Data integrity : Policy, SOPs, Check-lists

Rita Brusa

IMS MICRONIZZAZIONI

10th NOVEMBER, 2017

Policy aziendale

Piano di emergenza (Contingency Plan) | Piano di Recupero (Disaster Recovery)

Gestione documenti cartacei ed elettronici

Rilascio lotto

Revisione Audit trail

Sicurezza fisica e logica

Abilitazione utenti | Gestione password

Gestione della Configurazione

Gestione della Manutenzione

Archiviazione e Ripristino dei dati e del sistema

Backup | Archiviazione | Periodo di conservazione dei dati | Modalità di smaltimento dati | Gestione raw data

Verifiche periodiche ai sistemi informatici

Change Control

Trasmigrazione dei dati

Formazione

Manutenzione

Gestione eventi sistema

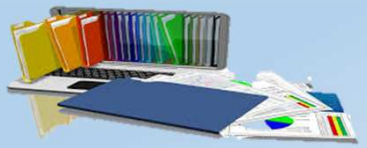
Qualifica fornitori

Contratto con terze parti (SLA : Service Technical Agreement)

Ticket

Firme elettroniche

Utilizzo dei sistemi – Manuali, Istruzioni Operative



POLICY

- Responsabilità
- Normative di riferimento
- Campo di applicazione
- Modalità e frequenza di verifica
- Misure adottate per la sicurezza
- Modalità di conservazione dei dati
- Cyber Security

POLICY

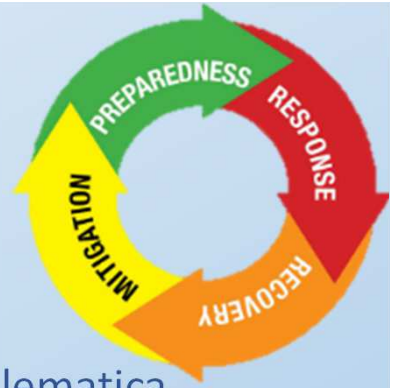
- **Direttiva Etica:**

Descrive in modo semplice e breve i principi morali adottati dalla società.

- **Codice di Condotta:**

In questo documento vengono ribaditi i comportamenti attesi dal personale e le azioni che l'azienda attuerà in caso di comportamenti fraudolenti.

PIANO DI EMERGENZA (CONTINGENCY PLAN)



1. **Preparazione**:
   Preparare un elenco delle misure da adottare per affrontare una problematica
2. **Identificazione:**
   Definire quali sono le aree più critiche, cioè dove o in che occasione dove è più probabile che si verifichi un problema
3. **Causa:**
   Capire quali possano essere le cause che possono originare il problema ed elencarle
4. **Contenimento:**
   Adottare una serie di azioni preventive per rimuovere o ridurre l'eventuale danno
5. **Pianificazione**
   Predisporre un piano per adottare le misure previste o per essere pronti ed avere già le azioni da intraprendere in caso di si debba verificare l'incidente

PIANO DI RECUPERO (DISASTER RECOVERY)

Gli eventi e le conseguenze possono essere così classificati:

Critici:

Applicazioni che non possono essere sostituite con metodi manuali. Il costo di una interruzione è molto alto.

Vitali:

Funzioni che possono essere svolte manualmente per un breve periodo di tempo con notevole impiego di risorse.

Tollerabili:

Funzioni che possono essere svolte manualmente per un lungo periodo di tempo o possono essere riattivate entro un breve intervallo di tempo.

Non-critici

Funzioni che possono rimanere interrotte per un lungo periodo di tempo, con un modesto, o nullo, costo per l'azienda, e lo sforzo per ripristinare il sistema è irrilevante.

GESTIONE DOCUMENTI CARTACEI ED ELETTRONICI

GESTIONE DOCUMENTI CARTACEI ED ELETTRONICI

Nella stesura della procedura devono essere considerati i seguenti capitoli:

- INTEGRITÀ DEI DATI
- CORREZIONI E MODIFICHE
- REVISIONE DEI DATI
- INVALIDAZIONE DEI DATI
- CONSERVAZIONE DEI DATI
- ARCHIVIAZIONE DEI DATI
- BACK-UP DEI DATI

RILASCIO LOTTO – REVISIONE AUDIT TRAIL

- Revisione Audit trail
  - ✓ Accessi (login)
  - ✓ Modifica dei files:
    creazione, cancellazione, spostamento, rinomina,
    eventuali riprocessamenti o ripetizioni
  - ✓ data in cui è stato registrato l'evento
  - ✓ nome dell'autore
  - ✓ Cambiamenti (ed es. di metodo analitico)
  - ✓ Cause del cambiamento

SICUREZZA FISICA E LOGICA
ABILITAZIONE UTENTI

Modalità di accesso ai software

- Gli accessi non possono essere generici, ogni azione deve poter essere attribuita ad un individuo specifico e non ad un ruolo
- Chi crea il dato né chi lo revisiona può avere i diritti di Amministratore
- I tecnici incaricati della manutenzione degli strumenti non devono avere tutti i privilegi di Amministratore: è sufficiente che gli vengano assegnati solo i privilegi specifici per i loro compiti. Bisognerà quindi assegnare loro un profilo a se stante.
- Tutte le modifiche effettuate al sistema dall'Amministratore devono essere visibili dal QA e approvate con la consueta gestione del sistema di qualità in essere

SICUREZZA FISICA E LOGICA
ABILITAZIONE UTENTI

- Responsabilità **QA**:
  - definire e rendere noti le gerarchie e i livelli di accesso degli utenti
  - precisare le abilitazioni dei singoli utenti
  - verificare e approvare l'attribuzione delle abilitazioni
  - predisporre e aggiornare il registro utenti
- Responsabilità **Amministratore** del sistema:
  - determinare i gruppi, attribuire le funzioni ai gruppi
  - abilitare gli utenti alle funzioni stabilite
  - disattivare gli utenti
  - modificare le abilitazioni degli utenti

SICUREZZA FISICA E LOGICA
ABILITAZIONE UTENTI

GESTIONE PASSWORD

- definire le regole di composizione delle password:
- il numero minimo di caratteri e tipologia,
- periodo di validità.

ARCHIVIAZIONE E RIPRISTINO DATI

BACKUP

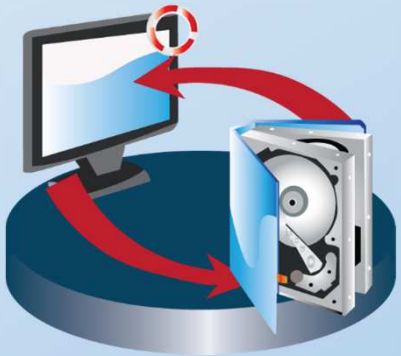
Copia di riserva su supporti di memorizzazione diversi da quello in uso.

- Modalità (manuale o automatico)
- Frequenza
- Supporto
- Quali file ⟸ analisi del rischio
- Tempi di conservazione
- Verifica e ripristino
- Responsabilità – esecuzione, controllo e verifica

ARCHIVIAZIONE E RIPRISTINO DATI

ARCHIVIAZIONE

Salvataggio dei dati in modo permanente e non più editabile



- Modalità (manuale o automatico)
- Frequenza
- Supporto
- Quali file ⟸ analisi del rischio
- Tempi di conservazione
- Responsabilità – esecuzione, cancellazione o smaltimento
- Dove :
  - documenti cartacei archivio o magazzino esterno
  - files informatici: server aziendale o cloud

VERIFICHE PERIODICHE

Verificare che i sistemi in esame siano in grado di funzionare correttamente e che siano stati mantenuti i parametri stabiliti in convalida:

- L'accesso ai sistemi è regolato secondo ruoli e competenze adeguatamente formalizzati
- Le stazioni di lavoro collegate al sistema centrale operano correttamente e la corrispondente documentazione è disponibile e aggiornata
- Le operazioni di salvataggio del sistema sono correttamente documentate ed eseguite
- La configurazione dell'audit trail è la stessa di quella convalidata

VERIFICHE PERIODICHE - CHECK LIST

- È possibile l'accesso di utenti non abilitati
- Esiste aggiornata la lista utenti e quella dei corrispondenti permessi
- È stato fissato un periodo di validità per le credenziali di accesso degli utenti
- È consentita la modifica data e ora
- L'audit trail è accessibile
- L'audit trail riporta gli accessi, le operazioni eseguite, eventuali modifiche e rielaborazioni dei dati
- È consentita la cancellazione dati, in caso affermativo a quale utenti è permessa questa operazione e la cancellazione risulta nell'audit trail
- È definito e funziona il tempo di scollegamento singole unità dopo periodo di inattività
- Esiste una procedura di backup?
- C'è evidenza oggettiva delle operazioni di Backup, conservazione e Restore
- Il training degli utenti è stato eseguito e documentato
- Viene seguita la procedura change control e c'è evidenza nell'audit trail dei change eseguiti
- Sia sul file che sulla copia stampata è presente il nominativo, la data e ora e il significato delle firme elettroniche
- I sistemi sono stati convalidati

CHANGE CONTROL

Ogni modifica ad un sistema computerizzato, incluse le modifiche alla configurazione del sistema, deve essere effettuata solo in modo controllato in accordo a procedure definite.

Tutte le modifiche devono essere approvate dal QA

Deve essere valutata la necessità di una riconvalida parziale o totale del sistema

Migrazione dati

Devono essere previste le azioni da compiere in caso di:

- aggiornamenti di software
- cambi di terminali

Assicurare la possibilità di recuperare i dati precedentemente archiviati.

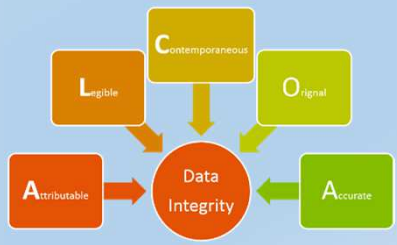
Riconvalida del sistema che preveda controlli per verificare che i dati non siano stati modificati in valore e/o significato durante il processo di migrazione

FORMAZIONE

Il programma di formazione deve prevedere che il personale sia reso consapevole dell'importanza dei principi del data integrity.

Il personale che utilizza i sistemi informatici deve essere formato per rivedere in modo efficiente i dati prodotti, compresi i metadati e gli audit trail

Il personale della QU deve essere formato su come prevenire e rilevare problemi legati all'integrità dei dati, come sovrascritture o cancellazioni, sia intenzionali che inconsapevoli. Il personale coinvolto nella revisione degli audit trail necessita un percorso formativo specifico.



MANUTENZIONE
GESTIONE RETE AZIENDALE

Verificare a scadenze predeterminate i principali componenti del sistema IT allo scopo di prevenire eventuali malfunzionamenti e mantenerne costanti a livelli ottimali le funzionalità.

Definire i test da eseguire e la loro periodicità, le responsabilità per la loro esecuzione.

QUALIFICA FORNITORI
CONTRATTO CON TERZE PARTI

- consulenti,
- fornitori di servizi,
- dipartimenti IT

attività di:

- fornitura,
- installazione,
- configurazione,
- integrazioni,
- validazione,
- mantenimento (anche tramite accesso remoto)

CONTRATTO CON TERZE PARTI
SLA : Service Technical Agreement

Caratteristiche dell'infrastruttura cloud

- GESTIONE ACCESSI
  La connettività al cloud deve essere gestita tramite accessi esclusivi che ne permettano il controllo e la gestione
- SERVER FARM
  Garantire la sorveglianza contro intrusione, incendio e anomalie ambientali.
  La Server Farm deve essere dotata di impianto di terra certificato, gruppi di continuità, e gruppo elettrogeno ad avvio automatico e sistema di diagnostica.
  I locali devono essere condizionati e allarmati

CONTRATTO CON TERZE PARTI
SLA : Service Technical Agreement

Caratteristiche dell'infrastruttura cloud

- BUSINESS CONTINUITY
  Assicurare che eventuali guasti di un componente dell'infrastruttura non abbia impatto oppure al massimo provochi un temporaneo disservizio normalmente gestibile senza alcuna perdita di dati.
  Garantire backup degli applicativi secondo una schedulazione concordata per quanto riguarda i dati e prevedere copia di sicurezza dei backup .
- DISASTER RECOVERY E RIPRISTINO
  Qualora si verifichino problemi di disponibilità del servizio, questi vanno analizzati e categorizzati a seconda della tipologia di impatto sul sistema in produzione:
  Deve essere concordato il tempo massimo che può intercorrere tra la ricezione della chiamata e la presa in carico del problema.

GESTIONE EVENTI DEL SISTEMA – TICKET

- Anomalie (incluse quelle dei sistemi di backup e restore);
- Fermi sistema per motivi diversi dalla manutenzione ordinaria del sistema;
- Altri avvenimenti che impediscono l'operatività normale del sistema.

L'iter del processo deve prevedere i seguenti passi:

1. Segnalazione dell'evento e apertura del ticket da parte dell'utente ;
2. attribuzione del ticket;
3. risoluzione del ticket;
4. chiusura del ticket e comunicazione all'utente

FIRME ELETTRONICHE

- Indicazione della validità della firma elettronica rispetto a quella manuale
- Responsabilità e competenze degli utenti
- Informazioni:
  - Nominativo del firmatario, la data e l'ora dell'apposizione della firma, lo scopo della firma (approvazione, autorizzazione, rilascio).
  - Collegamento al record firmato
  - Impossibilità di cancellazioni, copiature e falsificazioni
  - Presenza della firma sulla versione cartacea
- Verifiche

Rita Brusa
r.brusa@imsmicron.it