Politica per la sicurezza delle informazioni

Le informazioni devono essere gestite in modo sicuro, accurato e affidabile e devono essere prontamente disponibili per gli usi consentiti. E' utile sottolineare che per "utilizzo dell'informazione" si intende qualsiasi forma di trattamento che si avvalga di supporti elettronici, cartacei o consenta, in una qualsiasi forma, la comunicazione verbale. La norma ISO 27001:2013 (in Italia UNI EN CEI ISO / IEC 27001:2017) prevede che il responsabile del sistema di gestione per la sicurezza delle informazioni svolga periodicamente una "valutazione dei rischi" tenendo chiaramente in considerazione gli obiettivi strategici espressi nella presente politica, degli incidenti occorsi nel periodo e dei cambiamenti strategici di business e tecnologici accaduti; tale analisi dei rischi ha lo scopo di valutare il rischio di ogni asset (o beni con valore utilizzati nella tecnologia dell'informazione o comunicazione) da proteggere rispetto alle minacce individuate. La direzione condivide con il responsabile del sistema di gestione per la sicurezza delle informazioni la metodologia da impiegare per la valutazione del rischio, approvando il relativo documento; nella metodologia della redazione inoltre la direzione partecipa alla definizione dei parametri ed alla scala dei valori da impiegare, considerando al termine della valutazione i risultati ottenuti accettando la "soglia di rischio accettabile", il "trattamento di mitigazione dei rischi" oltre tale soglia, ed il rischio residuo a seguito del trattamento. Tale analisi sarà ponderata anche rispetto al valore del business dei singoli beni da proteggere e dovrà identificare chiaramente le azioni da intraprendere da classificare secondo una scala di priorità che rispetti gli obiettivi aziendali, il budget a disposizione e la necessità di mantenere la conformità alle norme e leggi vigenti. Detta analisi dovrà inoltre essere elaborata ogni qualvolta si verifichino cambiamenti tali da incidere sul profilo del rischio complessivo del sistema.

Obiettivi

L'obiettivo del sistema di gestione della sicurezza delle informazioni in NOUVELLE, è di garantire un adeguato livello di sicurezza dei dati e delle informazioni nell'ambito del campo di applicazione definito tramite l'identificazione, la valutazione ed il trattamento dei rischi ai quali i servizi stessi ed i software progettati e sviluppati sono soggetti. Il sistema di gestione della sicurezza delle informazioni di NOUVELLE, definisce un insieme di misure organizzative e tecniche procedurali a garanzia del soddisfacimento dei sottoelencati requisiti di sicurezza di base:

- Riservatezza: ovvero la proprietà dell'informazione di essere nota solo a chi ne ha i privilegi;
- Integrità: ovvero la proprietà dell'informazione di essere modificata solo ed esclusivamente da chi ne possiede i privilegi;
- Disponibilità: ovvero la proprietà dell'informazione di essere accessibile e utilizzabile quando richiesto dai processi e dagli utenti che ne godono i privilegi.

Con la presente politica, NOUVELLE intende formalizzare i seguenti obiettivi nell'ambito della sicurezza delle informazioni:

- Preservare al meglio l'immagine dell'azienda quale fornitore affidabile e competente.
- Proteggere il proprio patrimonio informativo.
- Evitare, per quanto possibile, i ritardi nel delivery.
- Adottare le misure atte a garantire la fidelizzazione del personale e la sua professionalità.
- Rispondere pienamente alle indicazioni della normativa vigente e cogente.
- Aumentare, nel proprio personale, il livello di sensibilità e la competenza sui temi della sicurezza.

Criteri per l'identificazione della tipologia delle informazioni.

NOUVELLE è consapevole sia dell'importanza della tutela della riservatezza delle informazioni in generale sia che non tutte le informazioni necessitano dello stesso grado di sicurezza e segretezza del dato. Poiché l'aumento dei livelli di protezione implica un aumento nell'utilizzo di risorse e un conseguente aumento di costi, NOUVELLE ha suddiviso le informazioni in categorie distinte ai quali applica diversi trattamenti. Ogni informazione può appartenere ad una o più categorie.

- Informazioni interne ed esterne.
    - Interne: fanno parte di questa categoria tutte le informazioni aziendali associate al personale, alle mansioni, ai ruoli, agli strumenti aziendali necessarie allo svolgimento dell'attività lavorativa quotidiana. Alle informazioni interne afferiscono anche tutti i dati clienti necessari all'erogazione del servizio o ad attività amministrative ad esso associate.
    - Esterne: fanno parte di questa categoria le informazioni del cliente o di terzi, fornite dal cliente, cui NOUVELLE viene a conoscenza nell'erogazione del servizio richiesto. A questa categoria appartengono:
        - i documenti e dati utilizzati per il test e il collaudo degli applicativi in licenza.
        - i documenti e dati utilizzati per il debug.
        - i documenti e dati che NOUVELLE conserva, elabora e gestisce conto terzi nelle proprie sedi.

- Informazioni identificative aziendali e personali.
    - Aziendali: fanno parte di questa categoria le informazioni che identificano o rendono identificabile una persona giuridica (azienda), solitamente sono informazioni pubbliche.
    - Personali: fanno parte di questa categoria le informazioni che identificano o rendono identificabile una persona fisica e che possono fornire dettagli sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica. Queste a loro volta possono contenere dati il cui grado di riservatezza sia sensibilmente diverso e sono di tipo:
        - identificativi: quelli che permettono l'identificazione diretta, come i dati anagrafici;
        - sensibili: quelli che possono rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, lo stato di salute e la vita sessuale;

- giudiziari: quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale o la qualità di imputato o di indagato.

La classificazione e la successiva modalità di trattamento dei dati per le diverse categorie sono indicate nelle procedure e nei documenti del sistema di gestione integrato per la qualità e la sicurezza delle informazioni

Responsabilità

Tutto il personale che a qualsiasi titolo collabora con l'azienda è responsabile dell'osservanza della presente policy ed è tenuto a partecipare alla segnalazione delle anomalie, anche formalmente non codificate, di cui dovesse venire a conoscenza.
Il Responsabile del sistema di gestione per la Sicurezza delle Informazioni si occupa della progettazione del sistema della Sicurezza delle Informazioni ed in particolare:

- Suggerire le misure di sicurezza organizzative, procedurali, tecnologiche a tutela della sicurezza e per la continuità delle attività di NOUVELLE.
- Controllare periodicamente l'esposizione dei servizi aziendali alle principali minacce.
- Verificare gli incidenti di sicurezza ed adottare le opportune contromisure.
- Emanare tutte le norme necessarie ivi inclusa la classificazione e divulgazione dei documenti affinché l'organizzazione aziendale possa condurre in modo sicuro le proprie attività.
- Pianificare per il personale un percorso formativo specifico e periodico in materia di sicurezza.
- Promuovere la cultura relativa alla sicurezza delle informazioni.
- Contribuire alla definizione delle contromisure da adottare a seguito di eventuali incidenti.

Tutti i soggetti esterni che intrattengono rapporti con NOUVELLE devono garantire il rispetto dei requisiti della sicurezza esplicitati dalla presente politica di sicurezza anche tramite la sottoscrizione di un "patto di riservatezza" all'atto del conferimento dell'incarico allorquando questo tipo di vincolo non è espressamente previsto nel contratto.

Applicabilità

La presente politica si applica indistintamente a tutti gli organi dell'azienda. L'attuazione della presente politica è obbligatoria per tutte le risorse di NOUVELLE, e va inserita nell'ambito della regolamentazione degli accordi nei confronti di qualsiasi soggetto esterno che, a qualsiasi titolo, possa venire a conoscenza delle informazioni gestite in azienda. NOUVELLE consente la comunicazione e diffusione delle informazioni verso l'esterno solo per il corretto svolgimento delle attività aziendali che avvengono sempre nel rispetto delle regole nonché delle norme e leggi cogenti.

28/04/2023

NOUVELLE s.r.l.
Via Giardini, 456/C
41100 MODENA
Part. IVA 02051850366

La Direzione