Scenario 2020: come garantire la resilienza organizzativa

Author : Federica Maria Rita Livelli

Date : 23 Marzo 2020

Scenario

Crisi geopolitiche, guerre dei dazi, pandemie, eventi metereologici estremi, *cyber attacks* sempre più dilaganti: i report pubblicati da *Allianz – Risk Barometer 2020* e dal *World Economic Forum - Global Risk Report 2020* avevano già preannunciato che, per quest'anno e gli anni a venire, lo scenario non sarebbe stato dei più rassicuranti. Di fatto, il 2020 - a fronte degli avvenimenti cui stiamo assistendo - promette di essere **un anno molto intenso, pieno di incertezze e rischi**; un vero e proprio mare tumultuoso in cui le organizzazioni devono essere in grado di navigare e superare le "tempeste".

La resilienza organizzativa: il nuovo mantra

Che cos'è la Resilienza e quali discipline contempla? In base alla ISO 22316:2017 - *"Societal Security Guides for organizational Resilience"* e alle *"BCI's 'Good Practice Guidelines"* (Ed. 2018), la Resilienza Organizzativa è definita come la *"capacità di un'organizzazione di assorbire e adattarsi ad un contesto in continuo mutamento".* Non per niente la parola Resilienza viene dal latino *resilìre, rimbalzare* (in questo caso rimbalzare dopo un imprevisto negativo).

È importante sottolineare come la Resilienza sia il calibrato risultato dell'applicazione dei principi di *Business Continuity & Risk Management*, *Crisis & Emergency Management*, *Cyber Security*, *Facility Security, Safety*, unitamente alla definizione di *Disaster Recovery & Communication Plan:* **organizzazioni "liquide" se non addirittura "gassose", altamente digitalizzate e innovative**, che necessitano conoscenze e informazioni originate sia dall'interno dei propri confini sia da altre organizzazioni ma, al contempo, anche di misure efficaci ed efficienti per gestire i rischi e garantire la continuità operativa.

I *Business Continuity & Risk Manager* - oggi più che mai - dovranno essere pronti a interagire con tutto il contesto aziendale, creando sistemi collaborativi e flessibili dove esperienze, competenze, informazioni, processi e obiettivi aziendali sono sempre più integrati. Non più un approccio per "silos", bensì logiche d'interazione e sinergiche complementarità.

Un **approccio "olistico"** più performante e vincente, come questo, potrà anche contare su dispositivi IoT e Artificial Intelligence in grado di elaborare scenari predittivi che tengano in considerazione sia gli effetti domino sia quelli collaterali, che saranno integrati nei processi di gestione del rischio e nelle pianificazioni aziendali.

Cambio culturale & formazione: binomio vincente

Fondamentale, in questo contesto, sarà attuare cambiamenti delle *policy* e garantire un maggior coordinamento, non solo con le funzioni interne, ma anche con i partner esterni a livello globale, come a livello degli organi delle comunità internazionali, dei governi, del settore privato, della società civile. Un cambio culturale vero e proprio, che comporterà, altresì, l'acquisizione di particolari *skill* digitali degli attori coinvolti e capacità trasversali, di tipo cognitivo e relazionale (i.e. *"soft skills"*).

L'insieme di queste competenze e capacità genera risorse resilienti e, quindi, **organizzazioni resilienti**, in grado di mantenere l'operatività in periodi di crisi, ma anche di mutare ed adattarsi - di volta in volta- allo scenario in cui si troveranno ad operare, come veri e propri camaleonti: la Resilienza non più come un insieme di fattori/attori isolati, bensì come un insieme di misure strategiche, skill e valori condivisi e incorporati, destinati a rendere le organizzazioni **più "sicure", affidabili e performanti**.

Conclusioni

Mi piace **immaginare l'organizzazione come un'orchestra sinfonica**, i *Business Continuity & Risk Manager* come direttori d'orchestra che dirigono la "*sinfonia*" organizzativa, i.e. contribuiscono a identificare i rischi e le minacce e a predisporre piani di *Business Continuity & Disaster Recovery*, in modo che tutti gli attori aziendali coinvolti imparino il proprio "repertorio" e siano pronti a "suonarlo" all'occorrenza. Pur mantenendo la propria identità di "solisti", gli orchestrali, all'atto dell'esecuzione della sinfonia, saranno in grado di interagire olisticamente, contribuendo - tutti insieme - alla buona riuscita della performance.

Fondamentale è la capacità di un'organizzazione di rispondere agli eventi, monitorare l'andamento, effettuare le debite analisi di contesto interno ed esterno, elaborare le esperienze passate e, mediante la tecnologia, riuscire a effettuare **analisi predittive**. Un'organizzazione - non passiva e conscia del contesto in cui si trova ad operare - sarà così pronta a perseguire i propri obiettivi grazie ad un acquisito grado di conoscenza e consapevolezza di sé.

Forse apparirà esagerato scomodare qui l'Oracolo di Delphi, ma la sua massima - "*Gnose seautón*" (i.e. "Conosci te stesso") - è sempre attuale e vale anche per le aziende.

Riferimenti

Allianz – *Risk Barometer*

2020, https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2020.pdf

World Economic Forum - *Global Risk Report 2020,* http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf

ISO 22316:2017 *Societal Security Guides for organizational Resilience,* https://www.iso.org/standard/50053.html

BCI's 'Good Practice Guidelines (ed. 2018), https://www.thebci.org/product/good-practice-guidelines-2018-edition---download.html

Articolo a cura di **Federica Maria Rita Livelli**