IVASS
ISTITUTO PER LA VIGILANZA SULLE ASSICURAZIONI

SERVIZIO NORMATIVA E POLITICHE DI VIGILANZA
DIVISIONE NORMATIVA

Rifer. a nota n. *del*

Classificazione III 1 1
All.ti n .

Alle imprese di assicurazione con sede legale in Italia
LORO SEDI
Alle imprese di riassicurazione con sede legale in Italia
LORO SEDI
Alle Ultime Società Controllanti con sede legale in Italia
LORO SEDI

Alle Rappresentanze per l'Italia di imprese di assicurazione e riassicurazione con sede legale in uno Stato terzo rispetto allo Spazio Economico Europeo.
LORO SEDI

Oggetto Orientamenti sulla sicurezza e sulla governance della tecnologia dell'informazione e comunicazione.

Il 6 aprile 2021 l'Autorità europea delle assicurazioni e delle pensioni aziendali e professionali (EIOPA) ha emanato gli orientamenti sulla sicurezza e sulla *governance* della tecnologia dell'informazione e comunicazione ("orientamenti"). Essi si applicano a decorrere dal 1° luglio 2021.

Gli orientamenti forniscono le indicazioni in materia di *governance* previste dalla direttiva 2009/138/CE ("direttiva Solvency II") e dal regolamento delegato (UE) 2015/35 (6) della Commissione ("regolamento delegato") da applicare nel contesto della sicurezza e della *governanc*e delle tecnologie dell'informazione e della comunicazione (ICT). Essi tengono conto degli orientamenti già espressi dall'EIOPA[1].

L'IVASS, con il regolamento n.38 del 3 luglio 2018, recante disposizioni in materia di sistema di governo societario delle imprese e dei gruppi, ha completato l'adeguamento al *framework Solvency II* della normativa secondaria di settore. I principi in esso contenuti e in particolare le disposizioni di cui all'articolo 16 in materia di sistemi informatici e *cyber security* sono in larga parte coerenti con i contenuti degli orientamenti.

Il maggior grado di dettaglio operativo e il carattere di novità di alcune previsioni richiedono una attenta rilettura dei processi, delle procedure organizzative e del sistema dei controlli attuati dalle imprese per assicurare il pieno raggiungimento degli obiettivi.

Al riguardo, si richiama in particolare l'attenzione sull'esigenza di integrare il sistema di gestione dei rischi tenendo conto anche delle esposizioni ai rischi in ambito ICT e *cyber security*, per i quali è richiesta, tra l'altro, sia la determinazione di limiti di tolleranza sia la predisposizione di *report* periodici all'Organo amministrativo, quale responsabile dell'istituzione e dell'esito del processo di gestione dei rischi (orientamento n. 4).

[1] Orientamenti sul sistema di *governance* e in materia di esternalizzazione a fornitori di servizi *cloud*

Inoltre, nell'ambito del sistema di *governance* e nel rispetto del principio di proporzionalità, è prevista l'istituzione di una Funzione, caratterizzata da indipendenza e obiettività, dedicata alla sicurezza informatica il cui responsabile riferisce all'Organo amministrativo. L'indipendenza e l'obiettività sarà assicurata con la separazione dai processi operativi e di sviluppo delle ICT. Alla Funzione sono attribuiti compiti di assistenza e *reporting* all'Organo amministrativo oltre che di monitoraggio e coordinamento delle attività in materia di sicurezza informatica (orientamento n. 7). La Funzione non è da annoverare tra le *funzioni fondamentali*, come definite dalla regolamentazione *Solvency II,* in quanto non menzionata negli articoli 268 e seguenti del regolamento delegato.

Nell'ambito dei sistemi ICT, è previsto che sia istituito e attuato un processo di *change management* affinché i cambiamenti introdotti siano censiti, valutati, autorizzati e attuati in modo controllato. È altresì richiesto che siano tracciati anche i cambiamenti sopravvenuti per cause urgenti o di emergenza (oggetto di un'analisi del rischio *ex post)* e che sia stabilito se i cambiamenti al contesto operativo abbiano un impatto sulle misure di sicurezza adottate o comportino l'adozione di ulteriori misure per mitigarne i rischi (Orientamento n. 18).

Infine, nell'ambito di una sana gestione della continuità operativa, in relazione alla quale il Regolamento n. 38/2018 prevede la predisposizione di un piano (art. 16, comma 2 lettera e), è richiesto che una analisi di impatto valuti l'esposizione a gravi interruzioni dell'attività e il loro potenziale impatto sotto il profilo quantitativo e qualitativo e che l'infrastruttura ICT sia ideata in modo da mitigare anche i rischi rilevati da tale analisi (Orientamento n. 20).

***

Nelle more di una più ampia revisione della regolamentazione secondaria, l'Istituto si aspetta che le imprese e le ultime società controllanti in indirizzo tengano conto di tutto quanto precede al fine di assumere iniziative utili per assicurare il massimo livello di conformità con gli orientamenti.

Distinti saluti

Per il Direttorio Integrato

Il Presidente

Firmato digitalmente da

LUIGI FEDERICO SIGNORINI