZZA NEI LUOGHI DI LAVORO, PER LA GESTIONE DEGLI IMPATTI AMBIENTALI E PER LA SICUREZZA DELLE INFORMAZIONI

Storia delle modifiche

Revisione	Data	Sezione modificata	Descrizione della modifica
6	28/02/2018	Storia modifiche Testo	Inserita sezione Inserito riferimento esplicito all'analisi del rischio Descritte modalità con cui viene valutata la criticità delle informazioni
7	19/02/2019	Testo	Aggiornamento: nuovi siti e GDPR
8	17/02/2020	/	Riesame e riemissione
9	22/02/2021	Varie	Inserimento estensione SGSI ai servizi di progettazione e sviluppo SW
10	24/01/2022	/	Riesame e riemissione
11	09/01/2023	Testo	Accorpamento CNI Digital Solution
12	04/04/2023	Pag. 2, pag. 6 Responsabilità e Obiettivi	Integrazione requisiti ISO 27017, ISO 27018, ISO 27701
13	08/01/2024	/	Riesame e riemissione

La DIREZIONE della **CNI S.p.A.** definisce la propria Politica come segue:

essere competitivi significa puntare a differenziare le caratteristiche dei propri servizi attraverso una costante ricerca volta al miglioramento dei processi aziendali dai punti di vista della qualità, della gestione aziendale e della sicurezza delle informazioni, con particolare riferimento ai processi di definizione e sviluppo nell'erogazione tanto del prodotto quanto del servizio. L'obiettivo della Direzione risulta essere quello di individuare e valutare i rischi e, in base alle risultanze di tale analisi, definire adeguate contromisure, processi e strumenti di controllo atti ad indirizzare gli sforzi di tutto il personale ad un'attenta gestione degli aspetti legati alla qualità del lavoro, all'impatto sull'ambiente e alla sicurezza delle informazioni trattate.

Si ritiene quindi necessaria una forte responsabilizzazione da parte di tutti a garantire la rigorosità del proprio operato per adempiere, con la massima attenzione, ai fattori indicati e per prevenire i rischi connessi. In particolare ciò va perseguito con:

- la definizione e condivisione di adeguate procedure operative (SGSI);
- l'efficienza operativa dei processi;
- la ricerca prioritaria di sicurezza e affidabilità dei processi;
- la continuità e l'efficienza dei processi organizzativi e operativi al fine di prevenire e ridurre al minimo l'impatto degli incidenti volontari o casuali;
- la protezione e la disponibilità di ogni risorsa tecnica, umana e patrimoniale; la riservatezza, la correttezza e la disponibilità di tutti i dati gestiti dalla CNI per conto dei propri clienti e la proprietà intellettuale di CNI o affidati da CNI a terzi;
- il rispetto delle leggi e normative vigenti, con particolare riferimento al Regolamento UE 2016/679;
- la prevenzione delle anomalie;
- l'efficace gestione delle emergenze;
- la garanzia che i dati conservati in cloud siano sicuri e protetti e fornire una modalità strutturata, basata sul privacy by design, per far fronte alle principali questioni giuridiche, legali e contrattuali legati alla gestione dei dati personali in infrastrutture informatiche distribuite.

Per tutto ciò la Direzione si impegna ad assumere un ruolo attivo nella promozione e guida di tutte le attività aventi influenza sulla qualità, sulla sicurezza e salute dei lavoratori, sull'impatto che l'azienda tutta può generare sull'ambiente che ci circonda e sugli aspetti legati alla sicurezza delle informazioni, attraverso la diffusione a tutti i livelli dei concetti qui esposti e la verifica dei risultati ottenuti.

In particolare, per la sicurezza delle informazioni, CNI stabilisce le responsabilità, le strategie, di seguito descritte:

Principi

Obiettivo primario è quello di garantire la riservatezza, l'integrità e la disponibilità dei dati gestiti da CNI per conto dei propri clienti nell'erogazione dei servizi di:

- trattamento documentale
- archiviazione
- conservazione informatica
- progettazione e sviluppo SW

dove si intende per:

- riservatezza la proprietà che le informazioni non siano rese disponibili o divulgate a persone o entità non autorizzate, garantita attraverso la definizione delle responsabilità interne per la gestione dei servizi e delle informazioni ad essi connesse, il controllo degli accessi fisici e logici agli archivi elettronici esclusivamente da parte di personale autorizzato e competente e cartacei e la definizione delle interfacce del cliente relativamente alla richiesta e alla consegna dei dati di proprietà del cliente stesso
- integrità la proprietà di salvaguardare l'accuratezza e la completezza delle informazioni e degli asset ad esse connessi, garantita attraverso il controllo degli accessi fisici e logici agli archivi elettronici e cartacei esclusivamente da parte di personale autorizzato e competente e la gestione dei back up dei dati e delle configurazioni dei sistemi informativi
- disponibilità la proprietà di essere accessibile e utilizzabile su richiesta da parte di soggetti autorizzati, garantita attraverso l'identificazione dei ruoli e delle funzioni, i diritti di accesso alle informazioni e agli asset aziendali per la gestione dei servizi e la definizione delle interfacce del cliente e delle modalità di gestione della richiesta e della consegna dei dati di proprietà del cliente stesso.

A tal fine, la CNI definisce le seguenti affermazioni riguardanti la sicurezza delle informazioni:

Analisi dei rischi

L'attività di analisi dei rischi svolta da CNI rispetto alla propria organizzazione, processi, infrastrutture, sistemi, processi, obiettivi è stata propedeutica all'identificazione ed implementazione delle contromisure e controlli da applicare ai servizi forniti al fine di assicurare la piena adeguatezza delle diverse componenti del sistema ai requisiti, vincoli ed obiettivi e la completa conformità rispetto agli aspetti legali, normativi, standard di riferimento.

Accettazione

Dipendenti, fornitori, partner, appaltatori e ogni altra terza parte deve accettare gli obblighi e le responsabilità di propria pertinenza, al fine di proteggere le informazioni, i beni e le risorse della CNI o affidate da CNI a terzi.

Accesso

L'accesso alle attività e alle risorse di CNI o affidate da CNI a terzi, nonché alle informazioni gestite da CNI per conto dei clienti, è autorizzato, controllato e monitorato sulla base dei seguenti criteri:

- l'accesso è autorizzato solo per le informazioni necessarie (principio della conoscenza minima o necessità di sapere);
- l'accesso è autorizzato solo per le informazioni relative alle attività specifiche (funzione di lavoro-correlati).

L'accesso ai locali della CNI è autorizzato controllato e monitorato in linea con la politica degli accessi fisici.

Assessment

CNI definisce la relazione tra:

- i costi necessari per l'attuazione delle misure al fine di tutelare le informazioni, le attività e le risorse della CNI o affidate da CNI a terzi;
- i rischi connessi con l'utilizzazione non autorizzata, con la modifica o la distruzione delle informazioni critiche.

Consapevolezza

La Direzione assicura che ogni dipendente, fornitore, imprenditore e terza parte è consapevole del proprio ruolo e dell'impatto delle proprie azioni sulla sicurezza delle informazioni della CNI.

Formazione

La Direzione assicura che ogni risorsa sia addestrata sulle politiche organizzative applicate e le procedure relative alla sicurezza delle informazioni.

Conformità a leggi e regolamenti obbligatori

I trattamenti delle informazioni, delle attività, delle risorse e delle soluzioni inerenti la protezione delle informazioni della CNI o gestiti dalla CNI per conto dei propri clienti sono conformi alle leggi e ai regolamenti applicabili.

Protezione

Ogni attività e risorsa della CNI o affidata da CNI a terze parti, nonché ogni informazione è protetta contro i problemi legati alla riservatezza, l'integrità e la disponibilità, in proporzione al loro valore e nel rispetto delle leggi vigenti.

In particolare, la criticità delle informazioni rispetto al sistema di conservazione è valutata prendendo in considerazione gli impatti che l'eventuale divulgazione impropria delle informazioni stesse può avere su (1) processi critici dell'organizzazione e in particolare sulla capacità di CNI di continuare l'erogazione del servizio ai propri clienti, (2) danni per il cliente, (3) posizione competitiva di CNI, (4) risultati economici e finanziari di CNI.

La classificazione delle informazioni (information classification levels) che ne consegue è riportata in apposita procedura del SGSI cui si rimanda (cfr. POI 4-01 - Gestione e Controllo della documentazione e delle registrazioni).

Responsabilità

Le responsabilità definite nel presente paragrafo sono generali e riguardano tutta l'organizzazione della CNI. Specifiche responsabilità connesse al campo di applicazione di gestione per la sicurezza sono definiti nel Piano di sicurezza della CNI.

Ognuno deve:

- proteggere la riservatezza, l'integrità e la disponibilità dei dati personali, delle informazioni gestite da CNI, la proprietà intellettuale e il patrimonio della CNI o affidati da CNI a terze parti;
- proteggere i beni materiali, i sistemi e le risorse della CNI o affidati da CNI a terze parti;
- proteggere i dati personali e ogni informazione, attività e risorse di propria competenza;
- contattare la Direzione, il Responsabile della Sicurezza e/o altre autorità competenti in caso di effettive o sospette violazioni della sicurezza;
- contattare la Direzione e/o il Responsabile della Sicurezza nel caso si riscontri qualsiasi necessità di modifiche della politica di sicurezza, requisiti, standard e procedure.

Ogni responsabile di servizio deve:

- essere in linea con la politica di sicurezza, requisiti, standard e/o procedure definiti e requisiti cogenti;
- individuare e definire i diritti di accesso delle risorse per le loro specifiche attività e responsabilità;
- richiedere alle terze parti di essere formalmente in linea con gli accordi di riservatezza (accordo di riservatezza);
- definire un livello accettabile di rischio a seguito della realizzazione di una valutazione del rischio.

Il Responsabile della Sicurezza deve:

- implementare la sicurezza sulla base delle politiche di sicurezza della CNI;
- garantire e monitorare il rispetto delle politiche di sicurezza, requisiti, norme e procedure definiti da CNI;
- monitorare informazioni e risorse fisiche sotto la propria responsabilità, al fine di definire il livello di controllo adeguato da attuare perché il controllo di sicurezza ere sia adeguato al valore delle informazioni/asset da proteggere e nel rispetto delle leggi e regolamenti obbligatori;
- garantire che le risorse CNI e i terzi siano formati e informati circa la politica, i requisiti, standard e/o procedure;
- realizzare un Piano di Sicurezza (cfr. Piano di Sicurezza) contenente gli aspetti di cui sopra e i seguenti contenuti:
  - la sicurezza organizzativa,

- le attività di sicurezza,
- la sicurezza personale,
- la sicurezza fisica e ambientale,
- la comunicazione e la gestione operativa,
- il controllo degli accessi,
- i sistemi di acquisizione, sviluppo e gestione,
- la gestione degli incidenti di sicurezza,
- la gestione della continuità operativa,
- la conformità legislativa;

- organizzare le attività relative alla gestione delle crisi, la pianificazione del disaster recovery e la pianificazione del ripristino delle attività in conformità ai requisiti definiti dalla CNI;
- fornire il necessario supporto alle funzioni competenti nella fase di selezione di una soluzione cloud-based volto a:
  - qualificare e/o selezionare dei cloud provider in relazione ai "livelli di maturità" in tema di cyber security governance;
  - scegliere la soluzione che meglio indirizza le esigenze di sicurezza, in base alla criticità delle informazioni trattate e agli impatti negativi per l'azienda in caso di "data breach".

Le risorse umane hanno le seguenti responsabilità:

- il rispetto dei requisiti di legge italiana (D. Lgs. 196/2003) ed europea (Regolamento UE 2016/679);
- rendere le risorse consapevoli delle conseguenze in caso di mancato rispetto della politica di sicurezza e della normativa in materia di protezione dei dati personali.

Il Responsabile del Servizio di Prevenzione e Protezione ha la seguente responsabilità:

- garantire l'applicazione del "Testo Unico in materia di Tutela della Salute e della Sicurezza Nei Luoghi di Lavoro" (D. Lgs. n. 81/2008) in CNI, al fine di garantire la sicurezza dei dipendenti CNI.

Le terze parti che collaborano con CNI devono:

- essere formalmente in linea con i controlli di sicurezza stabiliti dalla CNI, nel rispetto dei requisiti contrattuali;
- proteggere le risorse e le informazioni fisiche e intellettuali a cui possono accedere.

Il punto di partenza per la realizzazione di queste politiche è stato individuato nel perseguimento dei seguenti **obiettivi**:

- monitorare costantemente nel tempo il Sistema di Gestione Integrato secondo gli standard UNI EN ISO 9001, UNI EN ISO 14001 e UNI EN ISO 27001;
- estendere la certificazione ISO 27001 alle Linee Giuda ISO 27017 e ISO 27018;
- integrare il sistema esistente con i requisiti della ISO 27701 e conseguire la relativa certificazione;

- mantenere la certificazione AGID per la conservazione di documenti informatici;
- assicurare il rispetto dei requisiti qualitativi, quantitativi, temporali, di sicurezza nel lavoro, di sicurezza delle informazioni oltre che di rapporto qualità/prezzo, in conformità ai requisiti specificati e alle normative applicabili;
- mantenere costantemente monitorato il grado di conformità del sistema alle norme e leggi di riferimento;
- promuovere e implementare programmi di addestramento/formazione del personale a tutti i livelli al fine di ottimizzare il processo di consapevolezza e di crescita delle risorse umane, considerate come risorse critiche per lo sviluppo aziendale degli anni a venire.

La Direzione è conscia delle responsabilità che derivano dall'assunzione di tale impegno ed esorta tutto il personale dipendente al rispetto di tale politica operando affinché sia garantita, sempre e comunque la:

SODDISFAZIONE DEL CLIENTE

La presente politica di sicurezza è definita/aggiornata, divulgata e riesaminata ogni qualvolta si verifichi uno dei seguenti casi:

- incidenti di sicurezza,
- variazioni tecnologiche significative,
- modifiche all'architettura informatica,
- aggiornamenti delle prescrizioni normative,
- risultati delle eventuali attività di audit interni,

e comunque almeno una volta all'anno.

La Direzione della **CNI Digital Solution S.r.l.** acquisisce in toto quanto definito dalla presente politica al fine di uniformare obbiettivi e strategie di applicazione.

data Roma, 08.01.2024 **la Direzione**