IL WEBINAR INIZIA TRA QUALCHE MINUTO
GRAZIE PER AVER SCELTO DI PARTECIPARE

MASSIMO
CHIRIVÌ

ETHICAL HACKING
LABORATORIO

REDIGERE UN PIANO DI DISASTER RECOVERY

MÜSA
FORMAZIONE E LAVORO

About me

- Consulente e docente ICT dal 1996
- Consulente e docente ICT Security dal 2006
- Senior Trainer MUSA FORMAZIONE dal 2018
- Coordinatore Area IT Musa Formazione
- Lead Auditor Standard ISO 9001-14001-45001-27001-27017-27018
- Vice Presidente nazionale Associazione Italiana Professionisti della Sicurezza Informatica (Capitolo italiano dell'americana ISSA)
- Consulente e formatore di varie realtà nazionali e multinazionali (Multinazionali dell'energia, Industrie, Software House, Banche, Pubbliche Amministrazioni locali e centrali)
- Responsabile IT Security di varie realtà nazionali

Il percorso

1988: il mio primo corso di Linguaggio Basic (avevo 12 anni)

1990: programmavo in Basic sui Commodore 64

1996: nasce la mia prima società informatica che si occupa di sviluppo e sistemistica

2006: l'attività lavorativa inizia a crescere in modo importante nel mondo della security

2011: entro in un grande gruppo IT con quasi 1000 dipendenti

Dal 1988 al 2017: docente per migliaia di utenti

Dal 2018: a bordo di MUSA FORMAZIONE per IT Security

Dal 2018 inizia il percorso ISO

30 anni di vita nel mondo IT

La figura senior che viene ricercata nelle aziende e che può dare valore aggiunto nel percorso di crescita aziendale.

CompTIA Security +

4.2 Summarize the importance of policies, processes, and procedures for incident response.

- **Incident response plans**
- **Incident response process**
  - Preparation
  - Identification
  - Containment
  - Eradication
  - Recovery
  - Lessons learned
- **Exercises**
  - Tabletop
  - Walkthroughs
  - Simulations
- **Attack frameworks**
  - MITRE ATT&CK
  - The Diamond Model of Intrusion Analysis
  - Cyber Kill Chain
- **Stakeholder management**
- **Communication plan**
- **Disaster recovery plan**
- **Business continuity plan**
- **Continuity of operations planning (COOP)**
- **Incident response team**
- **Retention policies**

Alcuni concetti preliminari

- Disaster recovery: si intende l'insieme delle misure tecnologiche e logistico/organizzative atte a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi di business per imprese, associazioni o enti, a fronte di gravi emergenze che ne intacchino la regolare attività.
- Il Disaster Recovery Plan (DRP) è il documento che esplicita tali misure, compreso all'interno del più ampio piano di continuità operativa (BCP).

L’importanza della classificazione

- Disastri naturali
- Disastri manmade

L’importanza della classificazione

Bisogna stabilire il livello di gravità dell’eventuale disastro in base agli asset coinvolti

Dichiarazione d'intenti sulla tecnologia dell'informazione

Questo documento delinea le nostre politiche e procedure per il disaster recovery tecnologico, nonché i nostri piani a livello di processo per il ripristino delle piattaforme tecnologiche critiche e dell'infrastruttura di telecomunicazione. Questo documento riassume le nostre procedure consigliate. Nell'eventualità di una situazione di emergenza reale, possono essere apportate modifiche al presente documento per garantire la sicurezza fisica del nostro personale, dei nostri sistemi e dei nostri dati.

La nostra missione è garantire l'operatività del sistema informativo, l'integrità e la disponibilità dei dati e la continuità aziendale.

Dichiarazione politica

La direzione aziendale ha approvato la seguente dichiarazione di politica:

• L'azienda deve sviluppare un piano completo di disaster recovery IT.

• Per determinare i requisiti del piano di ripristino in caso di catastrofe, deve essere effettuata una valutazione formale dei rischi.

• Il piano di disaster recovery deve coprire tutti gli elementi infrastrutturali, i sistemi e le reti essenziali e critici, in base alle attività aziendali chiave.

• Il piano di disaster recovery deve essere testato periodicamente in un ambiente simulato per garantire che possa essere attuato in situazioni di emergenza e che la direzione e il personale capiscano come deve essere eseguito.

• Tutto il personale deve essere messo al corrente del piano di ripristino in caso di disastro e dei rispettivi ruoli.

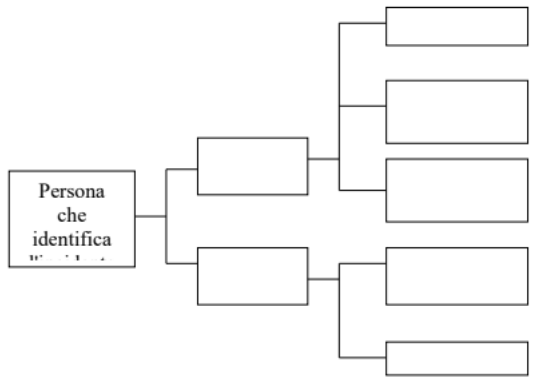
• Il piano di ripristino in caso di disastro deve essere aggiornato per tenere conto dell'evoluzione delle circostanze.

Obiettivi

L'obiettivo principale del programma di disaster recovery è quello di sviluppare, testare e documentare un piano ben strutturato e facilmente comprensibile che aiuti l'azienda a riprendersi nel modo più rapido ed efficace possibile da un disastro imprevisto o da un'emergenza che interrompa i sistemi informativi e le operazioni aziendali.

Ulteriori obiettivi sono i seguenti:

- La necessità di garantire che tutti i dipendenti comprendano appieno i loro doveri nell'attuazione di tale piano.
- La necessità di garantire il rispetto delle politiche operative nell'ambito di tutte le attività pianificate.
- La necessità di garantire che i dispositivi di emergenza proposti siano efficaci dal punto di vista dei costi.
- La necessità di considerare le implicazioni su altri siti aziendali
- Capacità di disaster recovery applicabili ai clienti chiave, ai fornitori e ad altri soggetti.



Informazioni di contatto sul personale chiave

Nome, titolo	Opzione di contatto	Numero di contatto
	Lavoro	
	Alternanza	
	Mobile	
	Casa	
	Indirizzo e-mail	
	Email alternativa	
	Lavoro	
	Alternanza	
	Mobile	
	Casa	
	Indirizzo e-mail	
	Email alternativa	
	Lavoro	
	Alternanza	
	Mobile	
	Casa	
	Indirizzo e-mail	
	Email alternativa	
	Lavoro	
	Alternanza	
	Mobile	
	Casa	
	Indirizzo e-mail	
	Email alternativa	
	Lavoro	
	Alternanza	
	Mobile	
	Casa	
	Indirizzo e-mail	
	Email alternativa	
	Lavoro	
	Alternanza	
	Mobile	
	Casa	
	Indirizzo e-mail	
	Email alternativa	

Albero delle chiamate di notifica

Lo stesso lavoro per i contatti esterni:

Energia
Acqua
Telecomunicazioni
Azienda hardware
Azienda software
Climatizzazione
Ecc.

Aggiornamento del piano

È necessario che il processo di aggiornamento del DRP sia adeguatamente strutturato e controllato. Ogni volta che vengono apportate modifiche al piano, queste devono essere completamente testate e devono essere apportate le opportune modifiche al materiale di formazione. Ciò comporterà l'utilizzo di procedure di controllo delle modifiche formalizzate sotto il controllo del Direttore IT.

Archiviazione della documentazione del piano

Le copie di questo piano, il CD e le copie cartacee saranno conservate in luoghi sicuri definiti dall'azienda. Ogni membro dell'alta direzione riceverà un CD e una copia cartacea del presente piano da archiviare a casa. Ogni membro del Disaster Recovery Team e del Business Recovery Team riceverà un CD e una copia cartacea del piano.
Una copia master protetta sarà archiviata su risorse specifiche stabilite a questo scopo.

Individuazione degli ASSET e stabilire RTO e RPO ogni asset

Tabella:

- **ASSET (Descrizione dettagliata)**
- **RPO**
- **RTO**

TOP TOPICS! Tutto si baserà su questo!

Il **Recovery Time Objective** (**RTO**) è il tempo necessario per il pieno recupero dell'operatività di un sistema o di un processo organizzativo in un sistema di analisi *Business Critical System* (ad esempio implementazioni di politiche di *Disaster recovery* nei Sistemi Informativi).

È in pratica la massima durata, prevista o tollerata, del *downtime* occorso. Nel calcolo del RTO deve essere compreso anche il tempo, successivo all'esecuzione del recupero-mediante il job di backup prescelto-di verifica di idoneità del sistema/informazione ripristinati: in pratica, l'utente o il servizio devono accedere al recuperato prontamente e pienamente, senza altre attese o buchi.
Aspetto di primaria importanza riveste il fatto che il valore di RTO sia definito, conosciuto e verificato, tenendo presente che se un *downtime* lungo danneggia la possibilità di fruire del servizio più di uno breve, il danno maggiore deriva dall'inconsapevolezza di quanto possa essere il tempo previsto per il ripristino dei servizi danneggiati.

Il **Recovery Point Objective** (**RPO**) è uno dei parametri usati nell'ambito delle politiche di disaster recovery per descrivere la tolleranza ai guasti di un sistema informatico. Esso rappresenta la quantità di dati prodotti ma non ancora sincronizzati, in caso di incidente o disastro, su un archivio (storage o file) di sicurezza. Indica quindi il massimo tempo che deve intercorrere tra la generazione di un'informazione e la sua *messa in sicurezza* (ad esempio attraverso backup) e, conseguentemente, fornisce la misura della massima quantità di dati che il sistema potrebbe perdere a causa di guasto improvviso.
In informatica, la quantità di informazioni archiviate, da sottoporre a copia di sicurezza o da recuperare, è tipicamente espressa in unità di tempo: secondi, minuti, ore o giorni di produzione di dati (indipendentemente dal *volume* di dati espresso in byte). In alcuni casi l'RPO si riferisce esplicitamente al dato contenuto nella RAM o nella cache temporanea: in pratica quello elaborato ma non ancora copiato su alcun archivio. Se non specificato, per archivio di sincronizzazione s'intende quello di backup rispetto a quello principale predefinito (pertanto l'RPO si riferisce all'incidente occorso al sistema di archiviazione principale, quello immediatamente connesso alla produzione delle informazioni).
Al diminuire dell'RPO desiderato/specificato si rendono necessarie politiche di sicurezza sempre più stringenti e dispendiose, che possono andare dal salvataggio dei dati su supporti ridondanti tolleranti ai guasti fino alla loro pressoché immediata replicazione su un sistema informatico secondario d'emergenza (soluzione in grado di garantire, in linea teorica, valori di RPO prossimi allo zero).

Definizioni Wikipedia

Strategia di backup

Di seguito sono elencati i principali processi aziendali e la strategia di backup concordata per ciascuno di essi. La strategia scelta è quella di un sito di ripristino completamente specchiato presso gli uffici dell'azienda, all'indirizzo _____. Questa strategia prevede il mantenimento di un sito duplicato completamente specchiato che consentirà il passaggio
istantaneo tra il sito attivo (sede centrale) e il sito di backup.

PROCESSO AZIENDALE CHIAVE	STRATEGIA DI BACKUP
Operazioni IT	Sito di ripristino completamente specchiato
Assistenza tecnica - Hardware	Sito di ripristino completamente specchiato
Assistenza tecnica - Software	Sito di ripristino completamente specchiato
Gestione delle strutture	Sito di ripristino completamente specchiato
Email	Sito di ripristino completamente specchiato
Acquisto	Sito di ripristino completamente specchiato
Recupero dai disastri	Sito di ripristino completamente specchiato
Finanza	Sito di ripristino completamente specchiato
Amministrazione dei contratti	Sito di ripristino completamente specchiato
Magazzino e inventario	Sito di ripristino completamente specchiato
Vendite di prodotti	Sito di ripristino completamente specchiato
Vendite di manutenzione	Sito di ripristino completamente specchiato
Risorse umane	Struttura di archiviazione dei dati fuori sede
Test del sito di ripristino con mirroring completo	Sito di ripristino completamente specchiato
Officina Sito di ripristino completamente specchiato -	Sito di ripristino completamente specchiato
Call Center	Sito di ripristino completamente specchiato
Sito web	Sito di ripristino completamente specchiato

Gestione del rischio

Esistono molte potenziali minacce di disturbo che possono verificarsi in qualsiasi momento e influenzare il normale processo aziendale. Abbiamo preso in considerazione un'ampia gamma di potenziali minacce e i risultati delle nostre deliberazioni sono inclusi in questa sezione. Ogni potenziale disastro ambientale o situazione di emergenza è stata esaminata. L'attenzione si concentra sul livello di interruzione dell'attività che potrebbe derivare da ciascun tipo di disastro.

- Un potenziale disastro
- Valutazione della probabilità
- Valutazione dell'impatto
- Breve descrizione delle conseguenze potenziali e delle azioni correttive

Risposta alle emergenze
Allarme, escalation e invocazione del piano
Pianificare gli eventi scatenanti

I fattori chiave che determinano l'attivazione del DRP presso la sede centrale sono ad esempio i seguenti:

- Perdita totale di tutte le comunicazioni
- Perdita totale di potenza
- Allagamento dei locali
- Perdita dell'edificio

Punti di ritrovo

Nel caso in cui sia necessario evacuare i locali, il piano di invocazione del DRP individua due punti di raccolta per l'evacuazione:

- Primaria - All'estremità del parcheggio principale;
- In alternativa, il parcheggio dell'azienda di fronte.

Attivazione della squadra di pronto intervento

Quando si verifica un incidente, deve essere attivato il Team di risposta alle emergenze (ERT). L'ERT deciderà in che misura invocare il DRP. A tutti i dipendenti deve essere consegnata una scheda di riferimento rapido contenente i dati di contatto dell'ERT da utilizzare in caso di disastro. Le responsabilità dell'ERT sono:

- Rispondere immediatamente a un potenziale disastro e chiamare i servizi di emergenza;
- Valutare l'entità del disastro e il suo impatto sull'azienda, sul centro dati, ecc;
- Decidere quali elementi del piano di DR devono essere attivati;
- Stabilire e gestire un team di ripristino in caso di disastro per mantenere i servizi vitali e ripristinare il normale funzionamento;
- Assicurarsi che i dipendenti siano informati e assegnare responsabilità e attività come richiesto.

Team per il ripristino d'emergenza

La squadra sarà contattata e riunita dall'ERT.

Le responsabilità della squadra comprendono:

- Stabilire strutture per un livello di servizio di emergenza entro 2 ore lavorative;
- Ripristinare i servizi chiave entro 4 ore lavorative dall'incidente;
- Ripristinare l'operatività ordinaria entro 8.0-24.0 ore dall'incidente;
- Coordinare le attività con il team di ripristino in caso di disastro, i primi soccorritori, ecc.
- Fare rapporto alla squadra di pronto intervento.

Allarme di emergenza, escalation e attivazione DRP

Questa politica e procedura è stata stabilita per garantire che, in caso di disastro o crisi, il personale abbia una chiara comprensione di chi deve essere contattato. Le procedure sono state elaborate per garantire che le comunicazioni possano essere stabilite rapidamente durante l'attivazione del ripristino in caso di disastro. Il piano di DR si avvarrà principalmente di membri chiave del management e del personale che forniranno le competenze tecniche e gestionali necessarie per ottenere un ripristino tecnologico e aziendale senza problemi. I fornitori di beni e servizi critici continueranno a supportare la ripresa delle operazioni commerciali man mano che l'azienda tornerà alla normale modalità operativa.

Allarme di emergenza

La persona che scopre l'incidente chiama un membro della Squadra di pronto intervento nell'ordine elencato:

Squadra di pronto intervento

- _____
- _____
- _____

Se non è disponibile, provare:

- _____
- _____

Il Team di risposta alle emergenze (ERT) è responsabile dell'attivazione del DRP per i disastri identificati nel presente piano, nonché in caso di qualsiasi altro evento che comprometta la capacità dell'azienda di operare normalmente.

Uno dei compiti nelle prime fasi dell'emergenza è quello di notificare al Disaster Recovery Team (DRT) che si è verificata un'emergenza. La notifica richiederà ai membri del DRT di riunirsi sul luogo del problema e conterrà informazioni sufficienti per comunicare efficacemente questa richiesta. Il Business Recovery Team (BRT) sarà composto da rappresentanti senior dei principali dipartimenti aziendali. Il leader del BRT sarà un membro senior del team di gestione dell'azienda e avrà la responsabilità di assumere la direzione generale del processo e di garantire che l'azienda ritorni alla normale operatività il prima possibile.

Procedure di DR per la gestione

I membri del team di gestione conserveranno una copia cartacea dei nomi e dei numeri di contatto di tutti i dipendenti dei loro dipartimenti. Inoltre, i membri del team di gestione terranno in casa una copia cartacea dei piani di ripristino in caso di disastro e di continuità operativa dell'azienda, nel caso in cui l'edificio della sede centrale sia inaccessibile, inutilizzabile o distrutto.

Contatto con i dipendenti

I dirigenti fungeranno da punti di riferimento per i loro reparti, mentre i dipendenti designati chiameranno gli altri dipendenti per discutere della crisi/del disastro e dei piani immediati dell'azienda. I dipendenti che non riescono a raggiungere il personale presente nella loro lista di chiamata sono invitati a chiamare il contatto di emergenza del membro del personale per trasmettere le informazioni sul disastro.

Personale di riserva

Se un dirigente o un membro del personale designato a contattare altri membri del personale non è disponibile o è incapace, il membro del personale di riserva designato svolgerà le funzioni di notifica.

Messaggi registrati/aggiornamenti

Per avere informazioni aggiornate sul disastro e sulla risposta dell'organizzazione, i membri del personale possono chiamare un numero verde indicato nella scheda DRP. I messaggi contengono informazioni sulla natura del disastro, sui siti di raccolta e aggiornamenti sulla ripresa del lavoro.

Strutture di ripristino alternative / Hot Site

Se necessario, verrà attivato il sito caldo presso XXX e la notifica verrà data tramite messaggi registrati o comunicazioni con i manager. Il personale del sito caldo sarà composto da membri del team di ripristino in caso di disastro solo per le prime 24 ore, mentre altri membri del personale si uniranno al sito caldo secondo le necessità.

Notifica al personale e alle famiglie

Se l'incidente ha provocato una situazione che potrebbe preoccupare i familiari più stretti di un dipendente, come il ricovero in ospedale di persone ferite, sarà necessario informare rapidamente i familiari più stretti.

Media

Contatto con i media

Il personale incaricato si coordinerà con i media, lavorando secondo le linee guida precedentemente approvate ed emesse per la gestione delle comunicazioni post-catastrofe.

Strategie dei media

1. Evitare la pubblicità negativa
2. Sfruttare le opportunità di pubblicità utile
3. Rispondere alle seguenti domande di base:
    - Che cosa è successo?
    - Come è successo?
    - Che cosa intende fare?

3. Media Team

- _____specificare i responsabili_____
- _____
- _____

Regole per i rapporti con i media

Solo il team media può entrare in contatto diretto con i media; chiunque altro venga contattato deve indirizzare i chiamanti o i rappresentanti dei media di persona al team media.

Assicurazioni

Nell'ambito delle strategie di disaster recovery e continuità operativa dell'azienda, sono state stipulate diverse polizze assicurative. Tra queste figurano le assicurazioni contro errori e omissioni, responsabilità civile degli amministratori e dei dirigenti, responsabilità civile generale e interruzione dell'attività.
Se è necessaria un'assistenza assicurativa a seguito di un'emergenza al di fuori del normale orario di lavoro, si prega di contattare:

_____

- Nome della politica
- Tipo di copertura
- Periodo di copertura
- Importo della copertura
- Persona responsabile per la copertura
- Prossimo rinnovo data

Assicurazioni

Nell'ambito delle strategie di disaster recovery e continuità operativa dell'azienda, sono state stipulate diverse polizze assicurative. Tra queste figurano le assicurazioni contro errori e omissioni, responsabilità civile degli amministratori e dei dirigenti, responsabilità civile generale e interruzione dell'attività.
Se è necessaria un'assistenza assicurativa a seguito di un'emergenza al di fuori del normale orario di lavoro, si prega di contattare:

_____

- Nome della politica
- Tipo di copertura
- Periodo di copertura
- Importo della copertura
- Persona responsabile per la copertura
- Prossimo rinnovo data

Questioni finanziarie e legali

Valutazione finanziaria

La squadra di pronto intervento deve preparare una valutazione iniziale dell'impatto dell'incidente sugli affari finanziari dell'azienda. La valutazione deve includere:

- Perdita di documenti finanziari
- Perdita di entrate
- Furto di libretti di assegni, carte di credito, ecc.
- Perdita di liquidità

Requisiti finanziari

Le esigenze finanziarie immediate dell'azienda devono essere affrontate. Queste possono includere:

- Posizione del flusso di cassa
- Capacità di prestito temporaneo
- Pagamenti imminenti per tasse, imposte sui salari, previdenza sociale, ecc.
- Disponibilità di carte di credito aziendali per pagare le forniture e i servizi necessari dopo la catastrofe.

Azioni legali

L'ufficio legale dell'azienda e l'ERT esamineranno congiuntamente le conseguenze dell'incidente e decideranno se ci possono essere azioni legali derivanti dall'evento; in particolare, la possibilità di richieste di risarcimento da parte o contro l'azienda per violazioni normative, ecc.

Esercizio DRP

Le esercitazioni del piano di disaster recovery sono una parte essenziale del processo di sviluppo del piano. In un'esercitazione del DRP nessuno viene promosso o bocciato; tutti coloro che partecipano imparano dalle esercitazioni: cosa deve essere migliorato e come può essere implementato. L'esercitazione del piano assicura che le squadre di emergenza abbiano familiarità con i loro compiti e, cosa più importante, siano fiduciose nelle loro capacità.

I piani di DR di successo entrano in azione in modo fluido ed efficace quando sono necessari. Ciò avverrà solo se tutti coloro che hanno un ruolo da svolgere nel piano hanno provato il ruolo una o più volte. Il piano deve essere convalidato anche simulando le circostanze in cui deve funzionare e vedendo cosa succede.

Piano di ripristino di emergenza per <Sistema Uno>

SISTEMA	

PANORAMICA	
SERVER DI PRODUZIONE	Posizione: Modello di server: Sistema operativo: CPU: Memoria: Disco totale: Maniglia del sistema: Numero di serie del sistema: Voce DNS: Indirizzo IP: Altro:
SERVER DEL SITO CALDO	Fornisci i dettagli
APPLICAZIONI (Usare il grassetto per il sito caldo)	
SERVER ASSOCIATI	

CONTATTI CHIAVE	
Fornitore di hardware	Fornisci i dettagli
Proprietari del sistema	Fornisci i dettagli
Proprietario del database	Fornisci i dettagli
Proprietari dell'applicazione	Fornisci i dettagli
Fornitori di software	Fornisci i dettagli
Stoccaggio fuori sede	Fornisci i dettagli

STRATEGIA DI BACKUP PER IL SISTEMA UNO	
Giornaliero	Fornisci i dettagli
Mensile	Fornisci i dettagli
Trimestrale	Fornisci i dettagli

SISTEMA UNO PROCEDURA DI RIPRISTINO IN CASO DI DISASTRO	
Scenario 1 Perdita totale dei dati	Fornisci i dettagli
Scenario 2 Perdita totale di HW	Fornisci i dettagli

CONTATTI	

Sistemi di file <data>

File System a partire da <data> File system minimi da creare e ripristinare dal backup: <Elenco>	Filesystem kbyte Usato Disponibile %usato Montato su <Fornisci i dettagli>.
Altri file critici da modificare	<Fornisci i dettagli>.
Le directory necessarie per la creazione	<Fornisci i dettagli>.
File critici da ripristinare	<Fornisci i dettagli>.
File secondari da ripristinare	<Fornisci i dettagli>.
Altri file da ripristinare	<Fornisci i dettagli>.

Modulo di valutazione dei danni

Attività chiave Processo interessato	Descrizione del problema	Entità del danno

Modulo per la gestione delle attività di DR

• Durante il processo di ripristino in caso di disastro, tutte le attività saranno determinate utilizzando una struttura standard;
• Ove possibile, questo piano dovrà essere aggiornato regolarmente durante il periodo di ripristino in caso di disastro;
• Tutte le azioni che si verificano durante questa fase devono essere registrate.

Nome dell'attività:
Numero di riferimento:
Breve descrizione:

Inizio Data/Ora	Completamento Data/Ora	Risorse coinvolte	In carica

Modulo di registrazione dell'evento di disaster recovery

• Tutti gli eventi chiave che si verificano durante la fase di disaster recovery devono essere registrati.
• Il responsabile del team di disaster recovery deve tenere un registro degli eventi.
• Questo registro degli eventi deve essere avviato all'inizio dell'emergenza e una copia del registro deve essere trasmessa al team di ripristino aziendale una volta controllati i pericoli iniziali.
• Il seguente registro degli eventi deve essere compilato dal responsabile del team di ripristino d'emergenza per registrare tutti gli eventi chiave durante il ripristino d'emergenza, fino al momento in cui la responsabilità passa al team di ripristino aziendale.

Descrizione del disastro:
Data di inizio:
Data/Ora di mobilitazione della squadra DR:

Attività svolte dal team DR	Data e ora	Risultato	Azione successiva richiesta

Lavoro del team di disaster recovery completato: <Data>.
Registro eventi trasmesso al team di ripristino aziendale: <Data>.

Modulo di segnalazione dell'attività di ripristino in caso di calamità

• Al termine dell'intervento iniziale di ripristino in caso di catastrofe, il leader del DRT deve preparare una relazione sulle attività svolte.
• Il rapporto deve contenere informazioni sull'emergenza, su chi è stato avvisato e quando, sulle azioni intraprese dai membri del DRT e sui risultati di tali azioni.
• Il rapporto conterrà anche una valutazione dell'impatto sulle normali operazioni aziendali.
• Il rapporto deve essere consegnato al responsabile del team di ripristino dell'attività, con una copia all'alta direzione, a seconda dei casi.
• Il leader del DRT preparerà un rapporto sul ripristino in caso di disastro al termine dell'intervento iniziale.

• Oltre al responsabile del team di recupero aziendale, il rapporto sarà distribuito all'alta direzione.

Il rapporto comprenderà:
• Descrizione dell'emergenza o dell'incidente
• Persone informate dell'emergenza (comprese le date)
• Azioni intraprese dai membri del DRT
• Risultati derivanti dalle azioni intraprese
• Una valutazione dell'impatto sulle normali operazioni commerciali
• Valutazione dell'efficacia del BCP e delle lezioni apprese
• Lezioni apprese

Mobilitazione della squadra di ripristino in caso di disastro

• In caso di emergenza che richieda il ripristino delle risorse dell'infrastruttura tecnologica, il team di disaster recovery deve essere informato della situazione e messo in standby.
• Il formato mostrato di seguito può essere utilizzato per registrare l'attivazione del team DR una volta completato il lavoro delle squadre di valutazione dei danni e di risposta all'emergenza.

Descrizione dell'emergenza:
Data di accadimento:
Data di completamento del lavoro del team di disaster recovery:

Nome del membro del team	Dettagli di contatto	Contattato il (ora/data)	Da chi	Risposta	Data di inizio richiesta
Commenti pertinenti (ad esempio, istruzioni specifiche emesse)					

Mobilitazione del team di recupero aziendale (BUSINESS RECOVERY)

- In caso di emergenza che richieda l'attivazione del team di disaster recovery, il team di business recovery deve essere informato della situazione e messo in standby.
- Il formato riportato di seguito verrà utilizzato per registrare l'attivazione del team di ripristino aziendale una volta completato il lavoro del team di ripristino in caso di disastro.

Descrizione dell'emergenza:
Data di accadimento:
Data di completamento del lavoro del team di disaster recovery:

Nome del membro del team	Dettagli di contatto	Contattato il (ora/data)	Da chi	Risposta	Data di inizio richiesta
Commenti pertinenti (ad esempio, istruzioni specifiche emesse)					

Monitoraggio dell'avanzamento delle attività di ripristino aziendale

• In questo periodo è necessario monitorare attentamente l'avanzamento delle attività di recupero tecnologico e aziendale.
• Poiché le difficoltà incontrate da un gruppo potrebbero influire in modo significativo su altri compiti dipendenti, è importante assicurarsi che ogni compito sia dotato di risorse adeguate e che non siano stati sottovalutati gli sforzi necessari per ripristinare le normali operazioni aziendali.

Nota: è necessario individuare una sequenza prioritaria, anche se, ove possibile, le attività saranno svolte contemporaneamente.

Attività di recupero (*Ordine di priorità*)	Persona/e responsabile/i	Data di completamento		Pietre miliari identificate	Altre informazioni rilevanti
		Stimato	Effettivo		
1.					
2.					
3.					
4.					
5.					
6.					
7.					

Al termine delle attività di business recovery, il leader del BRT deve preparare una relazione sulle attività intraprese e completate.

• Il rapporto deve contenere informazioni sull'evento di disturbo, su chi è stato informato e quando, sulle azioni intraprese dai membri del BRT e sui risultati di tali azioni.
• Il rapporto conterrà anche una valutazione dell'impatto sulle normali operazioni commerciali.
• Il rapporto deve essere distribuito al senior management, come appropriato.

Il contenuto del rapporto deve comprendere:
• Descrizione dell'incidente
• Persone informate dell'emergenza (comprese le date)
• Azioni intraprese dal team di recupero aziendale
• Risultati derivanti dalle azioni intraprese
• Una valutazione dell'impatto sulle normali operazioni commerciali
• Problemi identificati
• Suggerimenti per migliorare il piano di disaster recovery e/o di continuità operativa.
• Lezioni apprese

Modulo per le comunicazioni

• È molto importante che durante le attività di recupero e ripristino dell'attività aziendale siano tenute adeguatamente informate tutte le persone e le organizzazioni colpite.
• Le informazioni fornite a tutte le parti devono essere accurate e tempestive.
• In particolare, qualsiasi stima dei tempi di ritorno alle normali attività lavorative deve essere annunciata con cautela.
• È inoltre molto importante che solo il personale autorizzato si occupi delle query multimediali.

Gruppi di persone o organizzazioni colpite dall'interruzione	Persone selezionate per coordinare le comunicazioni alle persone/organizzazioni interessate		
	Nome	Posizione	Dettagli di contatto
I clienti			
Direzione e personale			
Fornitori			
Media			
Gli stakeholder			
Altri			

Restituzione delle operazioni aziendali recuperate alla leadership della business unit

• Una volta ripristinate le normali operazioni aziendali, sarà necessario restituire la responsabilità di operazioni specifiche al responsabile dell'unità aziendale appropriata.
• Questo processo deve essere formalizzato per garantire che tutte le parti comprendano il cambiamento di responsabilità generale e la transizione al business-as-usual.
• È probabile che durante il processo di recupero la responsabilità generale sia stata assegnata al responsabile del processo di recupero aziendale.
• Si presume che la direzione dell'unità aziendale sia pienamente coinvolta durante il recupero, ma affinché il processo di recupero sia pienamente efficace, la responsabilità generale durante il periodo di recupero dovrebbe probabilmente essere affidata a un team di processo di recupero aziendale.

Modulo di completamento del recupero di processi/funzioni

Il seguente modulo di transizione deve essere compilato e firmato dal responsabile del team di recupero aziendale e dal responsabile dell'unità aziendale responsabile, per ogni processo recuperato.
Per ogni processo aziendale recuperato deve essere utilizzato un modulo separato.

Nome del processo aziendale	
Data di completamento del lavoro fornito dal team di recupero aziendale	
Data di ritorno alla gestione della Business Unit *(se diversa dalla data di completamento)*	

Confermo che il lavoro del team di ripristino aziendale è stato completato in conformità al piano di ripristino in caso di disastro per il processo di cui sopra e che le normali operazioni aziendali sono state effettivamente ripristinate.

Nome del Team Leader del Business Recovery:
_____

Firma: _____

Data: _____

(Qui vanno inseriti tutti i commenti pertinenti del leader BRT in relazione alla restituzione di questo processo aziendale).

Confermo che il processo aziendale di cui sopra è ora accettabile per le normali condizioni di lavoro.

Nome: _____

Titolo: _____

Firma: _____

Data: _____