|  |  |
| --- | --- |
| P:\RER\sitoParER\Grafica\Loghi\logo-rer-+-ibc.jpg | P:\RER\sitoParER\Grafica\LogoParer-2013\LogoParer.jpg |
|  | |
| PG14 Gestione incidenti di sicurezza   |  |  | | --- | --- | | *Codice documento* | PG14\_GestIncSicurezza | | *Versione* | V1.0 |  |  |  |  |  | | --- | --- | --- | --- | |  | *Data* | *Nominativo* | *Funzione* | | *Redazione* | 24/05/2018 | Désirée Gnesini / Monia Perseo / Giovanni Galazzini | *Consulenti esterni* | | *Verifica* | 12/10/2018 | *Marco Calzolari* | *Responsabile della sicurezza dei sistemi per la conservazione* | | *Approvazione* | 12/10/2018 | *Marco Calzolari* | *Responsabile del Servizio* | | |
|  | |
| Il presente documento è rilasciato sotto la licenza **Attribuzione-Non commerciale** delle Creative Commons. | |

# Indice

Indice 3

Storia delle modifiche del documento 4

Classificazione del documento 4

Lista di distribuzione 4

Introduzione 5

Scopo della procedura 5

Campo di applicazione 5

1. Gestire gli eventi 10

1.1. Rilevare l’evento 10

1.2. Valutare l’evento 11

1.3. Processare l’evento (bassa gravità) 12

2. Gestire incidenti di sicurezza 13

3. Gestire attività post-incidente 13

Matrice RACI 14

Allegato: Comunicazioni di eventi/incidenti di sicurezza 15

# Storia delle modifiche del documento

| **Versione** | **Variazioni** | **Data** |
| --- | --- | --- |
| 1.0 | Prima emissione | 12/10/2018 |

# Classificazione del documento

|  |  |
| --- | --- |
| **Livello di Riservatezza** | *Ad Uso interno* |
| **Classificazione** | **PaRERDoc *2.4 Procedure/Esercizio*** |

# Lista di distribuzione

| **Soggetti da Notificare** | |
| --- | --- |
| ***Nominativi*** | ***Ruoli Organizzativi*** |
| Tutto il personale ParER |  |
| Responsabile SICTR |  |

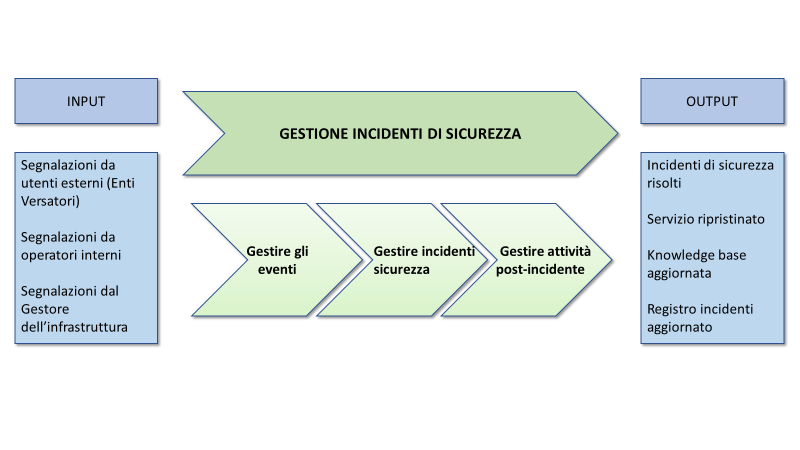
# Introduzione

## Scopo della procedura

La procedura *Gestione incidenti di sicurezza* descrive le modalità con cui vengono gestiti gli eventi che hanno un impatto sui requisiti di integrità, disponibilità e riservatezza dei dati conservati o del Servizio di conservazione.

L’obiettivo del processo viene raggiunto attraverso le seguenti attività:

* tracciare gli eventi rilevanti per la sicurezza delle informazioni;
* indirizzare le azioni di risposta ai fini del contenimento o prevenzione degli impatti;
* analizzare periodicamente gli incidenti/eventi registrati al fine di migliorare il sistema dei controlli interni e le capacità di risposta dell’organizzazione in maniera proporzionale agli effettivi rischi.



## Campo di applicazione

L’ambito di applicabilità del presente documento è circoscritto agli eventi relativi al sistema e al processo di conservazione rilevanti per la sicurezza delle informazioni.

A tale scopo si definisce:

* **Evento**: un cambiamento di stato, un’anomalia, un accadimento che di per sé non provoca necessariamente danno;
* **Incidente di sicurezza delle informazioni:** un evento che abbia effettivamente provocato una violazione dei requisiti di riservatezza, integrità e/o disponibilità delle informazioni legate a processi/servizi aziendali, con conseguente danno per l’organizzazione.

Un evento può quindi provocare o meno un incidente di sicurezza.

La procedura rileva quindi:

* Eventi rilevanti per la sicurezza, al fine di prevenire la possibile degenerazione in incidenti;
* incidenti, al fine di contenerli e minimizzarne gli effetti.

È stata definita una classificazione degli eventi/incidenti a partire della classificazione presente nel *Disciplinare tecnico per la gestione degli incidenti di sicurezza informatica della Giunta e dell’Assemblea Legislativa della Regione Emilia-Romagna*), arricchita di una categoria che riguarda una tipologia di eventi/incidenti specifica del servizio di conservazione:

* ***Codice Malevolo***;
* ***Accesso Non Autorizzato***;
* ***Denial of Service***;
* ***Malfunzionamento****;*
* ***Disastro***;
* ***Uso Inappropriato***;
* ***Errori*** *(classificazione non prevista dal Disciplinare regionale).*

Sono considerati eventi rilevanti per la sicurezza o incidenti tutti gli eventi riportati nella tabella seguente, tranne gli eventi appartenenti alla categoria dei Malfunzionamenti, che vengono considerati rilevanti solo se di gravità alta o media.

Le tipologie di eventi (qui di seguito elencati), che possono avere impatto sulla sicurezza del sistema di conservazione di ParER, sono valutati nell’ambito della specifica analisi del rischio.

| **Macro- tipologia evento/incidente** | **Tipologie evento/incidente** | **Descrizione** |
| --- | --- | --- |
| ***Codice Malevolo*** | *Contaminazione da Malware* | Un virus, worm, trojan, backdoor, spyware, o qualsiasi altro codice malevolo che infetti un Sistema. |
| ***Accesso Non Autorizzato*** | *Accesso logico non autorizzato (attacco deliberato)* | Accesso logico a reti, sistemi, applicazioni o altre risorse tecnologiche di proprietà del ParER da parte di personale non autorizzato. |
| *Accesso (fisico) non autorizzato al data center* | Accesso fisico alla porzione di Data Center di ParER da parte di personale non autorizzato. |
| *Accesso (fisico) non autorizzato agli uffici degli archivisti* | Accesso agli uffici degli archivisti da parte di personale non autorizzato. |
| *Accesso fisico agli uffici sistemisti non autorizzato* | Accesso agli uffici sistemistici da parte di personale non autorizzato. |
| *Intercettazione dati non autorizzata* | Accesso non autorizzato ai dati di conservazione |
| ***Denial of Service*** | *Attacco DoS* | Attacco informatico, intenzionale o non, alla disponibilità di una rete o sistema. Qualora abbia successo, comporta la difficoltà all’accesso o la totale indisponibilità di determinati sistemi e/o servizi. |
| ***Malfunzionamento\****  ***\****Sono gestiti in questo processo solo gli eventi/incidenti di categoria “Malfunzionamento” a gravità media/alta. | *Baco o malfunzionamento sw* | Danneggiamento software, oppure degrado delle performance (per cause esterne) o di servizio. |
| *Guasto hw apparecchiature ICT - server e storage* | Danneggiamento di un componente hardware (server, storage), oppure degrado delle performance (per cause esterne) o di servizio. |
| *Guasto hw apparecchiature ICT – LAN* | Danneggiamento di un componente hardware (rete), oppure degrado delle performance (per cause esterne) o di servizio. |
| *Guasto linee di comunicazione* | Danneggiamento di un componente che comporta l’indisponibilità del servizio di conservazione. |
| *Guasto hw impianti di data center* | Danneggiamento di un componente hardware (impianto di condizionamento, illuminazione, …), oppure degrado delle performance per cause esterne o di servizio. |
| ***Errori nel contenuto dei dati conservati*** | *Errori nel contenuto dei dati conservati:*   * *Errore gestione applicativa durante attività di manutenzione ordinaria e/o configurazione dei sistemi applicativi* * *Errore gestione sistemi durante attività di manutenzione ordinaria e/o configurazione delle infrastrutture IT* * *Errore operatori durante lo svolgimento del servizio di Conservazione)* | Errori che comportano la presenza di dati non corretti sul sistema che non possono essere corretti con le procedure standard. |
| ***Disastro*** | *Incendio del data center* | Evento distruttivo, legato alla porzione di data center dedicata a ParER, non provocato direttamente da azione di operatori informatici che condiziona direttamente l’operatività dei sistemi informatici. |
| *Allagamento del data center* | Evento distruttivo, legato alla porzione di data center dedicata a ParER, non provocato direttamente da azione di operatori informatici che condiziona direttamente l’operatività dei sistemi informatici. |
| *Incendio degli uffici degli archivisti* | Evento distruttivo, legato agli uffici degli archivisti, non provocato direttamente da azione di operatori informatici  che condiziona direttamente l’operatività dei sistemi informatici. |
| *Allagamento degli uffici degli archivisti* | Evento distruttivo, legato agli uffici degli archivisti, non provocato direttamente da azione di operatori informatici che condiziona direttamente l’operatività dei sistemi informatici. |
| *Incendio degli uffici sistemisti* | Evento distruttivo, legato agli uffici dei sistemisti, non provocato direttamente da azione di operatori informatici  che condiziona direttamente l’operatività dei sistemi informatici. |
| *Allagamento degli uffici sistemisti* | Evento distruttivo, legato agli uffici dei sistemisti, non provocato direttamente da azione di operatori informatici  che condiziona direttamente l’operatività dei sistemi informatici. |
| *Terremoto* | Evento distruttivo, non provocato direttamente da azione di operatori informatici che condiziona direttamente l’operatività dei sistemi informatici e l’accessibilità alle sedi del ParER. |
| ***Uso Inappropriato*** | *Controlli non adeguati rispetto ai requisiti di business e/o legali* | Violazione delle policy di sicurezza e delle normative relative alle licenze, agli standard e alle normative di legge. |
| ***Eventi/incidenti non rilevati o gestiti*** | *Eventi/incidenti non rilevati* | Eventi non rilevati contestualmente all’accadimento degli stessi. |
| *Eventi/incidenti non gestiti* | Eventi non gestiti contestualmente all’accadimento degli stessi. |

# Gestire gli eventi

## Rilevare l’evento

L’individuazione di un evento rilevante per la sicurezza si basa sul riconoscimento di segnali o eventi che possono provenire da utenti che utilizzano il sistema di conservazione, dal personale interno a ParER (Archivisti e Analisti) relativamente ai sistemi applicativi utilizzati per la conservazione e dal personale del Gestore dell’Infrastruttura (Servizio ICT regionale o Outsourcer del servizio di Disaster Recovery) durante lo svolgimento delle attività di gestione dei sistemi del ParER

Il Gestore dell’Infrastruttura e l'Outsourcer del DR intercettano notifiche di attacco da parte di dispositivi di sicurezza (IDS/IPS, SIEM), notifiche di anomalie da parte di dispositivi di rete e sistemi, esiti di analisi dei log (di rete, di sistema) e bollettini o note informative emanate da parte di organizzazioni affidabili (CERT, vendor di tecnologie, advisor accreditati, polizia postale, etc.).

ParER monitora costantemente i log applicativi e le applicazioni sviluppate con l’obiettivo di rilevare possibili vulnerabilità o minacce.

Per ogni ambito esiste un responsabile di riferimento che costituisce il punto di raccolta delle richieste/esigenze che emergono nell’area di competenza (di seguito nominati Responsabili). In particolare:

* per quanto riguarda gli eventi di tipo applicativo si fa riferimento al Responsabile Tecnologie e sviluppo sistema di conservazione;
* per quanto riguarda anomalie tecniche riconducibili ai fornitori degli Enti Versatori, si fa riferimento all’Area Tecnologie e sviluppo sistema di conservazione;
* per gli eventi relativi all’integrità dei dati, si fa riferimento al Responsabile Funzione archivistica di conservazione;
* per gli eventi rilevati dal personale che gestisce l’infrastruttura si fa riferimento al Responsabile Servizi tecnologici ed infrastrutture; nel caso in cui venisse rilevato un Incidente che coinvolge i Data Center di ParER, il personale è tenuto a coinvolgere immediatamente il Responsabile del Servizio;
* relativamente agli eventi legati alla violazione di policy, standard o normative, si fa riferimento al Responsabile della Sicurezza dei sistemi per la conservazione.

La segnalazione viene esaminata da uno dei Responsabili con lo scopo di:

* classificare l’evento secondo la tabella degli eventi codificati riportata nel paragrafo “Campo di applicazione”;
* verificare la potenziale o effettiva violazione di uno dei requisiti di sicurezza delle informazioni (confidenzialità, integrità, disponibilità) o di requisiti di compliance legale, anche in mancanza di corrispondenza con gli eventi riportati nella tabella degli eventi codificati.

Le segnalazioni di eventi non codificati devono essere inviate al Responsabile della Sicurezza dei sistemi per la conservazione (oppure ad un suo delegato) che procede, nei casi applicabili, all’analisi, alla codifica del nuovo evento, all’inserimento nel registro degli incidenti (“tool di Gestione delle richieste”) e all’aggiornamento della presente procedura.

Indipendentemente dal tipo di evento il Responsabile provvede all’invio di una mail di notifica al Responsabile della Sicurezza dei sistemi per la conservazione (oppure ad un suo delegato) per opportuna registrazione e monitoraggio dell’evento.

La mail di notifica dell’evento deve contenere al minimo le seguenti informazioni:

* Tipologia;
* Data evento;
* Descrizione evento.

Gli eventi individuati dal Gestore dell’infrastruttura e dall’Outsourcer del DR sono tempestivamente segnalati a ParER, in particolare al Responsabile della Sicurezza dei sistemi per la conservazione e al Responsabile Servizi Tecnologici ed infrastrutture per la conservazione che si occupa di:

* informare i soggetti interni a ParER;
* se possibile, mettere in campo azioni correttive (es. iniziative di comunicazione agli Enti) al fine di minimizzare l’impatto sugli utenti finali.

Per questi eventi si passa direttamente al *Sotto-processo PR04.03 Gestire attività post-incidente.*

Nel caso in cui l’incidente/evento sia valutato come “disastro” la risposta viene attuata in base alle procedure di gestione della Continuità Operativa e si innesca il *Sotto-processo PR04.03 Gestire attività post-incidente*.

## Valutare l’evento

La fase di valutazione ha lo scopo di determinare gravità e tipologia degli impatti dell’incidente/evento, in modo da definire:

* aree di competenza a cui indirizzare la notifica per le azioni di risposta;
* procedure esterne o modalità operative a cui indirizzare la notifica per le azioni di risposta ai singoli incidenti;
* priorità delle azioni correttive o di risposta; il grado di priorità è necessario per organizzare le attività di risposta e/o di adeguamento del sistema.

La valutazione viene svolta dagli stessi responsabili sulla base dei seguenti criteri presenti nel *Disciplinare tecnico per la gestione degli incidenti di sicurezza informatica della Giunta e dell’Assemblea Legislativa della Regione Emilia-Romagna*:

| **Gravità evento di sicurezza** | **Descrizione** |
| --- | --- |
| Alta | Il grado di compromissione di servizi e/o sistemi è elevato.  Si rilevano danni consistenti sugli asset.  Il ripristino è di medio o lungo periodo.  L’incidente presenta una tra le seguenti condizioni:   * danni a persone e rilevanti perdite di produttività; * rischio di azioni legali; * estesa infezione virale in grado di compromettere molteplici sistemi e di propagarsi nella rete; * compromissione di sistemi o di reti in grado di permettere accessi incontrollati a informazioni confidenziali; * siti web violati o utilizzati a fini di propagazione di materiale terroristico o pornografico; * frode o attività criminale che coinvolga servizi forniti dall’Ente; * impossibilità tecnica di fornire uno o più servizi critici a un elevato numero di utenti per un intervallo di tempo superiore ai 30 minuti nell’arco di una giornata; * impossibilità tecnica di fornire uno o più servizi critici ad un elevato numero di utenti per intervalli di tempo inferiori ai 30 minuti di tempo ripetuti su più giornate; * impossibilità tecnica di fornire uno o più servizi critici ad una piccola parte di utenti per un periodo di tempo superiore ai 30 minuti di tempo nell’arco di una o più giornate; * impossibilità tecnica di fornire uno o più servizi di criticità media per un periodo di tempo superiore ai 2 giorni lavorativi; * perdita di immagine e/o reputazione nei confronti degli utenti. |
| Media | L’incidente non presenta nessuna condizione che porti alla catalogazione “gravità alta”.  Il grado di compromissione di servizi e/o sistemi è di una certa rilevanza e possono essere rilevati danni sugli asset di una certa consistenza.  Il ripristino ha tempi che non compromettono la continuità del servizio. |
| Bassa | L’incidente non presenta nessuna condizione che porti alla catalogazione “gravità alta o media”.  Non vengono compromessi asset o servizi.  L’incidente presenta le seguenti condizioni:   * Interruzione dell’attività lavorativa di un numero ristretto di dipendenti; * contaminazioni multiple da virus in un medesimo sito; * molteplici sospetti di intrusione da parte di uno stesso attaccante. |

Nel caso in cui si trattasse di un evento configurabile come incidente di sicurezza a alta/media gravità, verrà inviata una mail di notifica al Responsabile della Sicurezza dei sistemi per la conservazione per l’avvio delle attività di gestione dello stesso.

## Processare l’evento (bassa gravità)

Il soggetto incaricato alla gestione dell’evento a bassa gravità analizza la segnalazione ed identifica una possibile soluzione o un workaround.

Qualora, durante l’analisi della soluzione identificata, l’operatore riscontri la necessità di attuare una change significativa al sistema, viene attivato la procedura *Gestione richieste di cambiamento*; in caso contrario si procede alla valutazione della tempistica per la risoluzione: nel caso in cui la soluzione o il workaround implichi tempi di applicazione “significativi” e comunque superiori agli SLA concordati con gli Enti produttori, si provvederà ad inviare opportuna notifica al Responsabile del Servizio.

Il responsabile della gestione dell’evento applica la soluzione o il workaround identificato di competenza al fine di risolvere l’evento/incidente; nel caso in cui l’applicazione della soluzione o del workaround necessiti dell’intervento di altre aree, verrà coinvolto il personale specifico.

In fase di chiusura viene inviata notifica al Responsabile della sicurezza del sistema di conservazione (oppure ad un suo delegato) per l’opportuno aggiornamento delle informazioni contenute nel Registro degli incidenti (“tool di Gestione delle richieste”) e per l’avvio delle attività di analisi post-incidente. Questo comporta l’attivazione dell’attività *Gestire attività post-incidente*.

# Gestire incidenti di sicurezza

Nel caso in cui evento sia valutato di gravità media o alta (incidente) ogni azione di risposta è subordinata alle indicazioni e/o all’approvazione del Responsabile Sicurezza dei sistemi per la conservazione.

In questo caso il Responsabile della Sicurezza dei sistemi per la conservazione, nel caso lo reputi necessario o opportuno, invia notifica alle autorità competenti esterne a ParER (es. Polizia Postale, Garante della Privacy), richiedendo un eventuale loro diretto intervento, e agli Enti produttori i cui dati risultano coinvolti.

Nel caso il sospetto di grave violazione fosse confermato, il Responsabile della Sicurezza dei sistemi per la conservazione decide se:

* richiedere l’intervento di specialisti esterni per azioni di indagine e preservazione di evidenze utili in caso di investigazione forense;
* richiedere al gruppo interno di competenza l’attuazione di azioni di risposta con particolari accorgimenti di registrazione e custodia di tutte le azioni condotte.

# Gestire attività post-incidente

ll Responsabile della Sicurezza dei sistemi per la conservazione (oppure un suo delegato), una volta concluso l’evento/incidente di sicurezza, effettua un’analisi delle vulnerabilità (in riferimento all’elenco dei controlli presenti all’interno del documento “Modello di analisi dei rischi”) associate all’evento/incidente, aggiornando l’apposita sezione del Registro incidenti (“tool di Gestione delle richieste”).

Il Responsabile della Sicurezza dei sistemi per la conservazione (oppure un suo delegato) inserisce/verifica la completezza delle informazioni relative all’incidente/evento di sicurezza nel Registro degli incidenti (“tool di Gestione delle richieste”).

Per ciascun incidente/evento sono previsti i seguenti campi informativi:

* Macro-tipologia;
* Tipologia;
* Vulnerabilità;
* Gravità;
* Struttura competente per la risoluzione;
* Data evento;
* Descrizione evento;
* Data soluzione;
* Soluzione adottata;
* Comunicato da;
* Modalità di comunicazione
* Riferimenti esterni.

Il Responsabile Sicurezza dei sistemi per la conservazione è responsabile del monitoraggio dell’avanzamento delle azioni di risposta e dell’aggiornamento delle informazioni contenute nel Registro degli incidenti (“tool di Gestione delle richieste”).

Nell’ambito delle attività di Riesame della Direzione, il Responsabile della Sicurezza dei sistemi per la conservazione provvede ad una revisione degli incidenti/eventi registrati nel periodo di osservazione, con l’obiettivo di:

* valutare l’andamento complessivo degli incidenti in una determinata finestra temporale,
* determinare l’efficacia delle procedure di gestione degli incidenti attraverso il confronto delle tendenze nei periodi precedenti,
* aggiornare le procedure di gestione dei rischi rispetto ai nuovi fattori di rischio identificati,
* indirizzare possibili miglioramenti nel sistema dei controlli.

La revisione viene documentata nell’ambito del documento di Riesame della Direzione che contiene:

* statistiche sugli incidenti/ eventi:
* numero totale;
* distribuzione per tipologia.

# Matrice RACI

| **RUOLI**  **ATTIVITÀ** | **Archivista** | **Responsabile Funzione Archivistica di Conservazione** | **Area Tecnologie e sviluppo sistemi di conservazione** | **Responsabile Tecnologie e Sviluppo Sistemi di Conservazione** | **Responsabile Esercizio Servizi di Conservazione** | **Fornitore** | **Ente** | **Responsabile della Sicurezza dei sistemi per la conservazione** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Gestire gli eventi |  |  |  |  |  |  |  |  |
| * 1. Rilevare l’evento | R | R | R | R | R |  |  | A |
| * 1. Valutare l’evento | R | R | R | R | R |  |  | A |
| 1.3 Processare l’evento (bassa gravità) | R | R | R | R | R | C | I | A |
| 1. Gestire incidenti di sicurezza |  | C | R | C | C |  |  | A,R |
| 1. Gestire attività post-incidente |  | C | C | C | C |  |  | A,R |

* **R, Responsible:** ha il compito di svolgere una particolare attività
* **A, Accountable:** è responsabile dei risultati dell’attività o ha un ruolo di approvatore
* **C, Consulted:** è coinvolto attivamente nel processo indirizzando le azioni da compiere o le decisioni da prendere
* **I, Informed**: è mantenuto informato sulle azioni da compiere o sulle decisioni prese. Il soggetto informato non può influenzare il risultato

# Allegato: Comunicazioni di eventi/incidenti di sicurezza

La tabella seguente illustra i flussi e le metodiche di comunicazione nella rilevazione e nella risoluzione di incidenti di sicurezza.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Classificazione dell’incidente** | **A chi comunicare** | **Quando comunicare** | **Responsabile** | **Modalità** |
| **Alto** | Enti Produttori  Utenti  Personale ParER  Servizio approvvigionamenti, patrimonio e logistica (in caso di danni all’edificio) | Al termine della macro-attività “Valutare l’evento” del *Sotto-processo PR04.01 Gestire gli eventi* | Responsabile della Sicurezza dei sistemi per la conservazione | E-mail / sistema di trouble ticketing |
| **Medio** | Enti Produttori (in caso di Errori nel contenuto dei dati conservati)  Personale ParER | Al termine della macro-attività “Valutare l’evento” del *Sotto-processo PR04.01 Gestire gli eventi* | Responsabile Funzione archivistica di conservazione | E-mail / sistema di trouble ticketing |
| **Basso** | Enti Produttori (in caso di Errori nel contenuto dei dati conservati)  Archivisti | Al termine della macro-attività “Valutare l’evento” del *Sotto-processo PR04.01 Gestire gli eventi* | Responsabile Funzione archivistica di conservazione | E-mail / sistema di trouble ticketing |