Pianificazione del disaster recovery plan

Guida operativa commentata per la gestione dei disastri
e per la continuità operativa

Versione: 1.0 – Estesa
Ambito: Risk Management & Cybersecurity
Destinatari: Direzione, IT, Sicurezza, Compliance
Documento: Versione online

Quando si verifica un disastro, l'azienda ne subisce le conseguenze. Un obiettivo della pianificazione aziendale è quello di mitigare l'interruzione della fornitura di prodotti e servizi al massimo grado possibile quando si verifica un'interruzione dovuta a un disastro. La continuità aziendale è la preoccupazione primaria.

Un piano di disaster recovery IT è il cardine di una strategia complessiva di continuità aziendale. Lo scopo della continuità aziendale è mantenere un livello minimo di servizio durante il ripristino dell'organizzazione alla normale operatività. Se un'azienda non riesce a predisporre un piano di disaster recovery, quando si verifica un disastro, rischia di:

- Perdere clienti a favore dei concorrenti
- Perdere finanziamenti
- Vedere rivalutata e ritenuta non necessaria l'esigenza dei suoi prodotti o servizi

Dognet Technologies incoraggia ogni organizzazione a implementare proattivamente un piano di Disaster Recovery IT. Per assistere in questo processo, forniamo un modello come punto di partenza per il piano personalizzato della vostra organizzazione. Vi preghiamo di contattare un rappresentante Dognet Technologies quando siete pronti!

Cronologia delle Revisioni del Piano di Disaster Recovery IT

REVISIONE	DATA	NOME	DESCRIZIONE

Indice generale

Dichiarazione di Intenti sulla Tecnologia dell'Informazione

Questo documento delinea le nostre politiche e procedure per il disaster recovery tecnologico, così come i nostri piani a livello di processo per il recupero delle piattaforme tecnologiche critiche e dell'infrastruttura di telecomunicazioni. Questo documento riassume le nostre procedure raccomandate. In caso di effettiva emergenza, potrebbero essere apportate modifiche a questo documento per garantire la sicurezza fisica delle nostre persone, dei nostri sistemi e dei nostri dati.

La nostra missione è garantire:

- Il tempo di attività dei sistemi informativi
- L'integrità e la disponibilità dei dati
- La continuità aziendale

Dichiarazione di Policy

La direzione aziendale ha approvato la seguente dichiarazione di policy:

- L'azienda svilupperà un piano completo di disaster recovery IT
- Sarà intrapresa una valutazione formale dei rischi per determinare i requisiti del piano di disaster recovery
- Il piano di disaster recovery dovrà coprire tutti gli elementi essenziali e critici dell'infrastruttura, i sistemi e le reti, in accordo con le attività chiave del business
- Il piano di disaster recovery dovrà essere periodicamente testato in un ambiente simulato per assicurare che possa essere implementato in situazioni di emergenza e che la direzione e il personale comprendano come deve essere eseguito
- Tutto il personale deve essere reso consapevole del piano di disaster recovery e dei propri rispettivi ruoli
- Il piano di disaster recovery deve essere mantenuto aggiornato per tenere conto delle circostanze mutevoli

Obiettivi

L'obiettivo principale del programma di disaster recovery è sviluppare, testare e documentare un piano ben strutturato e facilmente comprensibile che aiuterà l'azienda a riprendersi il più rapidamente ed efficacemente possibile da un disastro o emergenza imprevista che interrompe i sistemi informativi e le operazioni aziendali.

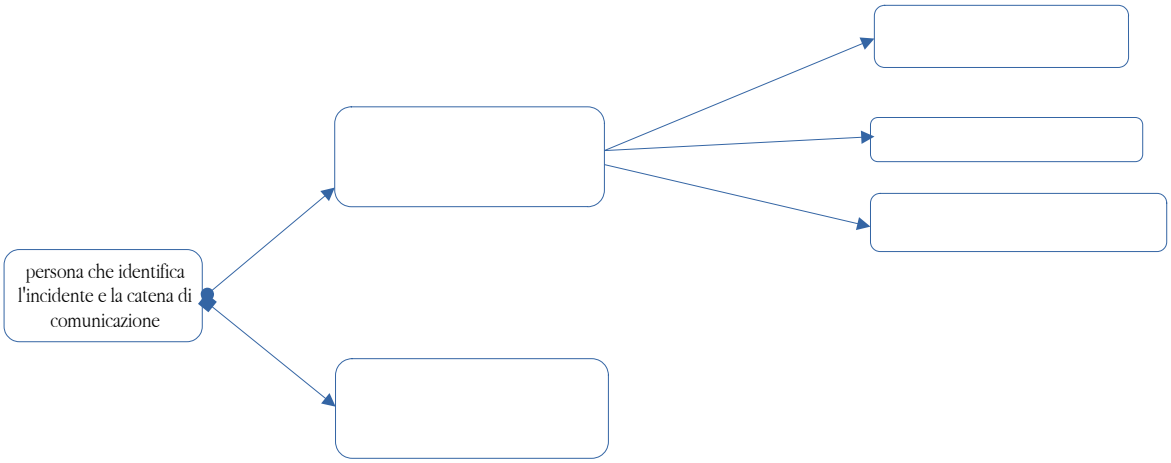
Gli obiettivi aggiuntivi includono:

- Assicurare che tutti i dipendenti comprendano pienamente i loro doveri nell'implementazione del piano
- Assicurare che le politiche operative siano rispettate in tutte le attività pianificate
- Assicurare che le disposizioni di contingenza proposte siano economicamente efficaci
- Considerare le implicazioni su altri siti aziendali
- Capacità di disaster recovery applicabili a clienti chiave, fornitori e altri

Informazioni di Contatto del Personale Chiave

NOME, TITOLO	OPZIONE DI CONTATTO	NUMERO DI CONTATTO
[Spazio per inserimento]	Lavoro	
	Alternativo	
	Mobile	
	Casa	
	Email	
	Email Alternativa	

Albero delle Chiamate di Notifica



Contatti Esterni

NOME, TITOLO	OPZIONE DI CONTATTO	NUMERO DI CONTATTO
Proprietario/Property Manager	Numero Account: Nessuno	Lavoro
	Mobile	
	Casa	
	Email	
Compagnia Elettrica		
Numero Account	Lavoro	
	Mobile	
	Casa	
	Email	
Operatore Telecom 1		
Numero Account		
	Lavoro	
	Mobile	
	Fax	
	Casa	
	Email	

1. Panoramica del Piano

1.1 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 dovrebbero essere apportate appropriate modifiche ai materiali di formazione. Questo comporterà l'uso di procedure formalizzate di controllo delle modifiche sotto il controllo del Direttore IT.

1.2 Conservazione della Documentazione del Piano

Copie di questo Piano, CD e copie cartacee saranno conservate in luoghi sicuri da definire da parte dell'azienda. Ogni membro della direzione senior riceverà un CD e una copia cartacea di questo piano da conservare a casa. Ogni membro del Team di Disaster Recovery e del Team di

Business Recovery riceverà un CD e una copia cartacea di questo piano. Una copia master protetta sarà conservata su risorse specifiche stabilite per questo scopo.

1.3 Strategia di Backup

I processi aziendali chiave e la strategia di backup concordata per ciascuno sono elencati di seguito. La strategia scelta è per un sito di recovery completamente speculare presso gli uffici dell'azienda in [località].

Questa strategia comporta il mantenimento di un sito duplicato completamente speculare che consentirà la commutazione istantanea tra il sito live (sede centrale) e il sito di backup.

PROCESSO AZIENDALE CHIAVE	STRATEGIA DI BACKUP
Operazioni IT	Sito di recovery completamente speculare
Supporto Tecnico - Hardware	Sito di recovery completamente speculare
Supporto Tecnico - Software	Sito di recovery completamente speculare
[Continua per tutti i processi elencati...]	

1.4 Gestione del Rischio

Ci sono molte potenziali minacce dirompenti che possono verificarsi in qualsiasi momento e influire sul normale processo aziendale. Abbiamo considerato un'ampia gamma di potenziali minacce e i risultati delle nostre deliberazioni sono inclusi in questa sezione. È stato esaminato ogni potenziale disastro ambientale o situazione di emergenza. Il focus qui è sul livello di interruzione aziendale che potrebbe derivare da ciascun tipo di disastro.

I potenziali disastri sono stati valutati come segue: Probabilità: 1=Molto Alta, 5=Molto Bassa Impatto: 1=Distruzione totale, 5=Fastidio minore

[Tabella delle valutazioni dei rischi specifici...]

2. Emergenza

2.1 Allarme, escalation e attivazione del piano

2.1.1 Eventi che Attivano il Piano

I principali eventi trigger presso la sede centrale che porterebbero all'attivazione del DRP sono:

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

2.2.2 Punti di Raccolta

Quando è necessario evacuare i locali, il piano di attivazione del DRP identifica due punti di raccolta per l'evacuazione:

- Primario – Estremità del parcheggio principale
- Alternativo – Parcheggio dell'azienda dall'altra parte della strada

2.2.3 Attivazione del Team di Risposta all'Emergenza

Quando si verifica un incidente, deve essere attivato il Team di Risposta all'Emergenza (ERT). L'ERT deciderà quindi in che misura il DRP deve essere attivato. Tutti i dipendenti devono ricevere una Quick Reference card contenente i dettagli 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 DR dovrebbero essere attivati
- Stabilire e gestire il team di disaster recovery per mantenere i servizi vitali e tornare al normale funzionamento
- Assicurare che i dipendenti siano notificati e assegnare responsabilità e attività secondo necessità

2.3 Team di Disaster Recovery

Il team sarà contattato e assemblato dall'ERT. Le responsabilità del team includono:

- Stabilire strutture per un livello di servizio di emergenza entro 2.0 ore lavorative
- Ripristinare i servizi chiave entro 4.0 ore lavorative dall'incidente
- Recuperare la normale operatività aziendale entro 8.0-24.0 ore dopo l'incidente
- Coordinare le attività con il team di disaster recovery, i primi soccorritori, ecc.
- Riferire al team di risposta all'emergenza

2.4 Allarme di Emergenza, Escalation e Attivazione del DRP

Questa politica e procedura è stata stabilita per garantire che in caso di disastro o crisi, il personale avrà una chiara comprensione di chi dovrebbe essere contattato. Sono state affrontate procedure per garantire che le comunicazioni possano essere stabilite rapidamente durante l'attivazione del disaster recovery.

Il piano DR si baserà principalmente su membri chiave della direzione e del personale che forniranno le competenze tecniche e gestionali necessarie per ottenere un regolare recupero tecnologico e aziendale. I fornitori di beni e servizi critici continueranno a supportare il recupero delle operazioni aziendali mentre l'azienda torna alla modalità operativa normale.

2.4.1 Allarme di Emergenza

La persona che scopre l'incidente chiama un membro del Team di Risposta all'Emergenza nell'ordine elencato: [Spazio per l'elenco dei contatti]

Il Team di Risposta all'Emergenza (ERT) è responsabile dell'attivazione del DRP per i disastri identificati in questo piano, così come in caso di qualsiasi altra occorrenza che influisca sulla capacità dell'azienda di operare normalmente.

2.4.2 Procedure DR per la Direzione

I membri del team di direzione manterranno una copia cartacea dei nomi e dei numeri di contatto di ogni dipendente nei loro dipartimenti. Inoltre, i membri del team di direzione avranno una copia cartacea dei piani di disaster recovery e continuità aziendale dell'azienda nei loro archivi domestici nel caso in cui l'edificio della sede centrale sia inaccessibile, inutilizzabile o distrutto.

2.4.3 Contatto con i Dipendenti

I manager fungeranno da punti focali per i loro dipartimenti, mentre i dipendenti designati chiameranno altri dipendenti per discutere della crisi/disastro e dei piani immediati dell'azienda. I dipendenti che non riescono a raggiungere il personale sulla loro lista di chiamate sono invitati a chiamare il contatto di emergenza del membro del personale per trasmettere informazioni sul disastro.

2.4.4 Personale di Backup

Se un manager o un membro del personale designato a contattare altri membri del personale non è disponibile o è incapacitato, il membro del personale di backup designato eseguirà i compiti di notifica.

2.4.5 Messaggi Registrati / Aggiornamenti

Per le ultime informazioni sul disastro e sulla risposta dell'organizzazione, i membri del personale possono chiamare un numero verde elencato nella carta DRP. I messaggi includeranno dati sulla natura del disastro, i punti di raccolta e aggiornamenti sulla ripresa del lavoro.

2.3.7 Strutture di Recovery Alternative / Hot Site

Se necessario, l'hot site presso SunGard sarà attivato e la notifica sarà data tramite messaggi registrati o attraverso comunicazioni con i manager. Il personale dell'hot site consisterà solo di membri del team di disaster recovery per le prime 24 ore, con altri membri del personale che si uniranno all'hot site secondo necessità.

2.3.8 Notifica al Personale e alle Famiglie

Se l'incidente ha provocato una situazione che potrebbe causare preoccupazione alla famiglia immediata di un dipendente, come il ricovero di persone ferite, sarà necessario notificare rapidamente i loro familiari immediati.

3. Media

3.1 Contatto con i Media

Il personale assegnato si coordinerà con i media, lavorando secondo le linee guida precedentemente approvate ed emesse per gestire le comunicazioni post-disastro.

3.2 Strategie Media

1. Evitare pubblicità negativa
2. Approfittare delle opportunità per pubblicità utile
3. Avere risposte alle seguenti domande di base:
    - Cosa è successo?
    - Come è successo?
    - Cosa intendete fare al riguardo?

3.3 Team Media

[Spazio per l'elenco dei membri del team]

3.4 Regole per Trattare con i Media

Solo il team media è autorizzato al contatto diretto con i media; chiunque altro venga contattato dovrebbe indirizzare chi chiama o i rappresentanti dei media presenti di persona al team media.

4. Assicurazione

Come parte delle strategie di disaster recovery e continuità aziendale dell'azienda, sono state stipulate diverse polizze assicurative. Queste includono errori e omissioni, responsabilità degli

amministratori e dei funzionari, responsabilità generale e assicurazione per l'interruzione dell'attività.

Se è richiesta assistenza relativa all'assicurazione a seguito di un'emergenza fuori dal normale orario di lavoro, si prega di contattare: [Tabella delle polizze assicurative]

Nome Polizza | Tipo di Copertura | Periodo di Copertura | Importo della Copertura | Persona Responsabile della Copertura | Prossima Data di Rinnovo

5. Questioni Finanziarie e Legali

5.1 Valutazione Finanziaria

Il team di risposta all'emergenza dovrà preparare una valutazione iniziale dell'impatto dell'incidente sugli affari finanziari dell'azienda. La valutazione dovrebbe includere:

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

5.2 Requisiti Finanziari

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

- Posizione del flusso di cassa
- Capacità di prestito temporaneo
- Pagamenti imminenti per tasse, imposte sul lavoro, previdenza sociale, ecc.
- Disponibilità di carte di credito aziendali per pagare forniture e servizi necessari post-disastro

5.3 Azioni Legali

Il dipartimento legale dell'azienda e l'ERT esamineranno congiuntamente le conseguenze dell'incidente e decideranno se possono esserci azioni legali risultanti dall'evento; in particolare, la possibilità di reclami da o contro l'azienda per violazioni normative, ecc.

6. Esercitazione del DRP

Le esercitazioni del piano di disaster recovery sono una parte essenziale del processo di sviluppo del piano. In un'esercitazione DRP nessuno passa o fallisce; tutti coloro che partecipano

imparano dalle esercitazioni – cosa deve essere migliorato e come i miglioramenti possono essere implementati. L'esercitazione del piano assicura che i team di emergenza abbiano familiarità con i loro incarichi e, cosa più importante, siano sicuri delle loro capacità.

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

Appendice A – Piano di Disaster Recovery Tecnologico

Modelli Piano di Disaster Recovery per <Sistema Uno>

PANORAMICA SERVER DI PRODUZIONE:

- Ubicazione:
- Modello Server:
- Sistema Operativo:
- CPU:
- Memoria:
- Disco Totale:
- Handle Sistema:
- Numero Seriale Sistema:
- Voce DNS:
- Indirizzo IP:
- Altro:

SERVER HOT SITE

APPLICAZIONI (Usare grassetto per Hot Site)

SERVER ASSOCIATI

CONTATTI CHIAVE:

- Fornitore Hardware
- Proprietari Sistema
- Proprietario Database
- Proprietari Applicazioni
- Fornitori Software
- Storage Offsite

STRATEGIA DI BACKUP PER IL SISTEMA UNO:

- Giornaliero
- Mensile
- Trimestrale

PROCEDURA DI DISASTER RECOVERY DEL SISTEMA UNO:

- Scenario 1: Perdita Totale dei Dati
- Scenario 2: Perdita Totale dell'Hardware

ADDENDUM AL SISTEMA
CONTATTI

FILE SYSTEMS	FILE SYSTEM AL	FILE SYSTEM MINIMI DA CREARE E RIPRISTINARE DAL BACKUP:
File system	Kbytes	Usati

Altri file critici da modificare:

- [spazio per elenco]

Directory necessarie da creare:

- [spazio per elenco]

File critici da ripristinare:

- [spazio per elenco]

File secondari da ripristinare:

- [spazio per elenco]

Altri file da ripristinare:

- [spazio per elenco]

Piano di Disaster Recovery per <Sistema Due>

PANORAMICA DEL SISTEMA: SERVER DI PRODUZIONE:

- Ubicazione:
- Modello Server:
- Sistema Operativo:
- CPU:
- Memoria:
- Disco Totale:
- Handle Sistema:
- Numero Seriale Sistema:
- Voce DNS:
- Indirizzo IP:
- Altro:

[Stessa struttura del Sistema Uno ripetuta per il Sistema Due]

Piano di Disaster Recovery per la Rete Locale (LAN)

PANORAMICA DEL SISTEMA: SERVER:

- Ubicazione:
- Modello Server:
- Sistema Operativo:
- CPU:
- Memoria:
- Disco Totale:

- Handle Sistema:
- Numero Seriale Sistema:
- Voce DNS:
- Indirizzo IP:
- Altro:

Piano di Disaster Recovery per la Rete Geografica (WAN)

PANORAMICA DEL SISTEMA: APPARECCHIATURE:

- Ubicazione:
- Tipo Dispositivo:
- Numero Modello:
- Specifiche Tecniche:
- Interfacce di Rete:
- Requisiti di Alimentazione:
- Numero Seriale Sistema:
- Voce DNS:
- Indirizzo IP:
- Altro:

Piano di Disaster Recovery per la Connettività Remota

PANORAMICA DEL SISTEMA: APPARECCHIATURE: [Stessa struttura della sezione WAN]

Piano di Disaster Recovery per le Comunicazioni Vocali

PANORAMICA DEL SISTEMA: APPARECCHIATURE: [Stessa struttura della sezione WAN]

Appendice B – Moduli Suggeriti

Modulo di Valutazione dei Danni

[Spazio per il modulo]

Modulo di Gestione delle Attività DR

- Durante il processo di disaster recovery tutte le attività saranno determinate usando una struttura standard
- Dove pratico, questo piano dovrà essere aggiornato regolarmente durante tutto il periodo di disaster recovery
- Tutte le azioni che si verificano durante questa fase dovranno essere registrate

Nome Attività: Numero di Riferimento: Breve Descrizione: Data/Ora di Inizio: Data/Ora di Completamento: Risorse Coinvolte: Responsabile: Processo Aziendale Chiave Interessato: Descrizione del Problema: Entità del Danno:

Modulo di Registrazione Eventi di Disaster Recovery

- Tutti gli eventi chiave che si verificano durante la fase di disaster recovery devono essere registrati
- Un registro degli eventi deve essere mantenuto dal leader del team di disaster recovery
- Questo registro degli eventi dovrebbe essere iniziato all'inizio dell'emergenza e una copia del registro passata al team di business recovery una volta che i pericoli iniziali sono stati controllati
- Il seguente registro eventi dovrebbe essere completato dal leader del team di disaster recovery per registrare tutti gli eventi chiave durante il disaster recovery, fino al momento in cui la responsabilità viene trasferita al team di business recovery

Descrizione del Disastro: Data di Inizio: Data/Ora Mobilitazione Team DR:

Attività Intraprese dal Team DR	Data e Ora	Risultato	Azione di Follow-Up Richiesta
Lavoro del Team di Disaster Recovery Completato:			

Modulo di Report delle Attività di Disaster Recovery

- Al completamento della risposta iniziale di disaster recovery, il leader del DRT dovrebbe preparare un report sulle attività intraprese
- Il report dovrebbe contenere informazioni sull'emergenza, chi è stato notificato e quando, le azioni intraprese dai membri del DRT insieme ai risultati derivanti da queste azioni
- Il report conterrà anche una valutazione dell'impatto sulle normali operazioni aziendali
- Il report dovrebbe essere consegnato al leader del team di business recovery, con una copia alla direzione senior, come appropriato

Il report includerà:

- Una descrizione dell'emergenza o incidente
- Le persone notificate dell'emergenza (incluse le date)
- Azioni intraprese dai membri del DRT
- Risultati derivanti dalle azioni intraprese
- Una valutazione dell'impatto sulle normali operazioni aziendali
- Valutazione dell'efficacia del BCP e lezioni apprese
- Lezioni apprese

Modulo di Mobilitazione del Team di Disaster Recovery

- A seguito di un'emergenza che richiede il recupero delle risorse dell'infrastruttura tecnologica, il team di disaster recovery dovrebbe essere notificato della situazione e messo in standby
- Il formato mostrato di seguito può essere utilizzato per registrare l'attivazione del team DR una volta che il lavoro dei team di valutazione dei danni e risposta all'emergenza è stato completato

Descrizione dell'Emergenza: Data Occorrenza: Data Completamento Lavoro del Team di Disaster Recovery:

Nome del Membro del Team	Dettagli di Contatto	Contattato il (Ora/Data)	Da Chi	Risposta Data Inizio Richiesta	Commenti Rilevanti

Modulo di Mobilitazione del Team di Business Recovery

[Stesso formato del modulo precedente ma per il team di business recovery]

Modulo di Monitoraggio del Progresso delle Attività di Business Recovery

- Il progresso delle attività di recupero tecnologico e aziendale deve essere monitorato attentamente durante questo periodo
- Poiché le difficoltà incontrate da un gruppo potrebbero influenzare significativamente altre attività dipendenti, è importante assicurarsi che ogni attività sia adeguatamente dotata di risorse e che gli sforzi richiesti per ripristinare le normali operazioni aziendali non siano stati sottostimati

Nota: Deve essere identificata una sequenza di priorità anche se, dove possibile, le attività saranno svolte simultaneamente.

Attività di Recovery (Ordine di Priorità)	Persona(e) Responsabile	Data di Completamento Stimata	Data di Completamento Effettiva	Milestone Identificate	Altre Informazioni Rilevanti

Modulo di Preparazione del Report di Business Recovery

- Al completamento delle attività di business recovery, il leader del BRT dovrebbe preparare un report sulle attività intraprese e completate
- Il report dovrebbe contenere informazioni sull'evento dirompente, chi è stato notificato e quando, le azioni intraprese dai membri del BRT insieme ai risultati derivanti da queste azioni
- Il report conterrà anche una valutazione dell'impatto sulle normali operazioni aziendali
- Il report dovrebbe essere distribuito alla direzione senior, come appropriato

Il contenuto del report includerà:

- Una descrizione dell'incidente
- Persone notificate dell'emergenza (incluse le date)
- Azioni intraprese dal team di business recovery
- Risultati derivanti dalle azioni intraprese

- Una valutazione dell'impatto sulle normali operazioni aziendali
- Problemi identificati
- Suggerimenti per migliorare il piano di disaster recovery e/o continuità aziendale
- Lezioni apprese

Modulo di Comunicazioni

- È molto importante durante le attività di disaster recovery e business recovery che tutte le persone e organizzazioni interessate siano tenute adeguatamente informate
- Le informazioni fornite a tutte le parti devono essere accurate e tempestive
- In particolare, qualsiasi stima dei tempi per tornare alle normali operazioni di lavoro dovrebbe essere comunicata con attenzione
- È anche molto importante che solo il personale autorizzato si occupi delle richieste dei media

Gruppi di Persone o Organizzazioni Interessate dall'Interruzione	Persone Selezionate per Coordinare le Comunicazioni	Nome	Posizione	Dettagli di Contatto
Clienti				
Management & Staff				
Fornitori				
Media				
Stakeholder				
Altri				

Modulo di Restituzione delle Operazioni Aziendali Recuperate alla Leadership dell'Unità Aziendale

- Una volta che le normali operazioni aziendali sono state ripristinate, sarà necessario restituire la responsabilità per operazioni specifiche al leader dell'unità aziendale appropriato
- Questo processo dovrebbe essere formalizzato per assicurare che tutte le parti comprendano il cambio nella responsabilità complessiva e la transizione al business-as-usual
- È probabile che durante il processo di recovery, la responsabilità complessiva possa essere stata assegnata al responsabile del processo di business recovery
- Si presume che la direzione dell'unità aziendale sarà pienamente coinvolta durante tutto il recovery, ma affinché il processo di recovery sia pienamente efficace, la responsabilità complessiva durante il periodo di recovery dovrebbe probabilmente essere con un team del processo di business recovery

Modulo di Completamento del Recovery del Processo/Funzione Aziendale

Il seguente modulo di transizione dovrebbe essere completato e firmato dal leader del team di business recovery e dal leader dell'unità aziendale responsabile, per ogni processo recuperato.

Dovrebbe essere utilizzato un modulo separato per ogni processo aziendale recuperato.

Nome del Processo Aziendale: Data di Completamento del Lavoro Fornito dal Team di Business Recovery: Data di Transizione di Ritorno alla Gestione dell'Unità Aziendale: (Se diversa dalla data di completamento)

Confermo che il lavoro del team di business recovery è stato completato in conformità con il piano di disaster recovery per il processo di cui sopra, e che le normali operazioni aziendali sono state efficacemente ripristinate.

Leader del Team di Business Recovery: Nome: Firma: Data:

(Eventuali commenti rilevanti del leader BRT in relazione al ritorno di questo processo aziendale dovrebbero essere fatti qui.)

Confermo che il processo aziendale di cui sopra è ora accettabile per le normali condizioni di lavoro. Nome: Titolo: Firma: Data:

Una gestione degli imprevisti e delle catastrofi è essenziale per poter continuare ad operare anche sotto un elevato momento di stress

Cybersecurity • Risk • Resilience