VALUTAZIONE DEL RISCHIO PER LA SICUREZZA DEI DATI

Indice

Stato della revisione del documento:

Rev. N. e Data	Motivo della Revisione
Rev. 0 del 25-07-2025	Prima emissione

1. Introduzione

Vivaldi & Cardino S.p.A è una azienda che opera in Italia dal 1960 nel settore delle pulizie e dei multiservizi, presso aziende pubbliche e private, e fornisce servizi di prima qualità per poter soddisfare le molteplici esigenze presenti sul mercato.

Nell'ambito delle sue attività, l'azienda entra in contatto con diversi documenti contenenti informazioni sensibili e per assicurarne una corretta conservazione non vengono archiviati localmente sui dispositivi, ma sono gestiti in sicurezza tramite un'infrastruttura IT mista che include sia server interni per la gestione dei dati aziendali, contratti e documentazione operativa, sia server in cloud gestiti e completamente sotto la responsabilità di fornitori esterni selezionati. I server interni sono protetti, regolarmente sottoposti a back up e dotati di soluzioni di sicurezza per garantire la protezione dei dati.

Questo documento di valutazione del rischio per la sicurezza dei dati evidenzia i principali rischi per la sicurezza delle informazioni, determinare le priorità di risposta alle minacce e stabilisce i controlli necessari per proteggere gli asset aziendali e i dati sensibili gestiti sia internamente che esternamente.

2. Risorse aziendali

Le risorse aziendali individuate sono suddivise nelle seguenti categorie:

Risorse tecnologiche (Asset IT):

- Server interni utilizzati per la gestione e l'archiviazione dei dati aziendali, dei contratti e della documentazione operativa.
- Server cloud e infrastrutture IT gestite da fornitori terzi, utilizzate per l'archiviazione di documenti riservati e dati sensibili (es. dati sanitari dei lavoratori e altre informazioni personali).
- Sistemi di backup, sia per i server interni (protetti da crittografia), sia per i dati in cloud, che garantiscono ridondanza e sicurezza delle informazioni.
- Reti aziendali e connessioni protette per l'accesso sicuro ai dati interni e cloud.
- Dispositivi endpoint, come PC, laptop e dispositivi mobili aziendali, dotati di soluzioni di sicurezza per la protezione dei dati locali e l'accesso sicuro ai sistemi centrali.
- Software gestionali e applicativi (ERP) utilizzati per la gestione operativa e amministrativa dell'azienda.
- Sistemi di posta elettronica e piattaforme di collaborazione aziendale.

Informazioni aziendali (Asset informativi):

- Dati relativi a clienti e fornitori.
- Documenti sanitari e sensibili dei dipendenti, archiviati in ambienti cloud sicuri.
- Informazioni riservate di progetto e dati strategici per il business.

- Documentazione finanziaria e contabile.

Risorse fisiche:

- Edificio aziendale, locali e uffici.
- Sistemi di sicurezza fisica, come impianti di videosorveglianza e accessi tramite badge.

Risorse umane:

- Dipendenti interni e consulenti esterni.
- Fornitori di servizi, in particolare quelli coinvolti nella gestione di infrastrutture cloud e dati sensibili.

3. Identificazione delle Minacce e delle Vulnerabilità

Minaccia	Descrizione	Vulnerabilità
Malware e Ransomware	Software dannoso che può colpire i dispositivi aziendali e i server interni.	Dispositivi non aggiornati; rischio di phishing.
Furto di dati e accesso non autorizzato	Accesso illecito a dati riservati o sensibili, sia tramite i server interni sia tramite server cloud dei fornitori.	Mancanza di autenticazione forte e controlli di accesso; vulnerabilità nella rete o nei sistemi cloud.
Compromissione della sicurezza dei fornitori	Rischio che i fornitori cloud subiscano una violazione dei dati aziendali.	Insufficiente verifica dei fornitori e mancanza di audit regolari sui protocolli di sicurezza.
Errore umano nella gestione dei dati	Rischio di condivisione accidentale o errata di documenti riservati, sia interni sia in cloud.	Assenza di procedure formali e formazione per la gestione dei dati sensibili.
Interruzione di servizio dei fornitori o dei server interni	Rischio che il fornitore cloud o i server interni subiscano un'interruzione di servizio.	Mancanza di un piano di continuità operativa sia per l'infrastruttura interna sia per i fornitori di cloud.
Disastri naturali	Incendi, alluvioni che possono danneggiare l'infrastruttura fisica locale.	Mancanza di un piano di continuità operativa per i server interni.

4. Valutazione del Rischio

Ogni rischio viene valutato in base a danno e probabilità di accadimento:

P (probabilità evento)					
	Molto probabile = 4	4	8	12	16
	Probabile = 3	3	6	9	12
	Poco probabile = 2	2	4	6	8
	Improbabile = 1	1	2	3	4
		Lieve = 1	**Medio = 2**	**Grave = 3**	**Molto grave = 4**
		D (entità danno)			

Significatività del rischio		**Priorità delle misure di tutela**
Rischio Basso **Valori da 1 a 3**	Rischi potenziali sotto controllo	Valutare eventuali azioni migliorative da pianificare nel ciclo di manutenzione ordinaria. Esempi: mettere in sicurezza il CED da rischi idrologici, incendi o furti, mediante sistemi di allarme e videosorveglianza.
Rischio Medio **Valori da 4 a 6**	Rischi da monitorare	Verificare che le misure di protezione siano adeguate. Promuovere azioni correttive o migliorative da implementare nel breve-medio termine. Esempi: cifratura automatica all'avvio delle macchine, installazione di agent per bloccare l'esecuzione di programmi non autorizzati.
Rischio Alto **Valori da 8 a 9**	Rischi significativi	Intervenire migliorando P e/o D. Attuare azioni correttive entro tempi brevi. Esempi: aggiornamento di firewall e server, verifica dei log di sistema, sensibilizzazione degli utenti, creazione di una DMZ perimetrale.
Rischio Molto Elevato **Valori da 12 a 16**	Condizione di rischio inaccettabile	Attuare immediatamente interventi correttivi. Esempi: aggiornamento antivirus, rafforzamento della sicurezza perimetrale, verifica continua di server, applicazioni, dispositivi mobili e firewall.

Descrizione Rischio	D	P	Livello di Rischio
Malware e Ransomware	Alto	Medio	Alto
Furto di dati e accesso non autorizzato	Alto	Medio	Alto
Compromissione della sicurezza dei fornitori	Alto	Medio	Alto
Errore umano nella gestione dei dati	Alto	Medio	Alto
Interruzione di servizio dei fornitori	Medio	Medio	Medio
Disastri naturali	Alto	Basso	Medio

5. Eventi critici e misure attive per garantire la continuità operativa (Business Continuity)

Gli eventi che potrebbero compromettere la continuità dei servizi aziendali, in particolare quelli legati al reparto IT, includono:

Interruzione o indisponibilità del personale IT, causata da:

- Scioperi o agitazioni sindacali;
- Assenteismo per malattia o indisponibilità prolungata;
- Assenza o malfunzionamento dei backup (backup non eseguiti, corrotti o irrecuperabili);
- Malfunzionamenti gravi dei server interni.

Eventi esterni o straordinari, tra cui:

- Calamità naturali (es. alluvioni, incendi);
- Attacchi informatici (hackeraggio, ransomware, DDoS);
- Furto di apparati IT e sistemi di archiviazione;
- Emergenze sanitarie, come nel caso della pandemia da COVID-19.

6. Priorità delle Risposte e Azioni di Mitigazione

Per mitigare i rischi legati alla gestione dei dati sensibili, sia su server interni sia presso fornitori cloud, sono attualmente in vigore le seguenti misure:

Gestione e Sicurezza dei Documenti Sensibili (interni e cloud):

- **Crittografia dei Dati**: Tutti i dati sensibili vengono cifrati sia in fase di archiviazione che di trasferimento, per garantirne la riservatezza anche in caso di accesso non autorizzato.
- **Controllo degli Accesso**: Implementazione di sistemi di autenticazione a più fattori (MFA) e gestione degli accessi basata sui ruoli (RBAC), per limitare l'accesso alle informazioni solo al personale autorizzato.
- **Monitoraggio e Logging**: Tutti gli accessi ai sistemi interni e cloud vengono registrati e monitorati costantemente. Sono previsti audit periodici per individuare eventuali anomalie o tentativi di accesso sospetti.

Gestione dei fornitori cloud e sicurezza interna:

- **Accordi contrattuali (NDA e SLA)**: Con ogni fornitore di servizi cloud sono stipulati accordi di riservatezza (Non Disclosure Agreement) e Service Level Agreement dettagliati, nei quali sono esplicitati standard minimi di sicurezza e requisiti di continuità operativa.
- **Audit e verifiche periodiche**: Vengono condotti controlli periodici sulle infrastrutture interne e su quelle dei fornitori, verificando il rispetto degli standard di sicurezza e l'aderenza a certificazioni come SOC 2 o ISO/IEC 27001.
- **Piani di continuità operativa e disaster recovery:** L'azienda assicura che siano attivi e testati sia il piano interno di disaster recovery sia quelli dei fornitori. Tali piani sono coordinati con le procedure aziendali interne di Vivaldi&Cardino.

Formazione e Sensibilizzazione del Personale:

- **Sessioni di Formazione Continua**: Il personale è periodicamente formato sulla protezione dei dati, sulla gestione sicura delle informazioni sensibili, sul riconoscimento delle minacce (phishing, ingegneria sociale) e sulle best practice operative.
- **Policy per la Condivisione Sicura**: Sono state redatte linee guida aziendali che regolano la condivisione di dati riservati, consentendola solo tramite canali approvati e sicuri, previa verifica dell'identità dei destinatari

7. Statement of Applicability

Di seguito sono elencati i controlli di sicurezza adottati da Vivaldi&Cardino per la gestione dei dati riservati in ambiente cloud, in conformità alle normative vigenti e alle best practice di sicurezza:

Controllo	Applicabilità	Descrizione
Crittografia dei Dati Sensibili	Applicabile	Tutti i dati riservati vengono cifrati sia in transito che a riposo, per garantirne la riservatezza anche in caso di accesso non autorizzato.
Controlli di Accesso e MFA	Applicabile	Viene utilizzata l'autenticazione a più fattori (MFA) e l'accesso è regolato da policy basate sui ruoli (RBAC), limitando l'accesso alle sole persone autorizzate.
Monitoraggio degli Accessi e Logging	Applicabile	Gli accessi ai dati sensibili vengono monitorati costantemente. Sono previsti audit periodici per rilevare eventuali anomalie o violazioni.
Contratti di Riservatezza (NDA)	Applicabile	Tutti i fornitori cloud sono vincolati da NDA e da SLA che definiscono chiaramente gli standard di sicurezza richiesti.
Audit di Sicurezza per i Fornitori	Applicabile	Sono effettuate verifiche periodiche sui fornitori per valutare la conformità ai requisiti di sicurezza e alle certificazioni riconosciute (es. ISO/IEC 27001, SOC 2).
Gestione della Continuità Operativa	Applicabile	I piani di disaster recovery dei fornitori cloud sono integrati con il piano di continuità operativa dell'azienda.
Formazione e Sensibilizzazione del Personale	Applicabile	Il personale riceve formazione periodica su tematiche di sicurezza informatica, gestione dei dati e prevenzione delle minacce.
Policy di Condivisione Sicura	Applicabile	Le informazioni riservate possono essere condivise solo attraverso canali approvati e sicuri, secondo procedure formalizzate.

8. Conclusione

L'adozione di un insieme strutturato di controlli di sicurezza per la gestione dei dati riservati su server cloud di fornitori esterni consente all'azienda di ridurre in modo efficace i rischi di compromissione, perdita o accesso non autorizzato alle informazioni sensibili, contribuendo a garantire:

- Riservatezza, attraverso meccanismi di cifratura e controllo degli accessi;
- Integrità, mediante il monitoraggio continuo e la verifica dell'affidabilità dei fornitori;
- Disponibilità, grazie alla presenza di piani di continuità operativa integrati e costantemente aggiornati.

Tali misure supportano una gestione responsabile delle informazioni aziendali, rafforzando la resilienza della Vivaldi & Cardino.

Data: 28/07/2025

L'Amministratore Delegato