**Identificazione dell’incidente**

*In questa sezione deve essere indicata informazioni generali su come l’incidente è stato identificato:*

* *Data e ora di rilevazione*
* *Modalità di rilevazione*
* *Tipologia dell’incidente*
* *Gravità dell’incidente*

**Descrizione dell’incidente**

*In questa sezione devono essere indicati informazioni dettagliate sull’incidente, in particolare:*

* *Data e ora di accadimento*
* *Modalità di accadimento dell’incidente*
* *Sistemi impattati*
* *Numero e tipologia di utenti impattati*
* *Durata dell’incidente (dal momento della rilevazione al ripristino)*
* *Si è trattato di data breach?*
* *Tipologia di dati coinvolti.*
* *Tipo di impatto per utenti ed azienda*

**Modalità di risposta all’incidente**

*In questa sezione devono essere riportate informazioni dettagliate sulle azioni di risposta intraprese, in particolare:*

* *Azioni di contenimento*
* *Azioni di rimozione*
* *Azioni di ripristino*
* *Comunicazioni interne ed esterne*
* *Eventuali notifiche ad esterni (Garante, Interessati, CSIRT, ecc.)*

**Conclusioni**

*In questa sezione devono essere riportate informazioni conclusive, come:*

* *Breve riepilogo dell’incidente*
* *Lezioni apprese*
* *Eventuali misure di sicurezza aggiuntive necessarie*