Da: "Lorenzo Possenti" <lorenzo.possenti@iside.bcc.it>
A: <npv@pec.bancaditalia.it>
Data invio: lunedì 19 novembre 2012 11.54
Oggetto: Riferimenti sulla Continuità Operativa del documento "Disposizioni di vigilanza prudenziale per le Banche"

Buongiorno,

mi chiamo Lorenzo Possenti e mi occupo di ContinuitÃ Operativa (programma PEVOPCO) per la societÃ informatica Iside S.p.A. del Credito Cooperativo.

Ho letto il Vostro documento per la consultazione “Disposizioni di vigilanza prudenziale per le banche” e colgo l’occasione per segnalare alcune note che potrebbero rientrare in un “brainstorming” sulla tematica.

Mi scuso anticipatamente per le informazioni di carattere operativo e la non esaustivitÃ delle segnalazioni e lascio a Vostro libero arbitrio il recepimento, l’utilizzo e la pubblicazione di eventuali osservazioni, commenti, proposte.

Sicuramente molto di quanto riportato nella presente Ãš giÃ stato ampiamente discusso e metabolizzato, in tal caso,Â non tenetene conto.

Colgo l’occasione per salutare cordialmente e resto a disposizione per varie e/o eventuali.

Lorenzo Possenti

NOTE

- <!--[if !supportLists]--> <!--[endif]-->A pag. 46 del documento di Banca D’Italia (allegato A) vengono descritte le tipologie di rischi operativi complessivi omettendo il rischio informatico;
- <!--[if !supportLists]--> <!--[endif]-->A pag. 53 del documento di Banca D’Italia nel campo annotazioni (fondo pagina), dove si fa riferimento al “Codice di protezione dei dati personali” Ãš presente il refuso dell’anno 3003, da sostituire con 2003;
- <!--[if !supportLists]--> <!--[endif]-->A pag. 53 del documento di Banca D’Italia si parla di “autenticazione forte”. Nel campo informatico si usano ormai assiduamente i termini anglofoni per descrivere la stessa cosa, ad esempio nel caso specifico “*strong authentication”* (si potrebbe mettere fra parentesi il termine inglese). Lo stesso vale a pag. 54 per la “Gestione dei cambiamenti che nella terminologia informatica viene chiamata “Change management” (si potrebbe mettere fra parentesi);
- <!--[if !supportLists]--> <!--[endif]-->A pag. 64/65, la continuitÃ operativa ha un perimetro ben piÃ¹ ampio del solo ambito informatico perchÃ© riguarda anche problematiche di altra natura, come ad esempio la sicurezza sul lavoro “Legge 81/08 – Compiti e responsabilitÃ ” che devono essere descritti nel “Documento di Valutazione del Rischio” (DVR); infatti il dlgs 81/2008, “Testo Unico della Sicurezza sul Lavoro”, (che sostituisce il precedente dlgs 626/94) ha apportato significativi cambiamenti all’attivitÃ di valutazione dei rischi aziendali, della quale il DVR costituisce la sintesi piÃ¹ efficace. Quindi nell’ambito di continuitÃ operativa dovrebbe essere perlomeno indicato il decreto legge, visto che nel documento si parla anche di: “indisponibilitÃ di personale essenziale per il funzionamento dell’azienda”;
- <!--[if !supportLists]--> <!--[endif]-->Non ho trovato nessun riferimento alla composizione della BIA (Business Impact Analysis) che risulta un documento fondamentale per la stesura del Piano di ContinuitÃ Operativa;
- <!--[if !supportLists]--> <!--[endif]-->Non ho trovato nessun riferimento alla composizione del Piano di rientro alla normalitÃ dopo un eventuale evento disastroso;
- <!--[if !supportLists]--> <!--[endif]-->Non ho trovato nessun riferimento al nuovo standard internazionale “ISO 22301” o alla metodologia ABILAB;
- A pag. 71 del documento di Banca D’Italia si parla della perdita di informazioni (cioÃš recovery point objective) ma nel documento non viene mai specificato il recovery time objective (massimo tempo di ripartenza dei servizi); ad esempio sempre a pag. 71 viene descritto il “a) per banche e gruppi bancari: entro 4 ore dalla dichiarazione dello stato di crisi”; le 4 ore corrispondono al valore temporale di RTO, basterebbe modificare la frase introducendo il concetto espresso comunemente nella tematica di DR o continuitÃ operativa, ad esempio: “a) per banche e gruppi bancari: entro 4 ore (RTO – Recovery time objective) dalla dichiarazione dello stato di crisi”;

Â

- Â Â Definizione di “Accountability” a pag. 46 del documento di Banca D’Italia. L’accountable Ãš definito nella RACI (**R**esponsible, **A**ccountable, **C**onsulted, **I**nformed). Solitamente le metodologie dicono cosa fare ma non come farlo e un tipico esempio riguarda l’assegnazione delle responsabilitÃ . In una tematica cosÃ¬ importante come la Business Continuity definire chi deve fare, che cosa risulta basilare; potrebbe essere inserito negli allegati un tipico esempio di “Matrice di Assegnazione delle ResponsabilitÃ (RAM)”, cioÃš:Â la matrice di assegnazione delle ResponsabilitÃ pone in relazione le risorse con le attivitÃ delle quali sono coinvolti, chiarisce i ruoli e le ResponsabilitÃ definendo: chi, fa, che cosa. Ad esempio per determinate tipologie di organizzazione:

RACI										
Descrizione	**Comitato di Crisi**	**Responsabile Comitato di Crisi**	**Responsabile del Piano diÂ ContinuitÃ Operativa (BCMS)**	**Responsabile Operativo DR**	**Team di intervento**	**Responsabile BCRS**	**Tutto il Personale**	**Servizi Generali**	**Direzione Risorse**	**Direzione Commerciale**
Rilevazione e segnalazione allarme	I	I	A	R	-	I	R	C	-	-
Valutazione Danno	I	R	R	R	I	-	-	IR	-	-

Dichiarazione Disastro	I	A	R	C	C	-	-	-	-	-
Comunicazione interna e fornitori	I	A	I	-	-	-	-	-	R	-
Comunicazione alla clientela e Mass media	I	A	I	-	-	-	-	-	I	R
Compilazione checklist generale	I	I	A	C	R	-	-	R	-	-
AttivitÃ di configurazione sistemistiche BCRS	I	A	I	C	I	R	I	-	-	-
AttivitÃ sistemistiche ed operative Iside	I	I	I	A	R	R	I	-	-	-

Â

Legenda

Â

Accountable Â - "**A**" Ãš aziendalmente chi approva la deliberable ed Ãš il ruolo a cui riporta il/i Responsible o che comunque dovrÃ svolgere un ruolo di supervisione del lavoro del/dei Responsible;

ResponsibleÂ - "**R**"Â Ãš aziendalmente il ruolo di colui che Ãš chiamato ad eseguire operativamente il task/ deliverableÂ (per ogni task Ãš possibile avere piÃ¹ Responsible);

ConsultÂ - "**C**" Ãš il ruolo di chi dovrÃ supportare il/i Responsible nello svolgimento del task fornendogli informazioni utili al completamento del lavoro o a migliorare la qualitÃ del lavoro stesso;

Inform - "**I**" Ãš il ruolo di chi dovrÃ essere informato in merito al lavoro del/dei Responsible e che dovrÃ prendere decisioni sulla base delle informazioni avute.

--

L.Possenti, ContinuitÃ Operativa Iside S.p.A.
via Rivoltana 95 - 20096 Limito di Pioltello (MI)
direct line: +39 02 75398452 , fax.: +39 02 75398228
Email: lorenzo.possenti@iside.bcc.it Web: isidenet.com

AVVISO DI RISERVATEZZA: Il testo e gli eventuali documenti trasmessi contengono informazioni riservate al destinatario indicato. La seguente e-mail Ãš confidenziale e la sua riservatezza Ãš tutelata legalmente dalle normative vigenti. La lettura, copia od altro uso non autorizzato o qualsiasi altra azione derivante dalla conoscenza di queste informazioni sono rigorosamente vietate. Se si ritiene di non essere il destinatario di questa mail, o se si Ãš ricevuto questa mail per errore, si prega di darne immediata comunicazione al mittente e di provvedere immediatamente alla sua distruzione. Prima di stampare, pensa all'ambiente.