IDWEB

DISASTER RECOVERY PLAN

OBIETTIVI DEL DISASTER RECOVERY PLAN

- Ridurre al minimo le interruzioni delle normali operazioni.
- Limitare l'entità dei disagi e dei danni.
- Minimizzare l'impatto dell'interruzione.
- Stabilire in anticipo modalità operative.
- Addestrare il personale alle procedure di emergenza.
- Provvedere a un ripristino agevole e rapido del servizio.

Il Piano di Disaster Recovery, ha la funzione di spiegare nel dettaglio le fasi necessarie per il ripristino delle risorse hardware e software utilizzate per l'erogazione del servizio IdSurvey da parte dei tecnici.
Nel piano di DR vengono altresì dettagliate le procedure operative necessarie per effettuare una corretta valutazione della situazione di emergenza/disastro che non consenta la normale erogazione dei servizi da parte di IdWeb. Nel presente documento vengono inoltre descritte le varie fasi

per provvedere al ripristino dei sistemi, ovvero del recupero dei dati e la configurazione delle procedure per arginare l'emergenza e avviare il successivo rientro alle normali condizioni operative.
La Società ha anche provveduto all'analisi delle minacce possibili e dei relativi rischi che possono derivare sia da una non corretta gestione dell'infrastruttura informatica, sia dall'integrità delle apparecchiature elettroniche e informatiche. La sicurezza e l'integrità dei dati, in termini di protezione degli stessi da varie tipologie di cause, esterne e interne alla Società, permette di raggiungere livelli di sicurezza che garantiscono una drastica diminuzione delle probabilità di rischio.

L'integrità fisica dei sistemi informatici, dettagliata nei paragrafi successivi, può infatti essere intaccata o distrutta da:

- Calamità naturali (alluvioni, terremoti, fulmini, etc.).
- Cause accidentali (incidenti, allagamenti, distruzione dell'edificio, distruzione di server o altri elaboratori elettronici in cui siano custoditi i dati trattati).
- Cause esterne (sommosse, rivolte, devastazioni, atti vandalici, eventi socio-politici, furti).

L'integrità fisica delle infrastrutture sono demandate al nostro fornitore cloud Microsoft Azure che ha le conformità e certificazioni per garantire la qualità e la sicurezza dei servizi.

L'elenco aggiornato e completo delle certificazioni è disponibile qui:
https://learn.microsoft.com/en-us/azure/compliance/

L'integrità dei dati, indispensabile per lo svolgimento del servizio, deve sempre essere garantita e potrebbe essere compromessa da semplici errori umani del personale, da guasti, dal non funzionamento della connessioni, da furto di dati o di credenziali di accesso al sistema, da azioni di

hacking. Per limitare la perdita dei dati o l'alterazione degli stessi è necessario predisporre livelli di sicurezza e garantire un corretto e costante backup dei dati trattati, come meglio dettagliato successivamente.

RECOVERY PLAN

In questa sezione viene descritta la soluzione di disaster recovery adottata dalla IdWeb per assicurare la continuità di funzionamento del sistema informatico a fronte di eventi dannosi che comportino un'indisponibilità del servizio.

PERSONALE ADDETTO AL RECOVERY PLAN E COMPETENZE

Personale coinvolto e autorizzato secondo le specifiche del GDPR.

Nome	Posizione	EMail	Telfono personale
Andrea Martinelli	Legale rappresentante	andrea.martinelli@idweb.it	Fare riferimenti alla rubrica aziendale.
Sandro Pazzi	Responsabile Sistemi software	sandro.pazzi@idweb.it	
Stefano Carsena	Responsabile Sistemi Informatici	stefano.carsena@idweb.it	
Luca Pitocchi	Responsabile comunicazione clienti	luca.pitocchi@idweb.it	

IdWeb applica un metodo formale di gestione del rischio che viene aggiornato almeno una volta all'anno tramite audit approfondito o in caso di modifiche importanti, relativo anche al trattamento di dati personali e informazioni sensibili (GDPR). Questo metodo ha l'obiettivo di rendere formali le analisi eseguite, come l'identificazione delle risorse, dei processi aziendali critici, delle minacce e delle vulnerabilità.
IdWeb applica una procedura formale di gestione delle risorse, i ruoli e le responsabilità sono definiti in modo chiaro.
Prima di ogni rilascio, gli aggiornamenti software sono regolarmente oggetto di test approfonditi. si possono eseguire eventuali test di intrusione (se applicabili). Il rilascio viene lanciato gradualmente (1/10/100/1000) e, in caso di rischio, è prevista un'operazione di rollback.
I processi di sviluppo vengono configurati e monitorati costantemente. Contengono i principi per un processo di sviluppo sicuro e le misure di "privacy by design".

Tutti i servizi IdWeb sono monitorati con i seguenti obiettivi:

- individuare gli incidenti di produzione e di sicurezza;
- monitorare le funzioni critiche;
- l'inoltro di alert al personale;
- avvisare i responsabili
- avviare le procedure necessarie;
- garantire l'integrità delle risorse monitorate.

IdWeb prevede un processo di gestione degli incidenti che permette di prevenire, rilevare e risolvere questo tipo di eventi nelle infrastrutture di gestione del servizio e nel servizio stesso. Questo processo include:

- una guida per la classificazione degli eventi ;
- il trattamento degli eventi di sicurezza;
- test del piano di risposta agli incidenti;
- la comunicazione con il cliente.

Queste procedure beneficiano di un processo di miglioramento continuo per il monitoraggio, la valutazione e la gestione globale degli incidenti e delle relative azioni correttive.

La classificazione degli incidenti avviene tramite la seguente tabella: Il Responsabile dei sistemi informatici è tenuto a utilizzare la seguente tabella per determinare il grado di severità dell'incidente.

Livello	Classe	Descrizione	Pesonale coinvolto
1	Ordinario	L'incidente non provoca disservizi significativi e l'impatto sull'operatività della società non è rilevante. L'evento è risolvibile con mezzi di intervento ordinari.	Responsabile del servizio o suo delegato
2	Significativo	Degrado o interruzione di una percentuale minoritaria (< 25%) del servizio per cui lo stesso continua ad essere erogato anche se in modalità rallentata.	A discrezione del responsabile Sistemi Informatici
3	Grave	Degrado o interruzione di una percentuale da media a elevata (26% < x < 55%) del servizio per cui lo stesso continua ad essere erogato ma causando gravi disservizi.	A discrezione del responsabile Sistemi Informatici
4	Disastroso	Incidente che causa l'interruzione di una percentuale da elevata a completa del servizio (56%<x<100%)	Legale rappresentante Responsabile Sistemi software Responsabile Sistemi Informatici Responsabile comunicazione con i Clienti

Di seguito sono riepilogate le fasi della soluzione di DR individuata da IdWeb:

Avvio del piano di emergenza:

1	Contattare il responsabile dei sistemi
2	Determina il grado di disastro
3	Contattare tutto il personale necessario
4	Determinare le azioni da eseguire e in quale sequenza
5	Implementare il piano di ripristino dell'applicazione più appropriato in base all'entità del disastro e eventualmente contattare il fornitore del servizio cloud tramite il supporto dedicato
6	Monitorare i progressi
7	Parallelamente al ripristino dei servizi avvisare gli utenti dell'interruzione del servizio e gestire la comunicazione con i clienti
8	Ripristino e dichiarazione di fine emergenza
9	Stesura della relazione finale
10	Valutare se l'emergenza è un DataBridge ed eventualmente attivare la relativa procedura
11	Valurare eventuali miglioramenti ai sistemi e al DRP

SICUREZZA E DI SALVAGUARDIA DEI DATI

Il backup è un punto fondamentale nelle procedure di DS e per garantire maggiori livelli di sicurezza è necessario che le copie di sicurezza dei dati siano collocate all'esterno della sede della Società, e dell'infrastruttura primaria che eroga il servizio.

IdWeb, per provvedere alla conservazione dei backup si è dotato di un'infrastruttura cloud, coadiuvata da uno specifico ambiente e organizzata come di seguito:

- Backup files: eseguito snapshot giornalmente e conservati per 30 giorni su infrastrutture con ridondanza di zona.
- Database SQL backup: completo 1 volta a settimana conservato per 14 giorni, 1 backup differenziale ogni giorno conservato per 7 giorni, e un backup dei log ogni 15 minuti conservato per 7 giorni, con ridondanza di zona.
- Macchina virtuale completa contenente i database SQL: snapshot ogni 4 ore conservata per 7 giorni, con ridondanza di zona.
- Macchine Kubernetes: snapshot ogni 4 ore conservata per 7 giorni.
- Backup aggiuntivo completo su server farm dislocata geograficamente.

IdWeb, inoltre, provvede all'esecuzione di test periodici in modo che sia garantito l'aggiornamento e il controllo dei piani di backup. I test sono programmati almeno ogni sei mesi e comunque ogniqualvolta il piano sia modificato.

Le infrastrutture Cloud vengono mantenute costantemente sotto controllo, 24/7. Qualsiasi malfunzionamento hardware rilevato sui servizi innesca automaticamente l'intervento da

parte dei team in datacenter, che provvedono a sostituire gli elementi difettosi.

INFORMAZIONI SULL'ARCHITETTURA CLOUD

Da 20 anni ospitiamo i dati dei clienti prestando la massima attenzione alla loro protezione. Per assicurare il più alto grado di sicurezza possibile, utilizziamo dispositivi efficaci e adottiamo una serie di best practice a tutti i livelli della nostra organizzazione e delle infrastrutture.

Sicurezza datacenter

- Data center conformi agli standard di settore, ad esempio ISO/IEC 27001:2013 e NIST SP 800-53, per la sicurezza e l'affidabilità.
- Accesso fisico ai server limitato al personale accreditato.
- Accesso ai datacenter consentito esclusivamente tramite sistemi di autenticazione multifattore per il personale accreditato.
- Sorveglianza video e umana 24/7.
- Sale dotate di sistemi di rilevamento di particelle di fumo e soppressione incendi.
- Personale tecnico presente 24 ore su 24, 7 giorni su 7.
- Data center dotati di sistemi di alimentazione ridondanti, inclusi UPS e gruppi elettrogeni, per garantire continuità del servizio in caso di interruzioni della rete elettrica.
- Microsoft Azure è conforme a un ampio ventaglio di standard internazionali (ISO/IEC 27018, SOC 1/2/3, GDPR, CSA STAR, ecc.), garantendo il rispetto delle normative in materia di protezione dei dati.

Sicurezza e caratteristiche

- Infrastruttura Microsoft Azure basata su tecnologia Hyper-V e servizi cloud nativi, con aggiornamenti e patch di sicurezza automatici inclusi.

- Connettività ad alte prestazioni grazie alla rete globale Microsoft, con disponibilità di ampia larghezza di banda.
- Supporto di reti virtuali isolate (Azure Virtual Network) con gestione sicura e scalabile delle subnet.
- Supporto Microsoft per incidenti 24/7/365.
- Portale Azure e API per la gestione delle risorse cloud.
- Strumenti integrati per il testing di resilienza e la verifica della continuità operativa.
- Servizi di monitoraggio avanzato tramite Azure Monitor e Application Insights.
- Gestione automatizzata dell'infrastruttura host con aggiornamenti e manutenzione trasparenti.
- Scalabilità on-demand delle risorse con provisioning rapido.
- Deploy automatico.
- Local Redundancy Storage.
- Sistema basato su standard Microsoft Azure riconosciuti a livello internazionale.
- SSL
- Backup tramite Azure Backup e soluzioni ridondate.
- Firewall e rete: Azure Firewall, Network Security Groups e protezioni a livello di rete.

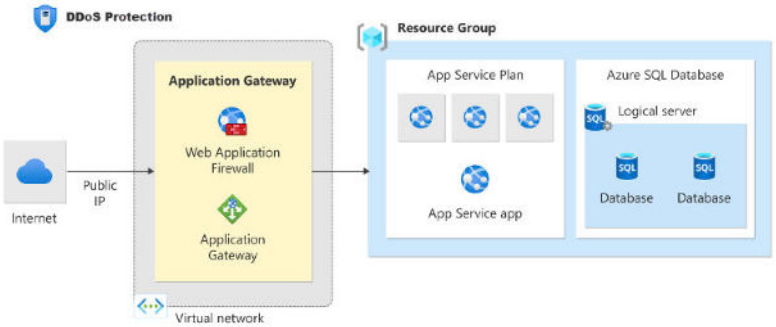
Protezione Anti-DDoS PRO

Con la crescita esponenziale del volume di dati online, gli attacchi distribuiti per l'interruzione del servizio (DDoS, Distributed Denial of Service) sono sempre più frequenti.
Un attacco DDoS ha l'obiettivo di rendere indisponibili server, applicazioni o intere infrastrutture, sovraccaricando la larghezza di banda o esaurendo le risorse di calcolo fino a bloccarne la capacità di risposta.
Per garantire la continuità del servizio, Microsoft Azure integra DDoS Protection.
La protezione si basa su tecniche di mitigazione automatiche che consentono di:

- analizzare in tempo reale e ad alta velocità il traffico di rete
- identificare e deviare il traffico malevolo prima che raggiunga le risorse

- filtrare i pacchetti non legittimi e consentire solo il traffico valido.

Questa protezione è attiva 24/7 e sfrutta la rete globale Microsoft per garantire resilienza anche contro attacchi su larga scala.



Certificazioni struttura server farm OnCloud
Il servizio Cloud è progettato e sviluppato secondo i più rigorosi standard di sicurezza internazionali, con un approccio Security by Design e Defense in Depth, che garantisce il massimo livello di protezione dei dati.
Microsoft Azure adotta un approccio trasparente e sottoposto a regolari processi di audit indipendenti. I sistemi di gestione della sicurezza sono certificati secondo ISO/IEC 27001 e conformi a numerosi altri standard, tra cui:

- ISO/IEC 27017 (controlli di sicurezza specifici per il cloud),
- ISO/IEC 27018 (protezione dei dati personali nel cloud),
- SOC 1, SOC 2 e SOC 3,
- PCI DSS (sicurezza dei dati di pagamento),
- CSA STAR (Cloud Security Alliance Security, Trust & Assurance Registry),
- GDPR compliance per la protezione dei dati personali,
- FedRAMP e HIPAA per specifici requisiti normativi internazionali.

L’elenco aggiornato e completo delle certificazioni è disponibile qui: https://learn.microsoft.com/en-us/azure/compliance/

TEST E AGGIORNAMENTI PERIODICI

Infrastruttura
Il test dell'infrastruttura va eseguito almeno ogni tre mesi. Il responsabile dei sistemi deve redigere un documento con il risultato dei test.

Tipo	Periodicità	Responsabile
Test integrità dati	Ogni 3 mesi	Responsabile sistemi software
Test database	Ogni 3 mesi	Responsabile sistemi software
Test del backup	Ogni 3 mesi	Responsabile sistemi informatici
Aggiornamenti secondari	Ogni 3 mesi	Responsabile sistemi informatici
Aggiornamenti importanti	Almeno 1 volta al mese	Responsabile sistemi informatici

Software
I test del sistema software sono fondamentali, devono essere eseguiti ad ogni release e devono rispecchiare la seguente tabella.

	Tipo	Responsabile
1	Test features sul ramo locale	Programmatore
2	Test su master	Team dei test
3	Test su release	Team dei test
4	Test vulnerabilità su release	Responsabile sistemi software Responsabile sistemi informatici
5	Test release installata su piattaforma clienti	Team dei test

Per qualsiasi ulteriore necessità in materia di privacy e sicurezza rivolgersi ai responsabili della sicurezza, al legale rappresentante e ai consulenti del GDPR.

Nome	Posizione	Recapiti
Andrea Martinelli	Legale rappresentante	Fare riferimenti alla rubrica aziendale.
Sandro Pazzi	Responsabile Sistemi software	
Stefano Carsena	Responsabile Sistemi Informatici	
Cristina Vicarelli	Consulente GDPR	
Laura Antonelli	Consulente GDPR	