Disaster Recovery Plan

Proprietario del documento:	Data creazione:
Approvato da:	Data ultima revisione:

Autorità

Abstract

1 Introduzione

1.1 Obiettivi del Disaster Recovery Plan

Indicazione dei principali obiettivi considerati nella stesura del Disaster Recovery Plan (DRP) e che si desidera perseguire con la sua applicazione.

1.2 Ambito di applicazione

Definizione del campo di competenza del presente piano, individuando i componenti software/hardware, i sistemi e/o le reti a cui si applica ed eventuali contesti.

1.3 Definizioni chiave

2 Predisposizione all'emergenza

2.1 Ruoli e responsabilità

2.1.1 Responsabile della Business Continuity e Disaster Recovery

Indicazione del Responsabile della Business Continuity e Disaster Recovery e dei principali compiti che assolve.

2.1.2 Team di risposta all'emergenza e contatti

Descrizione della composizione del team di risposta, precisando i relativi compiti e indicando eventualmente la gerarchia di autorità, nonché le informazioni di contatto.

2.2 Controlli preventivi

2.2.1 Valutazione del rischio

Identificazione e documentazione delle vulnerabilità delle risorse, determinando il rischio sulla base di minacce, vulnerabilità, probabilità e impatti.

2.2.2 Gestione dell'asset

Indicazione delle politiche di inventario e gestione di dispositivi fisici (quali workstation, server e storage) e di risorse software.

2.2.3 Monitoraggio continuo

Indicazione delle operazioni di rete e dei flussi di dati attesi per utenti e sistemi, descrizione degli strumenti di detenzione e analisi per individuare eventuali obiettivi e metodi di attacco sulla base di dati multipli e soglie definite.

2.2.4 Metodi di backup e memorizzazione off-site

Descrizione della soluzione di backup che si intende adottare, indicando ad esempio metodo e frequenza di backup, posizione dei dati archiviati, frequenza di rotazione dei supporti e metodo per il trasporto dei dati fuori sede.

2.3 Revisione e test del DRP

2.3.1 Test periodici e esercitazioni

Descrizione dei principali strumenti di test e verifica del Disaster Recovery Plan e dei principali aspetti posti sotto esame, come le procedure di notifica, il ripristino del sistema dal backup e l'analisi delle prestazioni del sistema con supporti alternativi.

2.3.2 Test report

Descrizione della documentazione che verrà prodotta e condivisa relativamente agli esiti delle periodiche prove ed esercitazioni.

2.3.3 Aggiornamento periodico del DRP

Indicazione della frequenza di aggiornamento periodico del DRP (almeno annuale) e dei criteri di aggiornamento eccezionale.

2.4 Formazione

Descrizione degli strumenti e della frequenza di formazione del personale coinvolto nella risposta all'emergenza, con particolare attenzione ai seguenti aspetti.

2.4.1 Coordinamento e comunicazione tra team

2.4.2 Processi specifici del team e responsabilità individuali

2.4.3 Procedure di segnalazione

2.5 Registro informatizzato

Descrizione della struttura, della frequenza di aggiornamento e dei mezzi di condivisione del registro informatizzato che deve essere disponibile per le figure preposte delle Aziende e che deve documentare simulazioni/esercitazioni, situazioni critiche o incidenti, audit e verifiche definite dalle Aziende Sanitarie.

2.5.1 Contenuti

2.5.2 Accessibilità

3 Gestione dell'emergenza

3.1 Identificazione dello stato di emergenza

3.1.1 Precursori e indicatori

Individuazione dei principali precursori e indicatori di una situazione di emergenza, nonché le principali sorgenti (quali per esempio software antivirus, software per il controllo dell'integrità dei file, sistemi di monitoraggio di terze parti, avvisi di sicurezza pubblici, log) che si intende considerare.

3.1.2 Criteri e procedura di attivazione

Indicazione dei criteri e delle persone preposte per l'attivazione del Disaster Recovery Plan, nonché le conseguenti azioni iniziali.

3.1.3 Valutazione dell'emergenza e definizione della priorità di ripristino

Definizione dei principali criteri di valutazione dello stato di emergenza e dei possibili livelli di criticità con indicazione della conseguente relativa allocazione delle risorse.

3.1.4 Stima dei tempi di ripristino

Definizione dei Recovery Time Objective (RTO) in relazione ai livelli di criticità e indicazione di eventuali step di recupero parziale dell'operatività.

3.2 Piano di comunicazione crisi

Descrizione delle procedure e dei metodi (manuali o automatici) utilizzati per informare il personale del team di risposta e tutti gli stakeholders interessati durante l'orario lavorativo e non lavorativo.

3.2.1 Soggetti notificati

3.2.2 Strategie di condivisione delle informazioni

3.2.3 Informazioni da trasmettere

3.3 Procedure operative

Definizione completa dei processi tecnici, delle tecniche, delle liste di controllo e dei moduli specifici utilizzati dal team di risposta, individuati sulla base delle policy e delle priorità.

3.3.1 Procedure di contenimento

3.3.2 Procedure di eradicazione

3.3.3 Procedure di ripristino

3.3.4 Checklist e moduli specifici

4 Attività post-emergenza

4.1 Ricostituzione

Indicazione delle azioni da intraprendere per testare e convalidare la capacità e la funzionalità del sistema e le successive operazioni di backup.

4.1.1 Test dei dati e delle funzionalità

4.1.2 Backup e memorizzazione off-site

4.2 Disattivazione del piano

4.2.1 Documentazione dell'evento

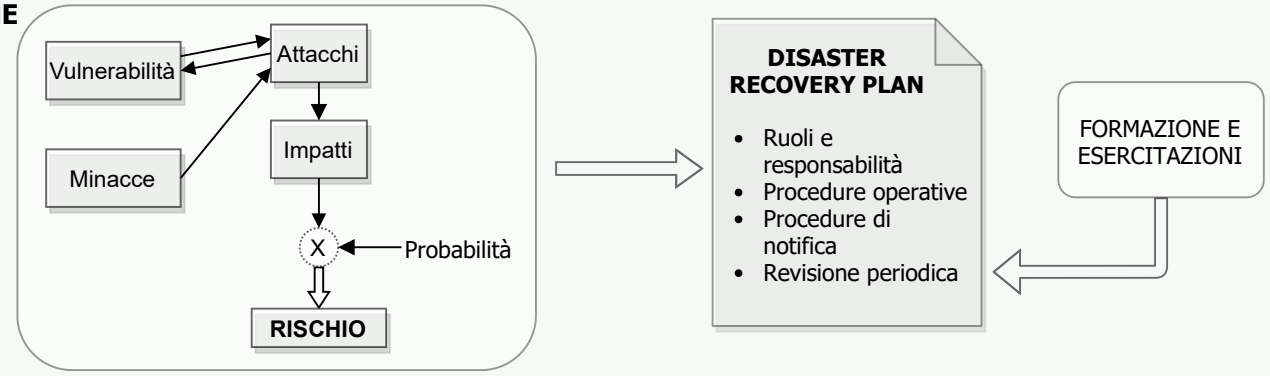
Definizione della documentazione che deve essere sviluppata e aggiornata durante e dopo la fase di emergenza (inclusiva di log delle attività, step di ripristino, eventuali problemi riscontrati e risultati dei test) al fine di permettere valutazioni oggettive e soggettive dell'incidente.

4.2.2 Metriche di valutazione della capacità di risposta ed efficacia

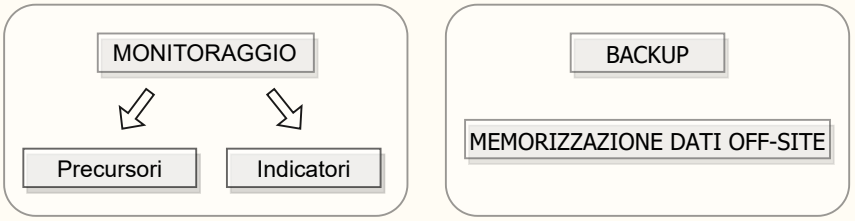
4.3 Aggiornamento del DRP post-emergenza

Indicazione dei criteri di aggiornamento del DRP in seguito alla risoluzione di una situazione di emergenza.

PREPARAZIONE



PREVENZIONE



RISPOSTA