Gli adeguamenti alla IORP2 e l'approccio al rischio informatico

Assetto organizzativo e documentale

Agenda

- I presidi informatici: cosa chiede la Iorp2 per i fondi pensione?
- Assetto organizzativo e documentale richiesto da Covip
- Direttive Covip del 29 luglio 2020 (sistema informativo, controllo e gestone del rischio, presidi informatici e relativi piani)
- Istruzioni di vigilanza in tema di trasparenza del 22 dicembre 2020 (sito web e telematizzazione)
- Riflessioni su individuazione e monitoraggio del cyber risk valide anche per fondi sanitari e casse di previdenza

DORA REGULATION

- Il 2 ottobre 2020, la Commissione europea ha avviato una consultazione sulla proposta normativa di un "Digital Operational Resilience Act" (DORA).

- Il testo in esame è stato pubblicato dalla Commissione Europea il 24 settembre, come parte del "pacchetto" di norme in materia di Finanza Digitale (Digital Finance Package) e affronta il delicato tema della cyber-resilienza del settore finanziario.

- OBIETTIVO: Armonizzazione completa delle disposizioni sulla resilienza operativa digitale e sulla sicurezza delle ICT

- Espressamente ricompresi IORP

Policy scritte

- Incremento della telematizzazione determina un incremento dell'esposizione al rischio informatico

- Piano del sistema informativo con presidi informatici e piano strategico sulle tecnologie dell'informazione e della comunicazione (due documenti distinti)

- Piani informatici e piani emergenza (due documenti distinti)

- Presidi cyber security e privacy

- Politica gestione rischi e valutazioni interne: l'approccio dei fondi pensione al cyber risk

Sito web, tecnologie informatiche e rapporti con gli aderenti (Istruzioni Covip 22 dicembre 2020)

- **Sito web – area pubblica**: info sul fondo e contatti, elenco documenti oggetto di pubblicazione, motori di calcolo e istruzioni di utilizzo **Aggiornamento info riportate entro 30 giorni dalla variazione**

- **Sito web – area riservata**: modifica dati personali, possibilità di chiedere liquidazioni, presentare reclami, ri-sottoposizione periodica del questionario di autovalutazione, motore di calcolo, info sulle prerogative esercitabili, variazioni accordi istitutivi, eventi societari rilevanti (per fondi aperti e Pip), archiviazione documenti e comunicazioni utili degli ultimi 10 anni di partecipazione o dalla liquidazione, mantenimento area fino a 6 mesi dalla cessazione della partecipazione al fondo, utenza fittizia per verifiche da parte di organi di controllo e Covip;
- **Aggiornamento info riportate entro 60 giorni dalla variazione**

- Sono esonerati dall'obbligo dell'area riservata i fondi pensione preesistenti rivolti esclusivamente a beneficiari e/o differiti.
- I fondi a prestazione definita non hanno l'obbligo dei motori di simulazione

Termini adeguamento sito web e telematizzazione

- il termine per la predisposizione del **sito web – area pubblica** è fissato al 28 febbraio 2021. I documenti, le informazioni e gli strumenti individuati dalla citata Sezione VI, al paragrafo 3.1 (motori di calcolo) devono essere oggetto di pubblicazione sul sito web – area pubblica entro il **31 luglio 2021** (ad eccezione delle informazioni in materia di trasparenza della politica di impegno e degli elementi della strategia di investimento azionario dei fondi pensione la cui pubblicazione resta fissata al 28 febbraio 2021)

- il termine per la predisposizione del **sito web – area riservata** è fissato al **30 giugno 2022.**

Telematizzazione

- Incentivare il processo di telematizzazione al fine di favorire la diffusione delle informazioni e semplificare la gestione dei rapporti tra i fondi e gli aderenti

- Efficace utilizzo dei siti web e delle tecnologie informatiche sia relativamente alla fase di adesione sia con riferimento alla gestione delle pratiche di liquidazione – **Piano strategico sulle tecnologie dell'informazione** (parte del Documento sulle politiche di *governance*)

- **Adesione on line** non obbligatoria (sollecito di Covip all'adozione ma non obbligo; tuttavia può essere necessaria per il collocamento del fiscalmente a carico nei fondi negoziali)

Informatizzazione, rischi e tecniche di difesa dalla minaccia cibernetica

- L'informatizzazione delle procedure e delle comunicazioni comporta un cyber risk, cioè la possibilità che le connessioni informatiche siano utilizzate per danneggiare l'ente oppure per entrare in possesso di informazioni sensibili della cui sicurezza l'azienda è responsabile

- Ogni azienda presenta alcuni elementi di vulnerabilità nell'ambito dell'organizzazione informatica e dei dati sensibili. Per proteggersi dalla minaccia «cibernetica» bisogna innanzitutto mettere in atto adeguate misure di prevenzione sia organizzative sia digitali e fisiche, facendo riferimento a quanto prescritto dal GDPR (Regolamento UE 2016/679).

- Queste soluzioni sono sufficienti? Alcune aziende decidono di optare per il trasferimento del rischio e sottoscrivere una polizza assicurativa cyber risk.

Danni che possono essere causati dai cyber attacchi

I **costi per ripristinare l'operatività del sistema.**
I **danni diretti derivanti dalla violazione dei dati personali** sia dell'ente sia dei clienti o dei fornitori. Rientra in questa categoria l'accesso non autorizzato a questi dati, la loro perdita, divulgazione, oppure alterazione. Secondo quanto stabilito dal GDPR (General Data Protection Regulation), immediata comunicazione all'Autorità di Controllo. Ciò porta all'avvio di un'istruttoria e occorre dimostrare che le misure messe in atto per la protezione dei dati personali erano a norma di legge (**Data Breach**)
I **danni per l'inattività** (blocco operativo)
L'**eventuale perdita dei dati**. Se i dati vengono persi oppure parzialmente o totalmente danneggiati, il loro ripristino comporta costi aggiuntivi
Le **richieste di risarcimento**. Uno degli obiettivi degli **attacchi hacker** è entrare in possesso dei dati personali, sia per acquisire informazioni sugli utenti sia a scopo di estorsione nei confronti del titolare del trattamento. Le aziende sono responsabili del trattamento dei dati personali e della loro sicurezza
I **danni indiretti - reputazionali**

Direttiva IORP2 - Istruzioni Covip

- Recepimento ad opera del **D.Lgs. 147/2018**
  (**modifiche al D.Lgs 252/2005 in vigore dal 1° febbraio 2019**)

- **Deliberazione Covip del 29 luglio 2020**
- **Direttive alle forme pensionistiche complementari in merito alle modifiche e integrazioni recate al d.lgs n. 252/2005**

- **Istruzioni di vigilanza per fondi pensione aperti** **del 13 gennaio 2021**

Assetto organizzativo - sistema dei controlli interni

Il fondo dovrà dotarsi di un **efficace sistema di controlli interni**

- Almeno **«controlli interni di linea»** da parte di risorse operative su determinate attività di propria competenza (controlli sistematici o a campione)
- Possibile istituzione di controlli interni di secondo livello con risorse del fondo che vigilano sui controlli di linea (in base alle dimensioni del fondo, complessità organizzativa, numerosità di incarichi in outsourcing)
- Eventuale **funzione di compliance** (non prescritta dalla normativa)
- La **Gestione del rischio** è un **controllo di II livello** previsto dalla normativa per la generalità dei fondi (può essere interno o esternalizzato) **– mappatura rischi cibernetici**
- Sull'adeguatezza di tale sistema nel suo complesso vigila la **Revisione interna (controllo di III livello) – Audit ICT**

Assetto documentale - sistema di governo

- **Documento sul sistema di governo** redatto dal CdA e reso pubblico annualmente insieme al bilancio/rendiconto:
- **«la prima pubblicazione andrà effettuata nel 2021 unitamente al bilancio/rendiconto per il 2020» (onere di pubblicazione di tutti i documenti entro luglio 2021 cfr delibera covip 25 febbraio 2021)**

- **Solo per fondi negoziali e preesistenti**
- Il documento sul sistema di governo è affiancato da altro **Documento sulle "politiche di governance"** in cui sono riportati gli aspetti più tecnici
- **«redatto in occasione della prima predisposizione del Documento sul sistema di governo»**

- **Raccolta delle politiche scritte e degli altri documenti obbligatori non destinati alla pubblicazione da approvare entro la data di predisposizione del Documento sul sistema di governo**

Il Documento politiche di governance «prende a riferimento»

- le politiche di gestione dei rischi e di revisione interna, nonché quella relativa all'attività attuariale (laddove rilevante);
- il sistema di controllo della gestione finanziaria;
- il piano strategico sulle tecnologie dell'informazione e della comunicazione;
- il sistema informativo del fondo pensione e i presidi di sicurezza informatici adottati;
- i piani di emergenza;
- la politica di esternalizzazione delle funzioni/attività;
- la politica di remunerazione;
- la politica di gestione dei conflitti di interesse.

Manuale operativo delle procedure per fondi negoziali e preesistenti (MOP)

È oggi obbligatoria per fondi negoziali e preesistenti, per esplicita indicazione Covip, la redazione del Manuale operativo delle procedure (MOP) da effettuare **entro la data di approvazione del bilancio relativo all'anno 2020 e da tenere costantemente aggiornato; rivedere procedure adesione con nuove regole Covip in vigore dal 1 maggio 2021)**

Il manuale deve descrivere:

- Le procedure che regolano l'attribuzione di compiti, i processi operativi, gli strumenti e le linee di riporto informativo sono inoltre formalizzate

No pubblicazione no trasmissione a Covip

RISCHI E CONTROLLI in chiave IORP2: nuove riflessioni sull'assetto organizzativo

- **RISCHIO OPERATIVO** (artt. 1, comma 3, lett. c-nonies e 5-ter, comma 4, d.Lgs 252/2005)

- rischio di subire perdite derivanti dall'inadeguatezza o dalla disfunzione di procedure interne, risorse umane o sistemi oppure da eventi esogeni

Rischio tollerabile

- Il **rischio tollerabile** è determinato dalla ricerca del miglior equilibrio possibile tra la soluzione di sicurezza assoluta ed altri fattori quali il beneficio per l'interessato, l'adeguatezza allo scopo, il costo effettivo.

- Il **rischio residuo** corrisponde all'alea che permane in ogni processo perché nessun processo è sicuro in modo assoluto

Nuovo Regolamento in materia di procedure sanzionatorie

- Art. 8 **Esclusioni:** Ai sensi dell'articolo 19-quinquies, comma 1, del decreto n. 252/2005, la COVIP **non procede alla contestazione degli addebiti** quando le infrazioni siano tali da **non poter recare pregiudizio** al tempestivo esercizio da parte della COVIP delle sue funzioni di vigilanza ovvero agli interessi dei potenziali aderenti, aderenti, beneficiari e altri aventi diritto a prestazioni da parte della forma pensionistica complementare.

Gestione del rischio VS Valutazione interna del rischio

- **Politica di gestione del rischio** (mappatura dei rischi e metodi per misurarli, aree di rischio, limiti di tolleranza, frequenza e contenuto delle verifiche)

- **Valutazione interna del rischio** (approvata dal CdA almeno ogni 3 anni, comprende la valutazione di efficacia della gestione del rischio, definisce i metodi di cui il fondo si è dotato per individuare i rischi nel breve e lungo periodo) **comprende la valutazione qualitativa dei rischi operativi (art.5-nonies, c.2, lett.g)**

- **Individuare i metodi necessari da seguire per tale valutazione entro dicembre 2020**, così da poter pervenire alla **prima valutazione interna del rischio entro il 30 aprile 2021**

- **Per i fondi aperti entro giugno 2021**

L'approccio all'own risk assessment (Valutazione interna del rischio)

- Descrizione di come la funzione di gestione del rischio è integrata nel processo gestionale del fondo
- Metodi di individuazione del rischio
- Valutazione di efficacia dei metodi e della politica di gestione del rischio
- Valutazioni di impatto e conclusioni sulla soglia di rischio del fondo
- Il cyber risk è tenuto in considerazione dalla maggior parte dei fondi; da molti valutato come top risk e i controlli attivati risultano di massimo livello rispetto ad altri processi

Presidi informatici (dai documenti dei fondi pensione)

- Sistemi di backup dei dati :

- La base dati del Fondo è gestita da……, che nel rispetto dei requisiti definiti dalla Norma ISO 27001 (per la quale è certificata da un organismo accreditato), assicura l'applicazione di logiche di backup e protezione degli accessi.

- Posta elettronica e documenti memorizzati su Drive

- Sicurezza della rete (sistema firewall capace di proteggere la rete informatica da virus e da eventuali intrusioni da parte di hacker)

- Disaster Recovery

- Controlli di accesso logico

- Controlli di accesso fisico

- **Rinvio a contratti di outsourcing e Mop**

Operatività online: prime prassi

- Distinzione tra procedure «semplici» e procedure «delicate»
  - Contributi e dichiarazioni
  - Premio
  - Switch
  - Trasferimento
  - Prestazioni

Operatività online: prime prassi

Prassi

- Autocompilazione in area riservata e invio cartaceo con documento identità (verifica firma?); invio tramite PEC o mail
- Autocompilazione in area riservata e caricamento modulo e documento identità (verifica firma?)
- OTP (poco frequente)
- SMS e/o Mail di conferma (procedura di cambio da blindare con verifica firma o di persona)

Rafforzamenti possibili

- Doppia autenticazione
- Firma elettronica
- Accesso con Spid 2° livello

Alert e cambio cellulare e mail

Alert sms/mail in occasione delle diverse fasi di lavorazione della pratica. Esempio:

- in occasione della **ricezione della domanda**
- quando **la richiesta è accolta, rifiutata o sospesa**
- al momento del **disinvestimento**
- **prima del pagamento** con indicazione della data di accredito con eventuale codice di conferma da inserire ad opera del richiedente

Procedura cambio user, password, cellulare e mail collegati all'aderente

- La richiesta è inviata all'assistenza del fondo con copia sottoscritta del documento di identità per ottenere il rilascio del numero di iscrizione che è la credenziale di accesso per rigenerare la password (valutare maggiori presidi di sicurezza)