*Il presente documento rappresenta un esempio di IT Disaster Recovery Plan che potrebbe essere adottato da un laboratorio di prova per il contenimento del rischio di “perdita di dati”.*

Information Technology Disaster Recovery Plan (IT DRP)

# **Politica aziendale**

La direzione aziendale del laboratorio di Prova XXXXX ha approvato la seguente politica:

* La società deve attuare piani di Business Continuity e Disaster Recovery efficaci
* Tutti i piani Business Continuity e Disaster Recovery devono includere elementi, sistemi e reti di infrastrutture essenziali e fondamentali, in base alle attività aziendali chiave
* I piani devono essere periodicamente testati in un ambiente simulato affinché possano essere implementati in situazioni di emergenza e la direzione e il personale sappiano come devono essere eseguiti
* Tutto il personale deve essere informato in merito ai piani e ai rispettivi ruoli
* I piani di Business Continuity e Disaster Recovery devono essere mantenuti aggiornati …..

**Analisi dell'impatto sull'attività operativa**

.

|  |  |  |
| --- | --- | --- |
| **Processo laboratorio di prova** | **Risorsa IT** | **Impatto sull'attività in caso di interruzione della risorsa** |
| *Accettazione campioni* | *- Server**- LIMS**- PC client* | *Ripercussione immediata sulla produttività, lo svolgimento dell'attività diventa critico dopo 24 ore* |
|  |  |  |
| *Esecuzione prove di laboratorio* | *- PC di gestione strumentazione analitica* | *Arresto immediato di esecuzione delle prova, lo svolgimento dell'attività diventa critico dopo 4 ore* |
|  |  |  |
| *Compilazione Rapporti di Prova* | *- Server**- LIMS**- PC client* | *Utilizzo di procedure manuali prestabilite, lo svolgimento dell'attività diventa critico dopo 48 ore* |
|  |  |  |
| *……..* |  |  |

|  |  |
| --- | --- |
| **Servizio IT** | **Esigenze aziendali in termini di:** |
|  | **RTO** | **RPO** |  |
| *Server* | *2 ore* | *24 ore* |
| *LIMS* | *3 ore* | *24 ore* |
| *PC client - ciascuno* | *1 ora* | *0* |
| *PC di gestione strumenti analitici* | *1 ora* | *5 ore* |
| *……..* |  |  |

Il **Recovery Time Objective (RTO)** è il tempo necessario per rendere nuovamente possibile l'operatività di un processo aziendale in seguito a un'interruzione IT (incluse tutte le azioni di recupero IT).

Il **Recovery Point Objective (RPO**) rappresenta la massima quantità di dati che il sistema può perdere a causa di guasto improvviso, senza essere in grado di recuperarli. Questo parametro consente il recupero fino a un "punto nel tempo" precedente al disastro.

**Pianificazione del ripristino delle attività**

**Dati di contatto**

|  |  |  |  |
| --- | --- | --- | --- |
| **Servizio IT** | **Nominativo contatto** | **Modalità contatto** | **Orari struttura** |
| *Server* | *Ditta XXXX* | *Telefono* | *…….* |
| *LIMS* | *Proactive sas* | *Casella vocale**050 703284* |  |
| *PC client*  | *Ditta XXXX* | *Telefono* |  |
| *PC di gestione strumenti analitici* | *Ditta yyyyy* | *Apertura tiket: www.sito.it* |  |
| *……..* |  |  |  |

**Procedure di Disaster Recovery (DR) approntate**

A seconda del tipo di incidente, è possibile attivare una o più procedure di Disaster Recovery.

## Piano di DR in caso di attacco ransomware

|  |  |
| --- | --- |
| **Scenario** | Ransomware rilevato su uno o più computer/server |
| **Cause possibili** | Malware spesso  |
| **Servizi IT e dati a rischio** | Applicativo LIMSDatabase LIMSSistema di archiviazione (backup)File Rapporti di Prova emessi |
| **Impatto** | Perdita o danneggiamento di dati |

|  |  |
| --- | --- |
| **Prevenzione** | * Proteggere la sicurezza e-mail per evitare tentativi di phishing.
* Rendere sicura la propria rete e l'ambiente IT con firewall e antivirus;
* Aggiornare costantemente Antivirus (procedura automatizzata)
* Formare i dipendenti all’utilizzo appropriato delle risorse aziendali IT (es. non installare software di dubbia provenienza, limitare la navigazione internet, non cliccare su link ricevuti a mezzo mail senza conoscere la provenienza;)
* Prevedere l’uso di una VPN per tutti i dipendenti non presenti in sede che utilizzano il Desktop Remoto
* Assicurarsi di avere impostato password complessa e con scadenza obbligatoria (Proactive LIMS >> Impostazioni Applicativo >> GDPR)

* Implementare un piano di backup e ripristino per tutti i dati critici utilizzando la strategia 3-2-1[[1]](#footnote-1)

3 - Conservare almeno **tre copie** dei dati.2 - Memorizzare i dati su **due diversi tipi di supporti**.1 - Proteggere **una copia** dei backup fuori sede.* Testare regolarmente i backup per garantire una corretta configurazione.
* Isolare i backup critici dalla rete (air gap) per assicurare la massima protezione (esempio se si utilizza un hard disk esterno NON metterlo in rete o rischia di essere compromesso anch’esso in un attacco Ransomware)
 |

|  |  |
| --- | --- |
| **Piano di azione in caso****di attacco ransomware** | * Scollegare l'hardware interessato **rimuovendo il cavo di rete.**
* Procedere con la formattazione dei dispositivi “infettati” dal ransomware virus
* Controllare il backup e procedere con le operazioni di ripristino
 |

## Ultimo Disaster Recovery Test Effettuato

|  |  |  |
| --- | --- | --- |
| **Processo testato** | **Data** | **Esito positivo o negativo rispetto alle esigenze aziendali** |
| Ripristino LIMS |  | RTO = 3 oreRecovery Time effettivo = | RPO = 24 oreRecovery point effettivo =  |
|  |  |  |
|  |  |  |

Prossimo Disaster Recovery test previsto: entro 12 mesi

1. **Alcuni supporti utili per il backup 3 2 1**

- SSD o hard disk esterno, ad esempio, avendo l’accortezza di conservare tale dispositivo in un altro luogo;

- Una seconda copia potreste caricarla su un servizio di cloud storage. In questo modo, avrete una copia letteralmente “offsite“, ovvero non nello stesso luogo fisico dove lavorate.

- Una terza soluzione che potrebbe essere un blu-ray, un DVD, o magari una scheda microSD.

- Un’altra soluzione che potreste considerare è un dispositivo NAS (Network Attached Storage). Con un NAS, avrete uno spazio di backup dedicato e protetto. [↑](#footnote-ref-1)