La Comunicazione - Note, Recensioni e Notizie n. 66
Anno 2022

Dalla business continuity alla resilienza operativa[1]

From business continuity to operational resilience

Giancarlo **Butti** ♦

♦ ISACA Milano

Sommario

Negli ultimi anni, anche in conseguenza di avvenimenti quali pandemia, rischio climatico, crisi energetica, guerra…, le organizzazioni hanno dovuto modificare il loro approccio alla continuità operativa aumentato le risorse dedicate a garantire la propria resilienza.

Il mondo finanziario e le più recenti normative che regolamentano tale materia costituiscono un ottimo esempio di questo nuovo tipo di approccio.

Abstract

In recent years, also as a result of events such as pandemics, climate risk, energy crisis, war ..., organizations have had to change their approach to business continuity by increasing the resources dedicated to guarantee their resilience.

The financial world and the most recent regulations governing this matter are an excellent example of this new type of approach.

Keyword

Resilience, business continuity, business impact analysis, disaster recovery, risk, incident

1 - Introduzione

Nel precedente articolo, **Aziende resilienti** (pubblicato su questa rivista nel 2019) è stato introdotto il tema della resilienza quale auspicata caratteristica delle organizzazioni.

Al riguardo si riprendono alcune definizioni tratte da 2 dei più autorevoli dizionari della lingua italiana, che ben si adattano allo spirito di questo articolo la cui finalità è quella di illustrare l'evoluzione delle tecniche di continuità operativa, proprio in un'ottica sempre più improntata a garantire la capacità di un'organizzazione di fronteggiare situazioni di crisi di varia natura:

[1] Le tabelle ed alcune parti del testo di questo articolo sono tratte dal volume ***G. Butti – Manuale di resilienza, ITER***, in corso di pubblicazione.

Treccani:

3. In psicologia, la capacità di reagire di fronte a traumi, difficoltà, ecc.

Garzanti:

2. capacità di resistere e di reagire di fronte a difficoltà, avversità, eventi negativi ecc.: resilienza sociale

Capacità di reagire di fronte ad un evento avverso, sia questo un atto volontario, involontario, fortuito.

Più in generale è la capacità di un'organizzazione di resistere a eventi che comprendono il mutare della congiuntura economica, l'evoluzione del mercato, i cambiamenti tecnologici…

2 – Essere resilienti

Il tema della resilienza delle organizzazioni, e quindi della loro reale capacità di affrontare situazioni di difficoltà, è di stretta attualità in quanto affrontare scenari di crisi sul lungo periodo è diventata ormai la norma.

La pandemia, sebbene attualmente sia meno incisiva, è solo il primo di uno scenario estremamente diffuso come estensione geografica e temporale, al quale si sono aggiunte la guerra in Ucraina e le relative conseguenze in termini sia economici sia, ad esempio, di crisi energetica.

A questi scenari "temporanei" si sommano quelli endemici, costituiti dalla crisi ambientale e climatica che, secondo The Global Risk Report 2022 saranno ai primi 5 posti (su dieci) degli scenari di rischio dei prossimi 5-10 anni.

Si è passati quindi da una gestione delle situazioni di crisi come fatto eccezionale (tanto che i normali piani di continuità operativa solitamente non erano pensati per essere in grado di gestire situazioni a scenari multipli, considerando la contemporanea presenza di scenari di crisi come un rischio residuo), ad una situazione nella quale gli eventi alla base di una crisi sono persistenti e si sommano fra di loro.

Alla contemporanea presenza degli scenari pandemico, guerra e crisi energetica… si possono ovviamente aggiungere i più tradizionali scenari di crisi solitamente considerati nella predisposizione dei piani di continuità operativa, e cioè quelli legati alla indisponibilità degli asset che supportano i processi aziendali considerati più rilevanti (indisponibilità di edifici, di personale essenziale, dei sistemi informativi, di dati e di documenti…).

Una situazione alquanto complessa che ha visto ripetuti interventi anche di natura legislativa, sia per quanto attiene l'emanazione di misure atte a mitigare dal punto di vista economico alcuni effetti della situazione di crisi (ad esempio quella legata al costo dell'energia), sia per

quanto riguarda una regolamentazione speciale di alcune fattispecie (ad esempio le misure atte a consentire la gestione semplificata da remoto dei contratti bancari).

Il legislatore non si è tuttavia limitato ad interventi tesi a fronteggiare nel breve termine gli effetti degli eventi di crisi, ma è intervenuto anche per predisporre specifiche normative che regolamentano la resilienza delle organizzazioni.

Questo è vero in particolare nel mondo finanziario (tab. 1); è infatti evidente che tale settore sia uno dei più interessati a garantire la propria resilienza e la capacità di assicurare l'erogazione dei propri servizi alla clientela (è stato infatti considerato come uno di quelli a rilevanza strategica nel corso della pandemia).

Le normative citate, pur riferendosi ad un settore specifico, sono tuttavia applicabili anche a molti altri ambiti e quindi possono costituire un punto di riferimento e delle buone pratiche a cui anche molte altre organizzazioni possono attingere e trarre spunto, al fine di implementare le proprie strategie di resilienza.

Spesso tali normative non si limitano infatti ad una generica affermazione di principi, ma entrano nello specifico con indicazioni dettagliate sulle azioni tecnico organizzative da intraprendere.

È quindi consigliabile, per chiunque desideri intraprendere un percorso per la definizione e implementazione di una strategia di resilienza, attingere a queste fonti informative, che si vanno ad aggiungere a documenti più specifici, quali ad esempio lo standard ISO 22316:2017(en)

Security and resilience — Organizational resilience — Principles and attributes.

Tale standard, al quale si rimanda per una completa consultazione, ha la rara caratteristica (condivisa fra gli altri con lo standard ISO 22301:2019(en) Security and resilience — Business continuity management systems — Requirements) di essere liberamente e completamente consultabile sull' Online Browsing Platform dell'ISO (iso.org).

3 - Resilienza e continuità

Entriamo ora un po' più nel dettaglio nel considerare quelli che sono gli aspetti che maggiormente possono differenziare resilienza e continuità operativa.

Mentre la seconda verte principalmente sulla costruzione di soluzioni tese a garantire la capacità di ripartenza di un'organizzazione dopo che un evento avverso abbia interrotto il normale svolgimento di uno o più processi aziendali, la resilienza punta sulla costruzione di soluzioni che consentano di prevenire tali interruzioni.

Ad esempio, nel mondo dei sistemi informativi, la resilienza di un sistema può trovare riscontro, relativamente a certi eventi, nella creazione di soluzioni di alta affidabilità/disponibilità, dove la ridondanza dei componenti limita o annulla gli effetti del verificarsi del guasto di un singolo componente.

Il paragrafo precedente contiene un elemento che è importante sottolineare; l'alta affidabilità/disponibilità è una soluzione che garantisce la resilienza solo per alcune tipologie di eventi. La continuità dei sistemi informativi può infatti essere vanificata da diverse tipologie di incidenti (si veda al riguardo la Tab. 2), ognuno dei quali prevede specifiche soluzioni di recupero e di resilienza.

Ad esempio, contro un attacco ransomware, la presenza di sistemi ridondanti non ha efficacia.

Per predisporre processi resilienti, come si può desumere da quanto fino a qui esposto, è necessario mettere in atto, preventivamente, una serie di misure tecniche ed organizzative.

Il piano di continuità operativa descrive prevalentemente quali soluzioni l'organizzazione ha individuato per poter riprendere ad operare dopo che un evento dannoso ha interrotto l'erogazione di un processo/servizio e dovrebbe anche descrivere le soluzioni messe in atto per limitare la probabilità che un evento dannoso possa provocare l'interruzione di un processo/servizio o che in caso di interruzione le conseguenze siano le più limitate possibili, ma solitamente questi aspetti, che sono fondamentali per rendere sempre più resiliente un'organizzazione, sono poco enfatizzati.

È evidente che la predisposizione sia delle misure preventive atte a limitare probabilità ed impatti in merito alle conseguenze di un evento dannoso, sia le misure di ripristino dopo che un evento dannoso abbia provocato una interruzione di un processo/servizio hanno un costo.

Tale costo deve essere sostenibile dall'organizzazione e cioè deve essere inferiore a quanto l'organizzazione perderebbe in termini economici (o di altra natura) in conseguenza della mancata gestione dell'evento stesso.

Diventa quindi particolarmente importante effettuare una accurata valutazione di quale sia il reale beneficio di una misura di resilienza o di una misura di continuità e per fare questo è necessario valutare il rapporto costo/benefici derivante dalla sua adozione.

Tabella 1. Alcune definizioni di resilienza nella normativa

Bank for International Settlements and International Organization of Securities Commissions: Guidance on cyber resilience for financial market infrastructures
…the ability of a bank to deliver critical operations through disruption*. This ability enables a bank to identify and protect itself from threats and potential failures, respond and adapt to, as well as recover and learn from disruptive events in order to minimize their impact on the delivery of critical operations through disruption. In considering its operational resilience, a bank should assume that disruptions will occur, and take into account its overall risk appetite and tolerance for disruption. In the context of operational resilience, the Committee defines tolerance for disruption as the level of disruption from any type of operational risk a bank is willing to accept given a range of severe but plausible scenarios.*
BCBS: Principles for Operational Resilience
Operational resilience as the ability of a bank to deliver critical operations through disruption. *This ability enables a bank to identify and protect itself from threats and potential failures, respond and adapt to, as well as recover and learn from disruptive events in order to minimize their impact on the delivery of critical operations through disruption. In considering its operational resilience, a bank should assume that disruptions will occur, and take into account its overall risk appetite and tolerance for disruption. In the context of operational resilience, the Committee defines tolerance for disruption as the level of disruption from any type of operational risk a bank is willing to accept given a range of severe but plausible scenarios*
EUROPA: DORA REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014 e (UE) n. 909/2014
digital operational resilience' *'means the ability of a financial entity to build, assure and review its operational integrity and reliability by ensuring, either directly or indirectly, through the use of services of ICT third-party service providers, the full range of ICT related capabilities needed to address the security of the network and information systems which a financial entity makes use of, and which support the continued provision of financial services and their quality throughout disruptions;*
UK Prudential Regulation Authority
"…the ability of firms and the financial sector as a whole to prevent, adapt, respond to, recover, and learn from operational disruptions*. The PRA's proposed approach to operational resilience is based on the assumption that, from time to time, disruptions will occur which will prevent firms from operating as usual and see them unable to provide*

their services for a period. The PRA considers that many firms currently may not sufficiently plan on the basis that disruptions will occur and are therefore not ready to manage effectively when they do."
US: Sound Practices to Strengthen Operational Resilience
"…the ability to deliver operations, including critical operations and core business lines, through disruption from any hazard. *It is the outcome of effective operational risk management combined with sufficient financial and operational resources to prepare, adapt, withstand, and recover from disruptions."*

4 - Analisi dei rischi e BIA (Business Impact Analysis)

La valutazione di quali siano le conseguenze di un evento dannoso per una specifica organizzazione avviene mediante l'esecuzione di un BIA e di una o più analisi dei rischi.

Solitamente, anche se sempre citata nelle buone prassi o negli standard di settore, la relazione (e la differenza) fra un'analisi dei rischi e una BIA nella predisposizione delle soluzioni di continuità operativa non è mai ben definita; non appare chiaro in particolare quale sia in tale contesto la reale funzione di un'analisi dei rischi.

Innanzi tutto in cosa sono differenti queste due attività, qual è il loro scopo e qual è l'importanza della loro relazione?

Chi si occupa di continuità operativa è abituato a ragionare in termini di BIA, cioè della valutazione delle conseguenze (impatto) della mancata erogazione di un determinato processo/servizio in conseguenza di un evento dannoso.

La BIA determina la rilevanza dei processi classificandoli come più o meno critici in funzione dell'impatto complessivo sull'azienda derivante dalla loro mancata erogazione.

La quantificazione, in termini quali/quantitativi, è una funzione del periodo di indisponibilità del processo analizzato.

Maggiore è la perdita economica (o le conseguenze di altro tipo, quali quelle sul piano reputazionale o legale) derivanti dalla mancata erogazione e maggiore sarà la rilevanza del processo.

La valutazione delle perdite viene effettuata considerando una serie di intervalli di tempo predefiniti, uguali per tutti i processi sottoposti ad analisi.

Ad esempio nel mondo finanziario si considerando intervalli a partire da 2 ore fino in genere a 72 ore (2, 4, 8, 24, 72…).

In altri settori l'intervallo minimo che viene preso in considerazione può essere molto più lungo, ad esempio di 24 ore e si arrivano a considerare anche intervalli di una o più settimane.

In questo modo è possibile stabilire una sorta di gerarchia fra i processi, in modo tale da individuare quelli che, essendo più rilevanti, devono essere riattivati per primi in caso di incidente.

Come appena descritto, nella BIA la valutazione delle conseguenze di un evento dannoso riguardano solo gli aspetti di continuità, cioè si prendono in considerazione solo le conseguenze derivanti dall'interruzione di un processo.

Inoltre nella BIA si ragiona considerando un evento come certo.

Si valutano cioè le conseguenze del verificarsi di un evento senza valutare se lo stesso possa realmente accadere. Le misure di recovery infatti sono pensate per operare dopo che un incidente è effettivamente accaduto.

L'analisi dei rischi invece può prendere in considerazione qualsiasi parametro ed in realtà un'organizzazione dovrebbe effettuare più di un'analisi dei rischi.

Le analisi dei rischi possono comprendere infatti diversi aspetti (rischio ICT, sicurezza fisica, safety, privacy…) e solo una valutazione complessiva di tutte conseguenze (di diversa natura) può portare a quantificare realmente gli impatti che un evento avverso ha su una organizzazione.

Non viene valutato quindi solo l'impatto derivante dal fermo di un processo, ma si potrebbero prendere in considerazione, ad esempio, le conseguenze della perdita di integrità e riservatezza di una informazione, le sanzioni derivanti da una violazione di dati personali, le conseguenze per la salute dei lavoratori e di terzi.

Ne consegue che la valutazione dei costi/benefici di una misura per aumentare la resilienza (o di recovery) potrebbe non essere completa se non si sono presi in considerazione tutti i possibili impatti così come accadrebbe nel caso in cui si esegua la sola BIA.

Altra rilevante differenza fra analisi dei rischi e BIA è che nella prima non viene valutato solo l'impatto di un evento dannoso, ma anche la probabilità che tale evento si verifichi.

In altre parole un rischio è una funzione di impatto e probabilità di accadimento di un evento dannoso.

Questo fa sì che in realtà il valore del rischio, introducendo il fattore probabilità, è sensibilmente inferiore al valore del solo impatto.

In altri termini se stabilisco che il valore dell'impatto è di 1 milione di euro, avrò questa perdita solo se l'evento avrà sicuramente luogo.

Tuttavia nell'analisi del rischio è veramente difficile considerare che la probabilità di accadimento sia del 100% e pertanto il valore di 1 milione di euro potrebbe ridursi di molto; se ad esempio stimo che la probabilità di accadimento sia del 10% il rischio sarà di 100.000 euro.

Nella BIA, che considera invece l'evento certo, la perdita sarà stimata comunque in 1 milione di euro.

È evidente che il considerare parametri così diversi per una quantificazione (rischio da una parte, solo impatto dall'altra) non aiuta a combinare i valori risultanti dalle 2 analisi.

Averne evidenza è però importante in quanto consente di fare valutazioni molto più esaustive per quanto attiene le potenziali perdite conseguenti ad un evento.

Altro fattore da prendere in considerazione riguarda il fatto che mentre nella BIA si definisce esattamente il periodo di riferimento per il quale definire il possibile impatto dai diversi punti di vista (come precedentemente indicato), nel caso dell'analisi dei rischi tale parametro di solito viene "erroneamente" omesso.

Non è dato di sapere quindi se ad esempio il rischio derivante dalla perdita di riservatezza di un'informazione sia valutato considerandolo nell'immediato, o dopo una settimana, o dopo un anno…

Per coerenza sarebbe opportuno considerare anche nell'analisi dei rischi tale fattore, ma solitamente chi svolge tale attività non è abituato a questo tipo di valutazione e questo rende ulteriormente difficile combinare i risultati di un'analisi dei rischi e di una BIA.

Dal punto di vista metodologico per lo svolgimento di BIA e analisi dei rischi è possibile operare secondo 2 diverse direttrici.

Se eseguite prima della BIA, le analisi del rischio possono comprendere un perimetro molto ampio.

In questo caso hanno una finalità autonoma e il loro coinvolgimento nella valutazione delle soluzioni di resilienza e continuità è condizionato dalle scelte di chi effettua tale valutazione.

Se eseguite dopo la BIA, le analisi del rischio, possono anche essere finalizzate unicamente alla predisposizione delle soluzioni di resilienza e di continuità e quindi possono limitarsi a valutare le aree considerate critiche dalla BIA stessa.

Tabella 2. EBA - Orientamenti sulla valutazione dei rischi ICT a norma del processo SREP - Classificazione dei rischi ICT - Rischi di disponibilità e continuità ICT

Rischi relativi ICT (elenco non esaustivo)	**Descrizione del rischio**	**Esempi**
Inadeguata gestione della capacità	La mancanza di risorse (ad es. hardware, software, personale, fornitori di servizi) può comportare un'incapacità di offrire un servizio che soddisfi esigenze aziendali, interruzioni di sistema, degrado di servizio e/o errori operativi.	• La mancanza di capacità può influenzare la velocità di trasmissione e la disponibilità della rete (Internet) per servizi come l'Internet banking. • La mancanza di personale (interno o esterno) può comportare interruzioni di sistema e/o errori operativi.
Guasti dei sistemi ICT	Perdita di disponibilità a causa di guasti hardware.	Guasti/malfunzionamento di dispositivi di archiviazione (hard disk), server o altre apparecchiature ICT, causati, ad esempio, da mancanza di manutenzione.
	Perdita di disponibilità a causa di malfunzionamenti software e bug.	• Loop infinito nel software applicativo che impedisce l'esecuzione delle operazioni. • Interruzioni dovute all'uso continuo di sistemi e soluzioni ICT obsoleti che non soddisfano più i requisiti attuali di disponibilità e resilienza e/o che non sono più supportati dai loro fornitori.
Inadeguatezza dei piani di ripristino in caso di disastro e della continuità dei sistemi ICT	Inefficienza delle soluzioni pianificate per la disponibilità e/o di continuità ICT e/o del piano di ripristino in caso di disastro (ad es. centri dati di ripristino alternativi) quando attivato per intervenire in caso di incidente.	Le differenze di configurazione tra il centro dati primario e quello secondario possono causare l'incapacità del centro dati alternativo di fornire la continuità di servizio prevista.
Attacchi informatici dirompenti e distruttivi	Attacchi per scopi diversi (ad es. movimenti militanti, ricatto) che comportano un sovraccarico dei sistemi e della rete, impedendo agli utenti legittimi di accedere ai servizi informatici online.	Gli attacchi di tipo DDOS (Distributed Denial of Service) hanno l'intento di interrompere il servizio e vengono eseguiti tramite una moltitudine di sistemi informatici su Internet controllati da un hacker, che invia a servizi Internet una grande quantità di richieste di servizio apparentemente legittime (ad es. servizi di e-banking).

5 - Le soluzioni per essere resilienti

Rendere resiliente un processo/servizio implica prima di tutto individuare le soluzioni che consentano di garantire la continuità degli asset che lo supportano (si vedano le Tab. 3a, 3b, 3c, 3d per alcuni esempi relativi ai principali asset coinvolti nell'erogazione di un processo) …

Tali asset sono costituiti, come già precedentemente evidenziato da:

- un edificio, nel quale sono allocate le componenti fisiche con cui realizzare il processo e le risorse umane che eseguono le varie attività sottostanti il processo stesso (Tab. 3b)
- i sistemi informativi (Tab. 3a)
- i dati e i documenti
- le materie prime ed i semilavorati, se si tratta di un processo produttivo
- gli impianti produttivi
- le persone che svolgono il processo (Tab. 3c)
- le utilities (energia, acqua, comunicazioni…) (Tab. 3d)
- gli eventuali soggetti esterni coinvolti a vario titolo nella erogazione del processo.

Per ognuno degli asset sopra individuati l'azienda dovrà individuare delle soluzioni (sostenibili dal punto di vista economico, secondo un rapporto costo/benefici valutato in base a quanto emerso dalle analisi dei rischi e dalla BIA) al fine di garantire sia la resilienza del processo cui concorrono, che il recovery dello stesso.

In realtà a questi elementi si aggiungono, per un'azienda, i clienti.

Senza clienti un'azienda non è in grado, teoricamente, di sopravvivere e quindi anche la predisposizione del proprio portafoglio di clienti dovrebbe essere pensato per garantire la resilienza dell'azienda, con una opportuna diversificazione degli stessi.

Come evidenziato nei paragrafi precedenti alcune soluzioni sono legate alla tipologia di evento e anche in questo caso vi è una certa differenza fra l'impostazione delle misure di resilienza e quelle di continuità.

Nel caso delle misure di recovery, infatti, tradizionalmente i piani di continuità operativa sono pensati per operare su scenari obiettivo.

In altri termini, la soluzione che viene individuata ad esempio per fronteggiare l'indisponibilità di un edificio, è indipendente dalla sua causa, in quanto l'obiettivo dell'intervento è quello di minimizzare il tempo di indisponibilità.

La soluzione, che può consistere ad esempio nel trasferire il personale in un altro edificio già predisposto a tale compito, viene attuata sia che l'indisponibilità dell'edificio principale sia causata dall'inagibilità dello stesso provocata da fumi tossici generati da un incendio ad un edificio vicino, sia da un incendio che ha distrutto l'edificio principale.

Si ragiona in altri termini con piani che pensano a soluzioni a brevissimo periodo.

Solo nel caso di soluzioni a lungo periodo infatti è necessario prendere in considerazione l'evento che ha causato l'indisponibilità.

Infatti, mentre nel caso dell'incendio di un edificio vicino a quello principale sarà possibile rientrare in quest'ultimo dopo pochi giorni, nel caso in cui l'incendio abbia interessato lo stesso edificio principale sarà necessario pensare alla sua ristrutturazione, ricostruzione o trasferimento definitivo in un altro edificio, con tempi risolutivi molto più lunghi.

Le soluzioni a lungo periodo possono in realtà anche non essere determinate preventivamente, ma individuate di volta in volta avendo predisposto, nel piano di continuità operativa, delle opportune risorse e deleghe affinché chi ha il compito di gestire la crisi abbia gli strumenti tecnico/economici per farlo.

Solo per alcuni asset, come i sistemi informativi, anche le soluzioni a breve termine sono condizionate dalla causa scatenante, in quanto diverse sono le soluzioni nel caso di un incendio al CED rispetto ad un attacco ransomware.

Per quanto attiene la predisposizione di misure di resilienza, queste sono invece spesso più puntuali.

Ad esempio per rendere resiliente un edificio, sarà necessario predisporre una serie di misure atte a contrastare specifici eventi: misure antisismiche contro i terremoti, dispositivi antincendio contro gli incendi, una adeguata collocazione per evitare rischi di allagamento o la presenza di vicini che svolgono lavorazioni pericolose (o viceversa la vicinanza di servizi di soccorso) …

Spesso le misure di resilienza e di continuità non sono fra loro così nettamente distinguibili; ad esempio per contrastare la mancanza di un fornitore critico, oltre alla presenza di adeguate clausole contrattuali, è opportuna la presenza contemporanea di un altro fornitore che svolga la stessa attività e che sia in grado di farsi carico del 100% del carico di lavoro in caso di necessità (indisponibilità dell'altro fornitore).

Questo tipo di soluzione, per come è impostata, fa sì che l'impatto in caso di indisponibilità di un fornitore sia minima e costituisce una trasposizione, per una diversa tipologia di asset, delle soluzioni di alta affidabilità/disponibilità predisposte per i sistemi informativi.

In realtà le conseguenze del passaggio del carico ad un solo fornitore potrebbe comportare una serie di attività non banali e quindi il reale impatto per l'azienda varia molto in funzione del tipo di servizio erogato dal fornitore.

Inoltre, non sempre è possibile trovare più di un fornitore e quindi, una possibile alternativa, consiste nell'essere preparati a reinternalizzare la lavorazione esternalizzata. Al riguardo ad esempio DORA, o anche altre normative in ambito bancario, prevedono espressamente che la banca predisponga soluzioni di exit strategy rispetto ai fornitori e relative soluzioni di cambio fornitore o reinternalizzazione.

Questo tipo di soluzione va di gran lunga preferita rispetto a semplici accordi contrattuali in quanto l'indisponibilità di un fornitore può essere legata a molteplici fattori; molte aziende italiane si sono trovate in difficoltà a causa della guerra in Ucraina in quanto importavano materie prime solo da aziende ucraine o russe.

Tabella 3a. Esempi di soluzioni di resilienza dei sistemi informativi

Sistemi informativi		
Evento	Soluzioni di resilienza	Soluzioni di continuità
Incidenti informatici		
• Guasti/malfunzionamenti hardware e software di varia entità e gravità che interessano i sistemi informativi • …	• Monitoraggio predittivo dei sistemi • Valutazione delle aree di manutenzione preventiva • Contratti con fornitori di sistemi che supportano processi critici per intervento immediato • Soluzioni in alta affidabilità/continuità degli asset informatici e degli impianti a loro supporto • …	• Soluzioni di contingency nel caso di malfunzionamenti applicativi • Ripristino dell'alta affidabilità • …
Incidenti di sicurezza logica		

• Malattia/infortuni
  ○ del soggetto
  ○ di parenti…
• Altri eventi indipendenti dalla volontà del soggetto
• Aspettativa
	• Attacchi di qualunque tipo e fonte
	• Errori
	• …
		• Recupero dai backup possibilmente mirato
		• …

Incidenti di sicurezza fisica		

• Incendi e altri eventi che distruggono/danneggiano i locali o gli asset informatici
• Furto di asset informatici
• …
	• Sistemi di protezione dei locali
	  ○ Antincendio
	  ○ Antieffrazione
	• Ridondanza infrastrutture di supporto
	  ○ Alimentazione
	  ○ Rete
	  ○ Condizionamento
	• Alta affidabilità/continuità asset informatici
	• Creazione di copie di backup e replica dei DATI (dati, configurazioni, s.o., applicativi…)
	• …
		• Sostituzione/riparazione componente/impianto
		• Disaster recovery
		• …

Tabella 3b. Esempi di soluzioni di resilienza degli edifici

Edifici		
Evento	Soluzioni di resilienza	Soluzioni di continuità
Indisponibilità temporanea		
• Sostanze contaminanti • Allarme bomba • Incendio e altri eventi con effetti limitati • Eventi che coinvolgono edifici vicini • Eventi che coinvolgono altre aree dell'edificio • Sciopero dei trasporti • Manifestazioni • Mancanza di energia e altre utilities	• Anti intrusione ○ Antifurto ○ Vigilanza ○ Videosorveglianza ○ Controllo accessi ○ Recinzioni ○ Cancelli ○ Grate alle finestre ○ Porta blindata ○ Serratura di sicurezza ○ Procedura di gestione degli accessi (comprese autorizzazioni, revoche, smarrimento badge…) ○ Procedura di gestione dei visitatori/ manutentori ○ Aree separate per ricevimento clienti/fornitori • Antincendio ○ Estintori ○ Idranti ○ Rilevatori ○ Allarmi ○ Porte taglia fuoco • Altre misure ○ Antisismica ○ Anti allagamento ○ Eventi atmosferici (fulmini)	• Spostamento verso altre sedi aziendali/non aziendali predisposte per accogliere il personale e dotate di tutti gli opportuni strumenti, collegamenti, dati, documenti… • Smart working • Servizio di trasporto verso le sedi alternative
Indisponibilità prolungata		
• Terremoti • Tsunami ed altri eventi naturali • Incendio • Bomba • Contaminazione prolungata		
Indisponibilità definitiva		
• Distruzione dell'edificio • Danneggiamento dell'edificio non sanabile • Contaminazione irreversibile		

Tabella 3c. Esempi di soluzioni di resilienza del personale

<table>
<tr><th colspan="3">Personale</th></tr>
<tr><th>Evento</th><th>Soluzioni di resilienza</th><th>Soluzioni di continuità</th></tr>
<tr><td colspan="3">Indisponibilità temporanea</td></tr>
<tr><td>• Malattia/infortuni
○ del soggetto
○ di parenti…
• Sciopero diretto o indiretto (trasporti…)
• Altri eventi improvvisi che coinvolgono direttamente o indirettamente il personale</td><td rowspan="4">• Ripartizione su più sedi del personale sottostante al medesimo processo:
○ Sedi aziendali
○ Sedi disponibili non aziendali
○ Smart working programmato
○ Smart working in emergenza
• Ripartizione del personale per collocazione temporale
○ Turnazione
• Condivisione della conoscenza
○ Job rotation del personale nell’ufficio o nell’azienda
○ Formalizzazione della conoscenza
○ Mappare ed evidenziare eventuali strumenti EUC e shawod ICT utilizzati per lo svolgimento dei processi
○ Formazione</td><td rowspan="4">• Utilizzo di personale di backup
○ Personale dello stesso ufficio appositamente addestrato
○ o Personale di altri uffici appositamente addestrato</td></tr>
<tr><td>Indisponibilità prolungata</td></tr>
<tr><td>• Malattia/infortuni
○ del soggetto
○ di parenti…
• Altri eventi indipendenti dalla volontà del soggetto
• Aspettativa</td></tr>
<tr><td>Indisponibilità definitiva</td></tr>
<tr><td>• Malattia/infortuni/morte/
○ del soggetto
○ di parenti…
• Cambio mansione
• Dimissioni/licenziamento
• Pensionamento</td></tr>
</table>

Tabella 3d. Esempi di soluzioni di resilienza delle utilities

Utilities		
Evento	Soluzioni di resilienza	Soluzioni di continuità

• Guasto agli impianti
  ○ Elettrico
  ○ Climatizzazione CED
  ○ Acqua
  ○ Rete geografica
• Mancanza di:
  ○ alimentazione elettrica
  ○ gas o altro tipo di combustibile
  ○ acqua
  ○ rete geografica
	• Impianti
	  ○ Ridondanza impianti essenziali (ad esempio impianto di condizionamento del CED)
	  ○ Ridondanza rete geografica
	  ○ Manutenzione programmata impianti
	  ○ Test periodico impianti
	• Alimentazione elettrica componente essenziale
	  ○ Ridondanza nella alimentazione
		• Alimentazione elettrica
		  ○ Batterie tampone
		  ○ Gruppo elettrogeno

6 - Conclusioni

È necessario rivedere il proprio approccio alla continuità operativa, dando maggior enfasi alle soluzioni che garantiscano una maggior resilienza ai propri processi. Se opportunamente approcciate tali soluzioni non necessariamente comportano oneri aggiuntivi; anzi in alcune situazioni potrebbero comportare anche dei risparmi significativi.

Si pensi ad esempio alla organizzazione del lavoro su turni per tutelare l'azienda rispetto ad uno scenario di indisponibilità del personale; tale organizzazione consente di ridurre gli spazi occupati e gli strumenti utilizzati in quanto questi vengono utilizzati in tempi diversi dal personale dei vari turni.

O ancora si pensi a organizzare il proprio sistema informativo su 2 diversi centri di elaborazione dati contemporaneamente attivi di cui l'uno costituisce non solo il disaster recovery dell'altro, ma anche la soluzione di alta affidabilità.

Per restare competitivi, ma al contempo resilienti limitando i costi, le soluzioni quindi non mancano.

7 - Bibliografia

[1] Bank for International Settlements and International Organization of Securities Commissions, "Guidance on cyber resilience for financial market infrastructures", 2016

[2] BCBS, "Principles for Operational Resilience", 2021

[3] Parlamento Europeo, "REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014 e (UE) n. 909/2014", in fase di pubblicazione

[4] EBA, "Orientamenti sulla valutazione dei rischi ICT a norma del processo SREP - Classificazione dei rischi ICT - Rischi di disponibilità e continuità ICT", 2017

[5] Banca d'Italia, "Circolare 285", 2013

[6] World Economic Forum, "The Global Risk Report 2022", 2022

[7] ISO, "ISO 22316:2017(en) Security and resilience — Organizational resilience — Principles and attributes", 2017

[8] ISO, "ISO 22301:2019(en) Security and resilience — Business continuity management", 2019

[9] Butti G., "Aziende resilienti", La Comunicazione N.R.&N., 2019

[10] Butti G., "I rischi nell'analisi dei rischi: gli errori da evitare per rendere fruibile e ripetibile l'analisi effettuata", Cybersecurity360, 2021

[11] Butti G., "Manuale di resilienza" ITER, in corso di pubblicazione