ANALISI DEI RISCHI CHE INCOMBONO SUI DATI

GIULIANO BRACCO, **Titolare** del trattamento, è consapevole:

- dell'importanza e del valore dei dati personali, dei dati industriali, delle informazioni e del know-how, i quali costituiscono una componente essenziale del proprio patrimonio;
- degli impatti derivanti da incidenti o errori in tema di sicurezza dei dati, nonché dalla eventuale perdita di riservatezza e integrità dei dati e/o dalla indisponibilità dei beni;
- della necessità di ridurre al minimo accettabile i danni derivanti da incidenti o errori in tema di sicurezza dei dati;
- delle leggi e delle disposizioni comunitarie vigenti in materia di sicurezza dei dati;
- dell'importanza del ruolo del personale nell'ambito della riduzione dei rischi errori in tema di sicurezza dei dati;
- dell'importanza della formazione e del coinvolgimento del personale in tutti gli aspetti inerenti la sicurezza dei dati.

Inoltre, è informato in merito all'entrata in vigore della L. 48/2008, detta anche "legge sui crimini informatici", che recepisce la Convenzione di Budapest in tema di criminalità informatica ed estende i casi di responsabilità amministrativa delle imprese e degli enti (d.lgs. 231/2001) per i reati commessi da amministratori, dirigenti, dipendenti, a vantaggio e nell'interesse dell'impresa o dell'ente.

Pertanto, **GIULIANO BRACCO** è particolarmente impegnato nella prevenzione dei seguenti crimini informatici, così definiti dal Codice Penale:

- delitti informatici e trattamento illecito di dati;
- **491bis** - Falsità in documento informatico pubblico o avente efficacia probatori
- **615 ter** - Accesso abusivo ad un sistema informatico o telematico;
- **615 quater** - Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici;
- **615 quinquies** - Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico;
- **617 quater** - Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche;
- **615 quinquies** - Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche;
- **635 bis** - Danneggiamento di informazioni, dati e programmi informatici;
- **635 ter** - danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità;
- **635 quater** - Danneggiamento di sistemi informatici o telematici;
- **635 quinquies** - Danneggiamento di sistemi informatici o telematici di pubblica utilità;
- **640 quinquies** - Frode informatica del certificatore di firma elettronica.
- **delitti in materia di violazione del diritto d'autore;**
- **171, l.633/1941 comma 1 lett. a) bis** - Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa;
- **171, l. 633/1941 comma 3** - Reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione dell'autore;
- **171-bis l. 633/1941 comma 1** - Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori;
- **171-bis l. 633/1941 comma 2** - Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati;
- **171-ter l. 633/1941** - Immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa.

L'opera di prevenzione è svolta attraverso una continua attività di vigilanza e di controllo, attuata anche mediante l'adozione di regolamenti, procedure e modelli organizzativi. Per le ragioni sopra esposte, il Titolare del trattamento, **GIULIANO BRACCO**, adotta le più idonee misure di sicurezza e di prevenzione atte a:

- ridurre al minimo i rischi,
- assicurare la protezione dei dati e degli strumenti di trattamento da minacce reali e potenziali,

- rispondere a situazioni di crisi in maniera efficace per assicurare la continuità dei servizi e della produzione aziendale,
- regolamentare l'accesso e l'uso degli strumenti di elaborazione elettronica,
- prevenire la commissione dei reati previsti dalla L. 48/2008,
- mantenere un elevato livello di vigilanza e il controllo.

L'Analisi del Rischio secondo la ISO/IEC 27001:2013

L'Analisi del Rischio è un processo formale e strutturato attraverso il quale si identificano i rischi e si determina la loro ampiezza. Questo significa che attraverso l'analisi del rischio è possibile definire le esigenze di sicurezza e individuare le più appropriate misure da adottare al fine di prevenirli o di ridurre il loro impatto. L'analisi del rischio può essere effettuata in molti modi, adottando metodi diversi che si basano su concetti analoghi. La scelta qui effettuata è quella di fare riferimento il più possibile a standard ufficialmente definiti e riconosciuti; pertanto si è adottato come modello di riferimento quello previsto dalle norme ISO.

La norma **ISO/IEC 27001:2013 Sistemi** di **Gestione** per la **Sicurezza** delle **Informazioni (SGSI)** tratta l'analisi del rischio richiamando la metodica e le definizioni riportate nella **Guida ISO/IEC 73:2009 e ISO31000:2009.** Vediamo di seguito le principali definizioni:

- **rischio:** combinazione della probabilità di un evento e della sua conseguenza.
- **probabilità:** frequenza teorica con la quale un evento si verifica.
- **evento:** verificarsi di un insieme di circostanze.
- **conseguenza:** esito di un evento.
- **minaccia:** possibile causa di evento indesiderato che può comportare danni ad un sistema o a una organizzazione.
- **vulnerabilità:** debolezza insita in un bene, in un processo, in un sistema, che può essere sfruttata da una minaccia per generare un evento indesiderato.
- **accettazione del rischio:** decisione di accettare un rischio.
- **mitigazione del rischio:** limitazione delle conseguenze di un evento.
- **riduzione del rischio:** diminuzione della probabilità e delle conseguenze.
- **trasferimento del rischio:** condivisione con altro soggetto dell'onere derivante da un rischio.

Calcolo dell'indice di rischio

Ad ogni evento (o categoria di eventi) viene assegnato un "valore del danno" per il **Titolare**, secondo il seguente criterio:

- AA – valore del danno altissimo = 5
- A – valore del danno alto = 4
- M – valore del danno medio = 3
- B – valore del danno basso = 2
- BB – valore del danno bassissimo = 1

Il "valore del danno" è l'espressione delle possibili conseguenze negative dovute alla lesione o alla compromissione di beni giuridici, patrimoniali e non patrimoniali del Titolare. Tali conseguenze negative possono riguardare:

- la violazione di una norma di legge
- le perdite monetarie per mancati ricavi
- le perdite monetarie per aumento di costi
- le perdite monetarie per indennizzi
- l'interruzione della continuità del business
- la lesione dell'immagine
- il mancato raggiungimento di obbiettivi e standard

Alle **minacce** vengono assegnati i seguenti valori:

- A – minaccia grave = 3
- M - minaccia media = 2
- B – minaccia lieve = 1

L’indice di probabilità utilizzato è il seguente:

- AA – probabilità altissima = 1
- A – probabilità alta = 0,8
- M – probabilità media = 0,6
- B – probabilità bassa = 0,4
- BB – probabilità bassissima = 0,2

Il calcolo dell'indice di rischio residuo **IRR** è effettuato per ogni minaccia individuata, moltiplicando il valore della minaccia stessa per il valore del danno e per l'indice di probabilità. Il valore massimo ottenibile è perciò 15, nella combinazione "peggiore" della terna: valore del danno – livello di minaccia - indice di probabilità.

A fronte dell'indice di rischio calcolato per ciascuna minaccia, viene effettuata una valutazione delle più opportune contromisure adottabili. A tale proposito è stato anche definito un Indice di Rischio Residuo Accettabile (**IRRA**), cioè il livello di rischio oltre il quale l'adozione di ulteriori misure o controlli comporta oneri eccessivi e non commisurati alle capacità economiche del **Titolare**. Il valore di **IRRA** definito dal **Titolare GIULIANO BRACCO** è **0,5.**

Minacce e loro conseguenze sui dati

Nella tabella che segue sono riportate le principali minacce, con l’indicazione delle conseguenze che dette minacce possono avere sui dati e sulla sicurezza dei trattamenti.

Tipo	**Minacce**	**Conseguenze sui dati o sulla sicurezza dei trattamenti**
Comportamento di soggetti interni, accidentali o volontari	Ingressi non autorizzati a locali/aree ad accesso ristretto	Danneggiamento hardware e software; possibilità di consultazione non autorizzata; distruzione, perdita, modifica di dati non consentita
	Sottrazione di documenti contenenti dati	Possibilità di consultazione non autorizzata; distruzione, perdita, modifica di dati e documenti non consentita
	Carenza di consapevolezza, disattenzione, incuria	Possibilità di consultazione non autorizzata; distruzione, perdita, modifica di dati non consentita
	Comportamenti sleali o fraudolenti	Acquisizione di dati da utilizzare con vantaggio personale (comunicazione informazione a concorrenti, atti di sabotaggio)
	Ignoranza procedurale	Possibilità di consultazione non autorizzata; distruzione, perdita, modifica di dati non consentita
	Errore o disattenzione	Possibilità di distruzione, perdita, modifica di dati non prevista (es. chiusura di computer mentre è in corso l'aggiornamento patch)
	Errore nella gestione della sicurezza	Danneggiamento hardware e software distruzione, perdita di dati (es. strumento elettronico incustodito durante la sessione di trattamento dati)
	Uso illegittimo di strumenti	Possibilità di utilizzo dei dati ad uso personale, consultazione non autorizzata; distruzione, perdita, modifica di dati non consentita
	Installazione non autorizzata di strumenti	Possibilità di consultazione non autorizzata; distruzione, perdita, modifica di dati non consentita, comunicazione o diffusione illegittima di dati
	Danneggiamento degli strumenti o apparati	Possibile distruzione, perdita, modifica non prevista dei dati
	Furto di strumenti e apparati	Possibilità di consultazione non autorizzata; comunicazione o diffusione illegittima di dati

	Installazione o produzione di copie di dati abusive	Acquisizione di dati da utilizzare con vantaggio personale e/o comunicazione o diffusione illegittima di dati
	Uso improprio del software	Possibile distruzione, perdita, modifica non prevista dei dati
	Furto o disinstallazione di software	Possibilità di consultazione non autorizzata; distruzione, perdita, modifica di dati non consentita
	Danneggiamento del software	Possibilità di consultazione non autorizzata; distruzione, perdita, modifica di dati non consentita
	Installazione non autorizzata di software	Possibilità di consultazione non autorizzata; distruzione, perdita, modifica di dati non consentita, comunicazione o diffusione illegittima di dati
	Erronea abilitazione all'accesso	Possibilità da parte di soggetti non incaricati di consultare, distruggere, modificare, comunicare, diffondere dati
	Modifica non controllata	Possibilità di modifica di dati non consentita
	Cancellazione	Possibilità di distruzione o perdita di dati non prevista
	Distruzione	Possibilità di distruzione o perdita di dati non prevista
	Diffusione illegittima	Possibilità di comunicazione o diffusione di dati non autorizzata
	Altri atti di sabotaggio	Possibilità di utilizzo dei dati ad uso personale, consultazione non autorizzata; distruzione, perdita, modifica di dati non consentita; comunicazione o diffusione di dati non autorizzata
	Sottrazione delle credenziali di autenticazione	Possibilità di accesso non consentito, distruzione, perdita, modifica di dati con responsabilità attribuita ad altri
Comportamento di soggetti esterni, accidentali o volontari	Azione di virus informatici o di altri programmi dannosi	Danneggiamento software e/o accesso non consentito, distruzione, perdita, modifica, invio di dati a terzi
	Spamming o altre tecniche di sabotaggio	Intasamento/blocco della casella postale con possibile perdita di dati
	Malfunzionamento, degrado, degli strumenti	Distruzione, perdita, modifica di dati
	Accessi esterni, fisici e logici, non autorizzati	Possibilità da parte di terzi non autorizzati di consultare, distruzione, modificare, comunicare, diffondere dati
	Ingressi non autorizzati a locali/aree ad accesso ristretto	Danneggiamento hardware e software; possibilità di consultazione non autorizzata; distruzione, perdita, modifica di dati non consentita
	Intercettazioni di informazioni in rete	Possibilità di accesso non consentito, distruzione, perdita, modifica di dati, comunicazione a terzi
	Sottrazione delle credenziali di autenticazione	Possibilità di accesso non consentito, distruzione, perdita, modifica di dati con responsabilità attribuita ad altri
	Uso illegittimo di strumenti	Possibilità di utilizzo dei dati ad uso personale, consultazione non autorizzata; distruzione, perdita, modifica di dati non consentita
	Danneggiamento degli strumenti	Possibilità di accesso non consentito, distruzione, perdita modifica di dati, comunicazione a terzi
	Furto o disinstallazione di	Possibilità di consultazione non autorizzata;

	software	distruzione, perdita, modifica di dati non consentita
	Danneggiamento del software	Possibilità di consultazione non autorizzata; distruzione, perdita, modifica di dati non consentita
	Furto di strumenti e apparati	Possibilità di consultazione non autorizzata; comunicazione o diffusione illegittima di dati
	Installazione non autorizzata di strumenti	Possibilità di consultazione non autorizzata; distruzione, perdita, modifica di dati non consentita, comunicazione o diffusione illegittima di dati
	Installazione non autorizzata di software	Possibilità di consultazione non autorizzata; distruzione, perdita, modifica di dati non consentita, comunicazione o diffusione illegittima di dati
	Installazione o produzione di copie abusive	Acquisizione di dati da utilizzare con vantaggio personale e/o comunicazione o diffusione illegittima di dati
	Altre intercettazioni	Possibilità di accesso non consentito, modifica di dati con responsabilità attribuita ad altri; comunicazione o diffusione illegittima di dati
	Altri atti di sabotaggio	Possibilità di uso dei dati ad uso personale, consultazione non autorizzata; distruzione, perdita, modifica illecita; comunicazione o diffusione di dati non autorizzata
	Furto di credenziali di autenticazione	Accesso non consentito, distruzione, perdita, modifica, diffusione di dati con responsabilità attribuita ad altri
Tecniche	Dismissione, rottamazione o Interruzione d'uso	Possibilità di consultazione e comunicazione di dati riservati contenuti su strumenti informatici dismessi o in assistenza per manutenzione
	Interventi di Manutenzione	Possibilità di consultazione e comunicazione di dati riservati da parte di chi esegue aggiornamenti, integrazioni, modifiche ai programmi
	Interruzione d'uso del sfwr	Impossibilità di consultazione e di trattamento di dati
	Interruzione della connessione	Rallentamento o blocco dell’attività operativa, con necessità di ricorso ad altri canali di comunicazione
	Guasto tecnologico	Possibilità di distruzione, perdita, modifica di dati o di comunicazione illegittima a terzi
	Guasti a sistemi complementari	distruzione e perdita di dati
Naturali	Terremoto o smottamento	Danneggiamento hardware e software, distruzione, perdita di dati
	Incendio, fulmine	Danneggiamento hardware e software, distruzione, perdita di dati
	Esplosione	Danneggiamento hardware e software, distruzione, perdita di dati
	Alluvione, allagamento	Danneggiamento hardware e software, distruzione, perdita di dati

Infrastruttura informatica e misure di sicurezza

Premesso che il sistema informativo di **NEW SYS SRL**, composto da:

- 1 computer client fissi,

- 2 computer client portatili,

- 0 tablet,

- 1 smartphone,

presenta una architettura Peer-To-Peer, esso è così sinteticamente descrivibile:
1 PC FISSO CON WINDWS 10 E 2 PORTATILE WINDOWS 10 COLLEGATI ALLA RETE AZIENDALE.
Le misure di sicurezza adottate sul server, ovvero sul client che svolge anche funzioni di server, sono le seguenti:
N.A.
Il sistema Firewall adottato presenta le seguenti caratteristiche:
FIREWALL WINDOWS DEFENDER
NEW SYS SRL ha adottato il seguente sistema antivirus e antimalware:
AVAST ANTIVIRUS SUI PC AZIENDALI
Il fornitore di connettività è:
Telecom
La posta elettronica Viene consultata attraverso caselle configurate su ciascun client e il server di posta utilizzato è Altro
(DIAMONDWEB)
Il processo di produzione e conservazione delle copie di sicurezza è il seguente:
BACK UP SETTIMANALE SU NAS ESTERNO E CLOUD ONE DRIVE.
NEW SYS SRL utilizza il seguente sistema di gestione:
PROGRAMMA LIGA DI LEONARDO TECH PER FATTURAZIONE, PREVENTIVI, ANAGRAFICA CLIENTI E FORNITORI E MAGAZZINO.

Sicurezza fisica e antintrusione

Per quanto concerne la sicurezza fisica e antintrusione, la sede di **NEW SYS SRL** ubicata in VIA GUIDO MOTTA 13 – 12036 REVELLO, presenta le seguenti caratteristiche:
- la sede è videosorvegliata
- l'ingresso, nelle ore di lavoro, è presidiato
- il server e gli apparati di rete sono protetti da incendio, fumi, discontinuità di alimentazione elettrica
- Le copie di sicurezza dei dati e i supporti di memorizzazione sono custoditi in cassetti o armadi sicuri
- È applicata la "politica della scrivania pulita"
- Gli addetti al trattamento sono formati e consapevoli in materia di data protection