BancaStato

Crescere insieme.

BancaStato
BANCA DELLO STATO DEL CANTONE TICINO

Il “rischio sicurezza” in Banca

Manifestazione ATED / AIEA

M. Molteni
Responsabile Servizio sicurezza BancaStato

Hotel Villa Sassa - Lugano
mercoledì, 19 gennaio 2011
16:30 – 17:10

Un mare di parole
produce una goccia di fatti.

Proverbio cinese

Dimentico quello che ascolto.
Ricordo quello che vedo.
Imparo quello che faccio.

Proverbio cinese

Di cosa parleremo?

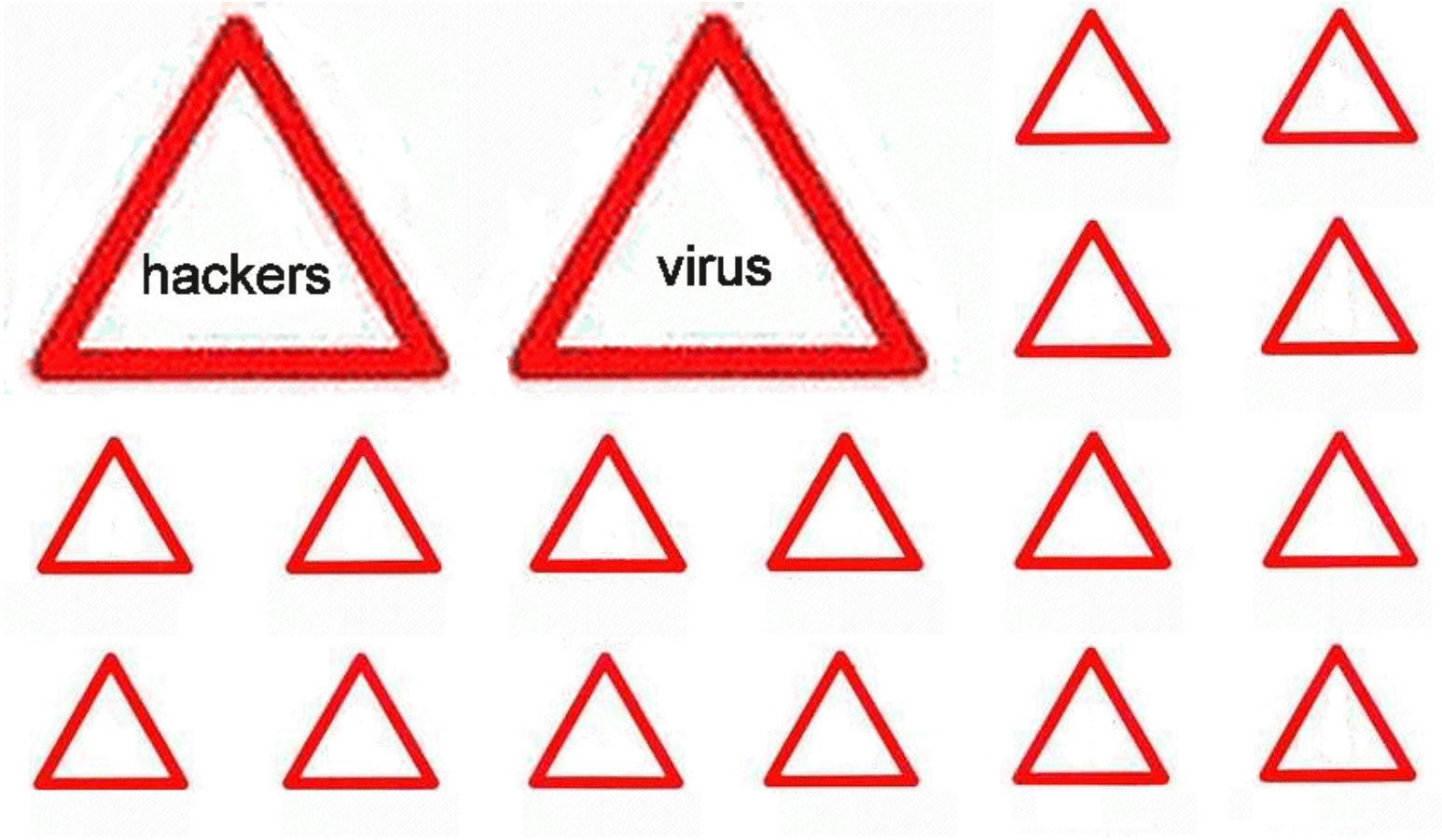
- **Rischi (definizione, gestione)**
- **Rischio sicurezza in Banca**
- **Business Continuity Management (BCM)**
- **Gestione della continuità aziendale**

Il rischio (definizione)

I pericoli nel mondo reale...

Il rischio (definizione)

... e quelli nel mondo digitale.



Il rischio (definizione)

- ***Incidente*** ***(Incident)***
  - ***Situazione, circostanza*** **o** ***insieme di circostanze*****,**
  - **con possibilità di conseguenze dannose o negative.**

- ***Minaccia*** ***(Threat)***
  - ***Atto*** **compiuto per incutere timore.**
  - ***Discorso*** **fatto per spaventare.**

P E R I C O L O

CAUSA ***(identificare - misure preventive)***

EFFETTO ***(gestire - misure di protezione)***

- ***Rischio*** ***(Risk)***
  - ***Conseguenza*** **(*evento*) che si può manifestare**
  - **a seguito di situazioni, circostanze o insieme di circostanze**
  - **non sempre prevedibili (*pericoli*).**

Il rischio (gestione)

- **Gestione del rischio**
- **- Analisi del rischio (identificazione, classificazione e valutazione)**
- **- Trattamento del rischio (modalità, controlli, misure)**
- **- Monitoraggio**
- **- Reporting**

Il rischio (gestione)

- **Gestione del rischio**

- **- Analisi del rischio (identificazione, classificazione e valutazione**)
- *Una corretta gestione del rischio, a livello aziendale, comporta lo svolgimento di un'attività di **analisi del rischio**, a carattere ricorrente su base periodica definita, seguita da una chiara politica di **trattamento dei rischi** identificati.*

- *L'analisi del rischio comporta un'attività di identificazione e classificazione e una di valutazione.*

- *L'attività di identificazione e classificazione deve essere sufficientemente approfondita da permettere poi una valutazione il più possibile oggettiva e significativa.*

- ***I rischi ritenuti, classificati secondo la tipologia di rischio considerata, sono identificati, classificati e valutati secondo lo schema classico dell'analisi del rischio (probabilità evento / impatto potenziale), laddove la probabilità è realistica e l'impatto a livello aziendale potrebbe risultare elevato.***

Gestione del rischio

- **- Analisi del rischio (identificazione, classificazione e valutazione**)
- *- identificazione e classificazione del rischio =*
  tipologia di rischio considerata + rischi ritenuti per tipologia considerata
- > Tipologia di rischio considerata:
  - *rischio strategico e finanziario*
  - *rischio sicurezza*
  - *rischio IT*
  - *rischio legale / fiscale*
  - *rischio compliance*
  - *rischio immagine / reputazione*
  - *...*
- > Rischi ritenuti per tipologia considerata:
  - *mancanza di..., non adeguatezza di, non trasparenza di...,*
  - *non affidabilità di..., non continuità di..., non conformità di...,*
  - *indisponibilità di, inaccessibilità a...,*
  - *errori / omissioni, guasti / malfunzionamenti,*
  - *...*

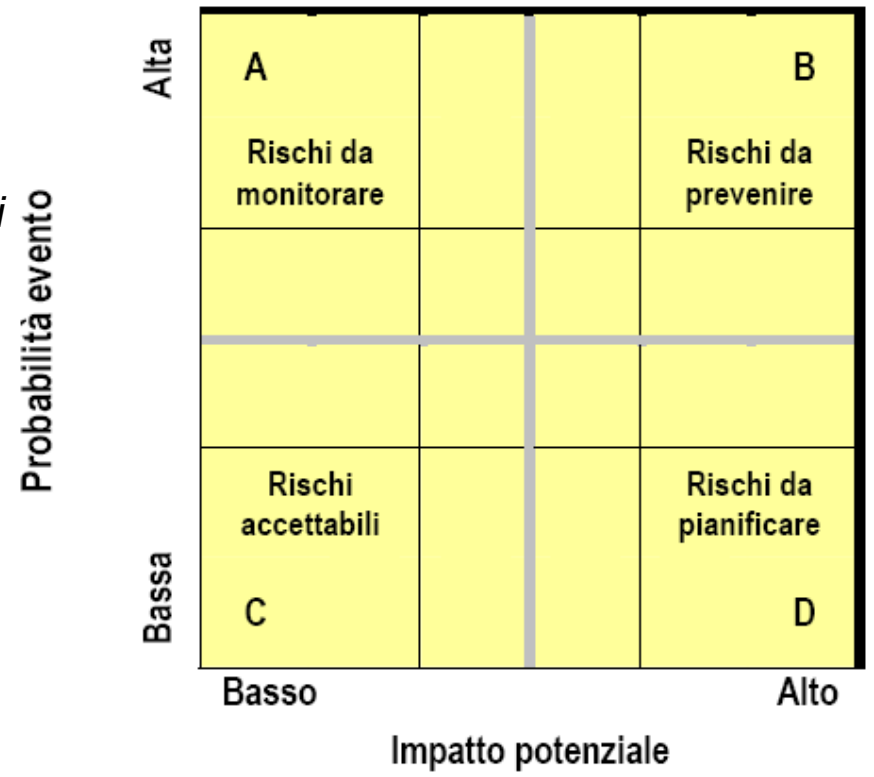
Il rischio (gestione)

- **Gestione del rischio**

- **- Analisi del rischio (identificazione, classificazione e valutazione)**
- *- valutazione*

  La valutazione dei rischi comporta, per ogni voce di rischio (evento ritenuto), la formulazione di una valutazione in termini di probabilità / impatto, considerandone le possibili conseguenze (ad es.: il probabile impatto in termini di danneggiamento dell'immagine e della reputazione della Banca come pure di possibile perdita finanziaria).

- ***IMPATTI (esempi)***
- *- Interruzione di uno o più servizi alla clientela*
- *- Disservizi / ritardi verso la clientela / il fronte*
- *- Danni di immagine / di reputazione*
- *- Perdite finanziari / aumento costi*
- *- Conseguenze legali / penali*



Il rischio (gestione)

- **Gestione del rischio**

- **- Trattamento del rischio**
  Il trattamento del rischio comporta, per ogni rischio ritenuto e valutato, l'identificazione della modalità di trattamento voluta, dei controlli (ex-ante, ex-post) e delle misure adottati.

- *La modalità di trattamento del rischio è, tipicamente, quella di:*
- *- **ignorare il rischio** prassi che rappresenta di per se un rischio strategico*
- *- **evitare il rischio** adeguando la propria strategia (approccio minimalista al trattamento del rischio identificato)*
- *- **mitigare il rischio** introducendo delle misure organizzative e tecniche di protezione preventive/dissuasive e dei controlli "ex-ante" ed "ex-post" adeguati*
- *- **trasferire il rischio** condividendolo con terzi (ad es.: outsourcing) oppure optando per una o più coperture assicurative adeguate*
- *- **assumersi il rischio** riconoscendolo formalmente e tenendolo sotto controllo monitorandolo; l'assunzione del rischio comporta una sua accettazione in termini di impatto valutato (infatti l'accettazione del rischio implica una sua non mitigazione e un suo non trasferimento)*

Il rischio (gestione)

- **Gestione del rischio**

- **- Misure in essere (*misure di sicurezza*)*:**
- *- misure preventive: a prevenzione dei pericoli (in termini di probabilità possibile)*
- *- misure di protezione: a contenimento dei rischi (in termini di impatti potenziali)*

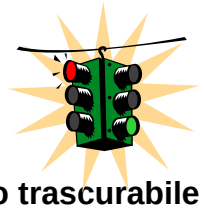
- **- Misure d'urgenza da attuare**

- **- Monitoraggio (controlli "ex-ante" / "ex-post")**

- (*****) ad es. sistemi di allarme, misure antincendio, divieto di fumare, generatori, gruppi di continuità, centro EDP di backup, backup dei dati, ridondanza rete IT, DMZ, IDS/IPS, soluzioni anti-malware, controllo e traccia accessi (stabile e IT), videosorveglianza, contratti/SLA terze parti, profilo collaboratori, ...

Il rischio (gestione)

- **Gestione del rischio**

- **- Reporting:**
- **- Apprezzamento del rischio per tipologia di rischio considerata (sintesi)**
- **- Apprezzamento del rischio per evento ritenuto per tipologia (dettaglio)**
- *> Tipologia di rischio*
- *> Rischio ritenuto*
- *> Probabilità (alta / media / bassa)*
- *> Impatto (alto / medio / basso) + ev. descrizione*
- *> Trattamento (mitigato / trasferito / assunto) + ev. descrizione (misure)*
- *> Livello di rischio*
- **(☺ 😐 ☹ oppure**  **oppure legenda**

  Nessun effetto / Rischio trascurabile / Rischio significativo / Rischio elevato / Rischio catastrofico)

- *> "**La copertura del rischio XYZ è ritenuta insufficiente / sufficiente / adeguata."***

Il rischio sicurezza (definizione)

- **Il rischio sicurezza è un rischio di tipo operativo.**

- ***Il rischio sicurezza è definito come il rischio che nasce da situazioni che possono compromettere il livello di riservatezza, integrità e disponibilità esistente, con particolare riferimento alla protezione delle persone, dell'informazione / del segreto bancario e alla garanzia di continuità del servizio erogato alla clientela (per quanto applicabile singolarmente).***

- **Il rischio sicurezza può generare sia un rischio legale, sia un rischio compliance, sia altri rischi operativi o derivare da essi.**

Il rischio sicurezza (tipologie)

- ***Rischi umani*** *(a seguito di comportamenti inadeguati, errori, negligenze, attività dolose, attività criminali, ...)*

- ***Rischi organizzativi*** *(a seguito di processi e controlli non adeguati, ...)*

- ***Rischi tecnici*** *(a seguito di attacchi, malfunzionamenti, guasti, ...)*

- ***Rischi edilizi*** *(a seguito di malfunzionamenti, guasti, ...)*

- ***Rischi ambientali*** *(a seguito di incendi, black-out, danni della natura, ...)*

Il rischio sicurezza (situazioni)

- **eventi o calamità naturali (ad es. incendi, allagamenti, perdite d'acqua o gas, ecc.)**
- **abusi, malversazioni, danneggiamenti, negligenze o errori umani**
- **malfunzionamenti o guasti alle infrastrutture e alle installazioni**
- **truffe, furti (di vario genere), rapine, minacce (di qualsiasi natura),**
- **aggressioni (di qualsiasi genere), atteggiamenti sospetti, falsificazioni varie**
- **denunce da parte della clientela (soprattutto se di natura patrimoniale)**
- **telefonate o scritti ostili, catene di S. Antonio, bufale digitali (hoax)**
- **abusi dell'utilizzo di Internet e della posta elettronica**
- **incidenti / attacchi / intrusioni di natura informatica / telematica**
- **autorizzazioni di accesso agli stabili o alle risorse IT non conformi alla funzione occupata**
- **alterazione / perdita di informazioni (cartacee ed elettroniche)**
- **tracce informatiche**
- **social network / spam / malware (virus e affini)**
- **phishing / social engineering**
- **viaggi all'estero**
- **...**

Il rischio sicurezza e il “fattore umano”

- **Il rischio zero o la sicurezza al 100%**
- **non saranno mai raggiungibile**
- **indipendentemente**
- **dagli investimenti fatti.**

- **Non è infatti una problematica esclusivamente**
- **TECNICA,**
- **ma soprattutto**
- **ORGANIZZATIVA**
- **e strettamente dipendente dal**
- **"FATTORE UMANO".**

Cosa fa BancaStato

- **Servizio sicurezza**

- **Business Continuity Management (BCM) e Stato maggiore di crisi (SM)**

- **Formazione / informazione / consapevolezza**

Servizio sicurezza BancaStato: missione

- **Assicurare la protezione**

- ***delle persone*** **(clienti, dipendenti e personale esterno),**
- ***delle informazioni*** **(in forma elettronica e non),**
- ***degli immobili*** **occupati dalla Banca,**
- ***delle infrastrutture e delle installazioni*** **(tecniche e IT) e**
- ***dei valori***

- **garantendone, per quanto applicabile singolarmente,**
- **un livello ottimale di**

- ***riservatezza*****,** ***integrità*** **e** ***disponibilità***

- **in conformità con la normativa vigente (interna ed esterna)**

Servizio sicurezza BancaStato: obiettivi

- **Garantire una sorveglianza e un controllo adeguati atti a prevenire / contenere il *rischio sicurezza*.**

- **Garantire il rispetto del segreto bancario, commerciale e professionale (obblighi contrattuali).**

- **Minimizzare altri rischi operativi e i rischi di ledere l'immagine e il buon nome della Banca.**

- **OBIETTIVI DA CONDIVIDERE DA PARTE DI TUTTI**

Servizio sicurezza BancaStato: macro-attività (estratto)

Prevenire / dissuadere

- - politica di sicurezza (parte integrante della politica di rischio della Banca)
- - normativa interna (regolamenti, direttive, ordini di servizio) ed esterna (compliance)
- - gestione incidenti / gestione rischi (analisi, valutazione, trattamento, misure, monitoraggio)
- - definizione / attuazione di misure preventive (organizzative, tecniche ed edilizie) per ridurre le probabilità di un incidente
- - definizione / attuazione di misure di protezione (organizzative, tecniche ed edilizie) per minimizzare le conseguenze di un incidente
- - profilo standard di autorizzazione (stabili + IT) per funzione DGRU
- - formazione, informazione, consapevolezza
- - ...

Controllare

- - sistema di controllo interno (controlli prioritari, controlli operativi)
- - controlli ex-ante, ex-post
- - ...

Contenere / Adeguare

- - definizione / attuazione di misure di tipo correttivo, adattativo ed evolutivo (org., tecniche ed edilizie)
- - ...

Business Continuity Management (BCM)

- **Cosa faremmo se...**

Business Continuity Management (BCM)

- Un Business Continuity Management (di seguito BCM) adeguato alle caratteristiche dell'azienda costituisce una precondizione per l'autorizzazione a esercitare l'attività.
- La responsabilità del BCM ricade sul CdA e sulla Direzione Generale (v. circolare FINMA "Sorveglianza e controllo interno", circ. FINMA 06/6).
- Secondo le raccomandazioni ASB in vigore il BCM deve contenere le seguenti componenti:
  - *Business Impact Analysis (standard minimo obbligatorio)*
  - *Business Continuity Strategy (standard minimo obbligatorio)*
  - *Business Continuity Planning*
  - *Business Continuity Testing*
  - *Organizzazione della gestione delle crisi (Stato Maggiore di crisi)*
  - *BCM Reporting*
  - *BCM Training*
  - *BCM Communication*
- Le raccomandazioni dell'ASB in materia di BCM devono essere implementate con efficacia (grado di copertura) ed efficienza (tempo e risorse impiegate), giustificabile in un'ottica costi/benefici sostenibile.

Business Continuity Management (BCM)

- **Il Business Continuity Management (BCM),**
- costituisce l'insieme delle misure organizzative, tecniche ed edilizie da realizzare
- nel caso in cui un evento a carattere eccezionale (disastroso, catastrofico, …)
- possa pregiudicare la continuità operativa corrente ("continuità aziendale")
- dei servizi bancari ritenuti prioritari (critici) e, di conseguenza, il servizio alla clientela.

- **Parlare di "continuità aziendale" significa occuparsi di:**
  - **pericoli** (incendi, allagamenti, approvvigionamento, eventi naturali, malfunzionamenti, danneggiamenti, attacchi, assenze di massa, ...)
  - **rischi** (inaccessibilità stabili, indisponibilità risorse)
  - **impatti** (disservizi, ritardi, perdite finanziarie, danni di immagine / di reputazione)
  - **risorse e processi aziendali** (risorse = collaboratori, informazioni, immobili, infrastrutture e installazioni tecniche/IT, provider esterni, outsourcing, key people/function)
  - **misure di sicurezza in essere** (organizzative, tecniche ed edilizie)
  - **misure d'urgenza da attuare** (definite caso per caso)

Business Continuity Management (BCM): i pericoli

- **Incendi** (stabili / aree critiche)
- **Allagamenti** (stabili / aree critiche)
- **Approvvigionamenti** ("provider" energia / telecomunicazione / trasporti / denaro)
- **Eventi naturali** (terremoti, esondazioni, …)
- **Malfunzionamenti** (infrastruttura IT, hardware e software)
- **Danneggiamenti** (vandalismi, malversazioni, errori, inadempienze)
- **Attacchi** (dall'esterno / dall'interno, IT / fisici)
- **Pandemia** (assenze di massa / in ambiti specifici)

Business Continuity Management (BCM): i rischi

- **Inaccessibilità degli stabili**

- **Indisponibilità dei sistemi IT**
- **Indisponibilità delle applicazioni IT**
- **Indisponibilità dell'infrastruttura IT**

- **Indisponibilità delle informazioni (cartacee / elettroniche)**

- **Indisponibilità della rete Bancomat**
- **Indisponibilità della rete telefonica (interna / esterna)**
- **Indisponibilità di Internet**

- **Assenza delle persone**

- **...**

Business Continuity Management (BCM): gli impatti

- **Interruzione di uno o più servizi alla clientela**
- **Disservizi / ritardi verso la clientela / il fronte**
- **Danni di immagine / di reputazione**
- **Perdite finanziari / aumento costi**
- **Conseguenze legali / penali**
- **...**

Business Continuity Management (BCM): le misure

- Misure antincendio / Divieto di fumare
- Piani di evacuazione
- Generatori / Gruppi di continuità
- Centro EDP di backup
- Backup dei dati
- Ridondanza rete IT
- DMZ, IDS/IPS, soluzioni anti-malware
- Controllo e traccia accessi (stabili e IT)
- Videosorveglianza
- Servizio sanitario aziendale
- Centrale sorveglianza / Centrale allarmi
- Servizio sicurezza / Servizio picchetti
- Direttive interne / ordini di servizio / istruzioni tecniche
- Contratti / SLA terze parti
- Profilo collaboratori
- Formazione e informazione collaboratori
- ...

La problematica della “continuità aziendale”

- **Obiettivi della “continuità aziendale”:**
- **Sopravvivere (restare nel “business”)**
- **Evitare / limitare le conseguenze**
- **Reagire su base pianificata**
- **Ripristinare nel minor tempo possibile**
- **La problematica della “continuità aziendale” non è di competenza dei soli tecnici, ma deve essere affrontata a livello del “management” dell’azienda**
- **I requisiti chiave devono essere decisi dal “business”**

La problematica della “continuità aziendale” (2)

- **I primi passi da muovere:**

- **Creare consapevolezza sulla problematica**

- **Capire il proprio “business” e le sue criticità / i suoi punti deboli**
  (in termini di persone, di processi, di infrastrutture,...)

- **Capire da cosa bisogna proteggersi (identificazione eventi “catastrofici”)**
- **Capire i rischi a cui si è confrontati (gestione dei rischi “business”)**
- **Capire gli impatti a cui si va incontro (analisi degli impatti “business”)**

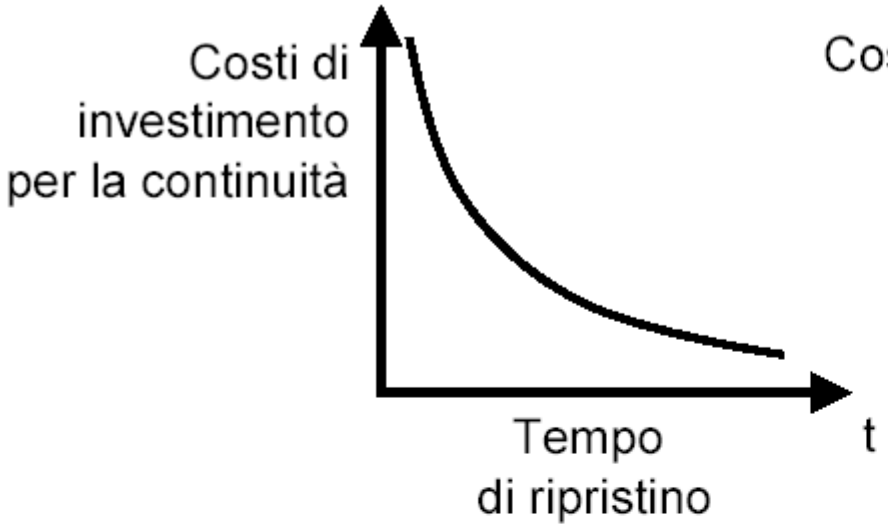
- **Definire e implementare le misure di sicurezza necessarie**

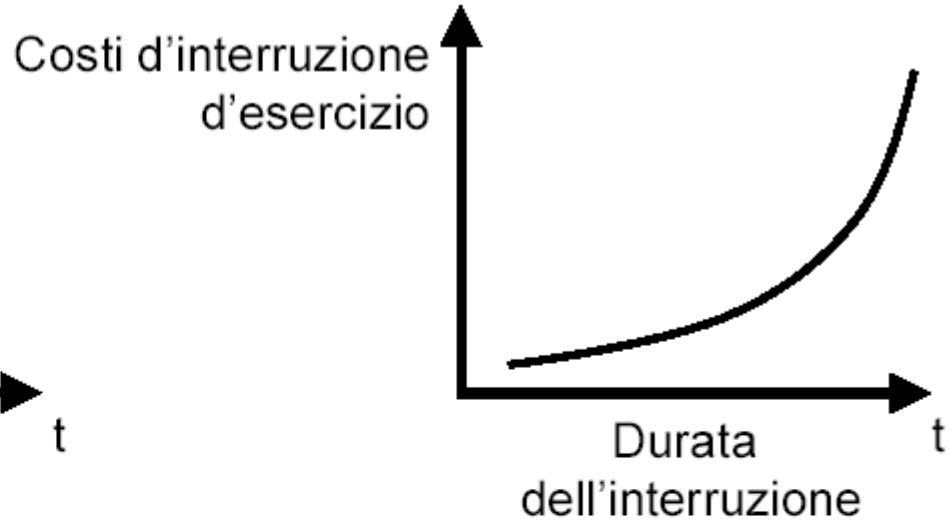
- **Definire le misure di urgenza (per poi attuarle secondo necessità)**

La problematica della “continuità aziendale” (3)

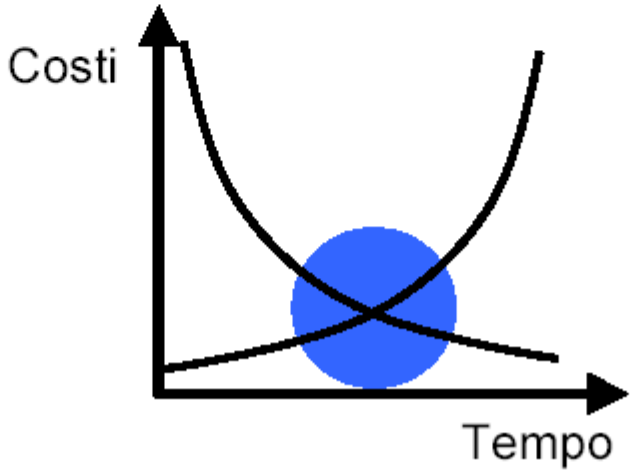
- **Analisi costi / benefici, compromesso tra:**
- **costi e investimenti per la continuità**
- **vs.**
- **costi d’interruzione della continuità di esercizio / costi di ripristino**

La problematica della continuità aziendale (4)





PREVENZIONE



REAZIONE

La problematica della continuità aziendale (5)

- **Due misure temporali fondamentali:**

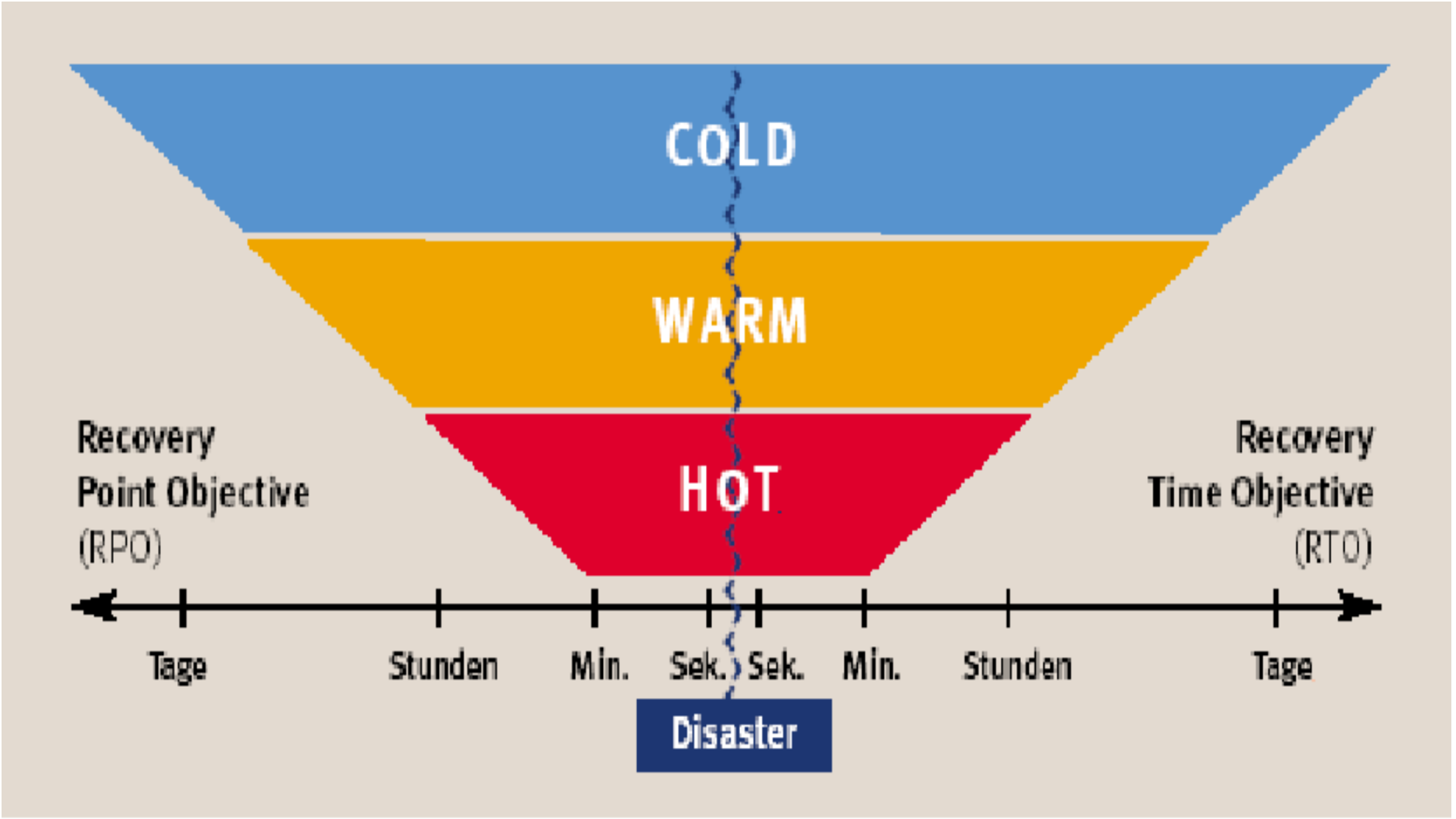
- **RPO (Recovery Point Objective)**
- Obiettivo: i dati aziendali critici non possono essere più vecchi di un certo tempo definito, indicato come RPO.

- Corrisponde a: intervallo di dati persi (lost-data)

- **RTO (Recovery Time Objective)**
- Obiettivo: in un certo tempo definito, indicato come RTO, i sistemi IT critici per il business (sistemi, applicazioni e dati) vengono ripristinati.

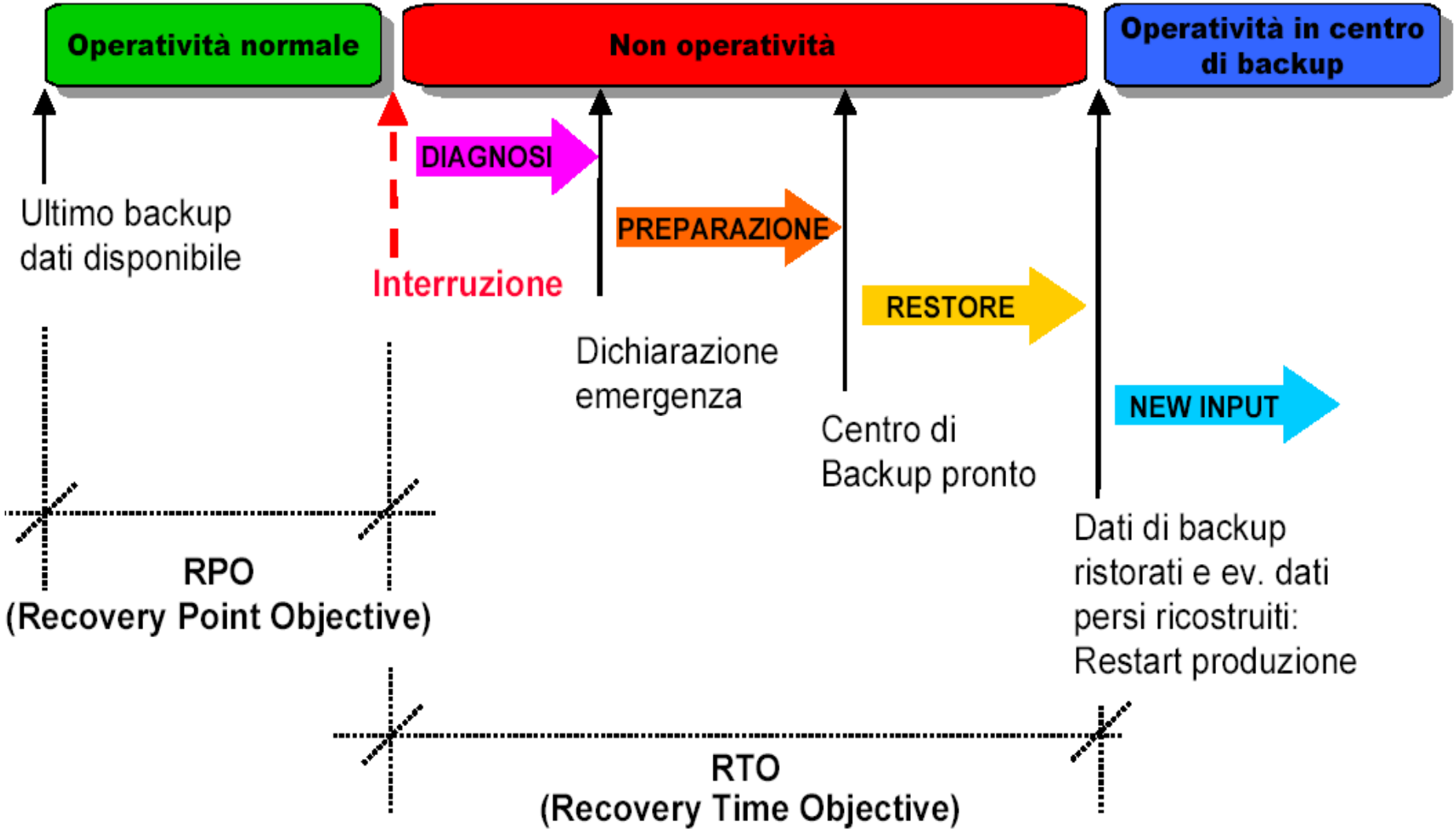
- Corrisponde a: intervallo di non disponibilità (down-time).

La problematica della continuità aziendale (6)



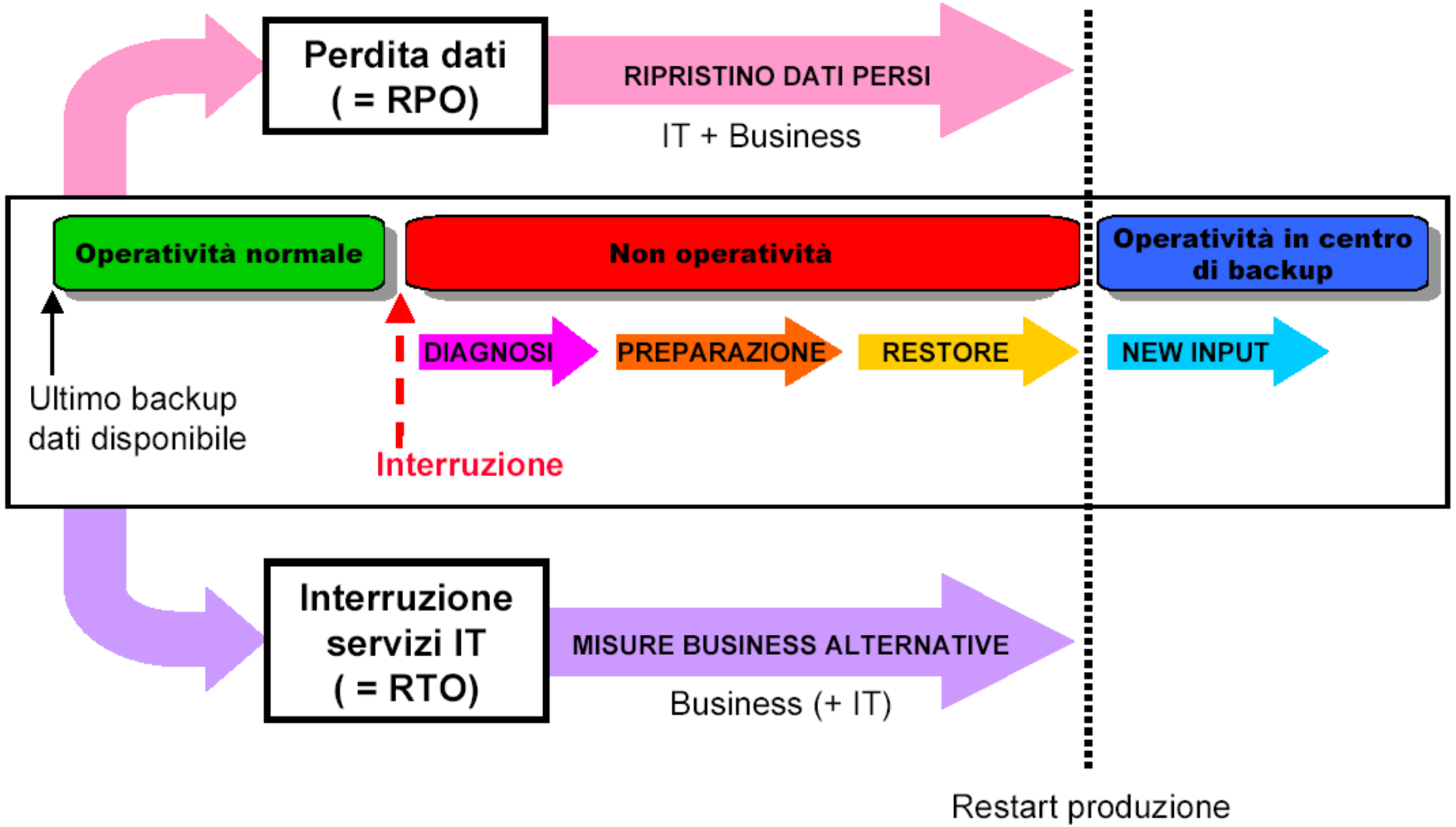
Analisi temporale degli eventi in caso di disastro (1)

Il punto di partenza: gli eventi



Analisi temporale degli eventi in caso di disastro (2)

La dimensione chiave: il business



Analisi temporale degli eventi in caso di disastro (3)

Classi di continuità e soluzione tecnica

Classe 1 (0 < RPO, RTO < alcune h)	2. centro di calcolo (hot standby) Infrastruttura in- o outsourced Mirroring dei dati
Classe 2 (RPO=4h, RTO=8-24h)	2. centro di calcolo (warm standby) Infrastruttura in- o outsourced Mirroring dei dati
Classe 3 (RPO=24h, RTO=72h)	2. centro di calcolo (cold standby) Spesso outsourced Standard recovery da tape
Classe 4 (RPO=24h, RTO alcuni d)	2. centro di calcolo (cold standby) “Quick-ship” program Standard recovery da tape

Come procedere: un possibile modello

Ciclo di vita del Business Continuity Management (BCM):

- **Capire il proprio "business"**
- **Identificazione e analisi dei rischi ("risk assessment")**

- **Analisi di impatto "business"**
- **(processi *critici* – risorse/sistemi *critici* correlati ai processi *critici*)**
- **Strategia di continuità del "business"**
- **(approccio hot/warm/cold, periodo *critico* di ripristino accettabile, approvazione da parte della Direzione)**
- **Sviluppo e implementazione del piano di continuità**
- **(SM crisi / Chi decide cosa / Chi avvisa chi, quando e come / Quali sono le priorità / Quali sono le misure di urgenza da sganciare, Compiti, Tempi, …)**
- **Test (pianificazione / esecuzione)**
- **Monitoraggio/aggiornamento**

- **Riattualizzazione dei rischi**
- **Creare e diffondere una "cultura BCM"**

Business Continuity Management (BCM)

- **Incident Management <> Business Continuity Management**
- IM: un'interruzione della continuità del servizio normalmente erogato alla clientela < di 4 ore
- BCM: un'interruzione della continuità del servizio normalmente erogato alla clientela > di 4/6 ore

- **I servizi da considerare come prioritari possono essere i seguenti (esempi):**
  - casse
  - traffico pagamenti
  - borsa e tesoreria
  - contabilità finanziaria
  - registro centrale / segretariato clienti
  - amministrazione titoli
  - amministrazione crediti
  - ...

Business Continuity Management (BCM)

- **Eventi ritenuti (rischi mitigati BCM)**
- - inaccessibilità servizio traffico pagamenti
- - inaccessibilità servizio borsa e tesoreria
- - inaccessibilità stabile Sede
- - inaccessibilità stabile succursale o agenzia
- - indisponibilità centro EDP
- - indisponibilità rete IT stabile Sede
- - indisponibilità rete IT stabile Succursale o Agenzia
- - indisponibilità applicativi IT prioritari
- - pandemia, ...

Stato Maggiore di crisi + Piani d'azione BCM

- **Eventi non considerati (rischi assunti BCM)** — **Stato Maggiore di crisi**
- - più eventi, tra quelli considerati, che si verificano contemporaneamente o a cascata
- - indisponibilità del centro EDP principale e di quello di backup contemporaneamente
- - ...

- **Altri eventi straordinari (non BCM)** — **Stato Maggiore di crisi**
- (intesi come situazioni di emergenza che richiedono decisioni critiche urgenti e che esulano dalle normali competenze direttive e decisionali e non possono essere gestite con i mezzi ordinari (ad es. situazioni di crisi economica internazionale, di cambiamenti repentini dei tassi d'interesse, dei tassi di cambio,…)

Formazione / informazione / consapevolezza

- **Adempiere agli obblighi di segretezza, trasparenza, vigilanza e discrezione, rispettando il segreto bancario, professionale e commerciale.**
- Legge federale sulle banche e le casse di risparmio, LBCR 952.0 – art. 47: segreto bancario, art. 43: segreto professionale
- Legge federale sulle borse e il commercio di valori mobiliari, LBVM 954.1 – art. 43: violazione del segreto professionale
- Legge federale sulla protezione dei dati, LPD 235.1 – art. 35: violazione dell'obbligo di discrezione
- Codice penale, RS 311.0 – art. 273: spionaggio economico – art. 162 violazione del segreto di fabbrica o commerciale

- **Condividere gli obiettivi del Servizio sicurezza in materia di sicurezza (riservatezza, integrità, disponibilità).**
- **Collaborare attivamente (essere proattivo e non solo reattivo).**
- **Attenersi alla normativa interna in essere (regolamenti, DI e OS).**
- **Tutti i collaboratori sono responsabili di garantire la protezione delle informazioni aziendali che gestiscono.**

Formazione / informazione / consapevolezza

- **Massimo riserbo sulla clientela.**
- **Professionalità e discrezionalità >>> qualità del servizio.**
- **La prudenza e l'attenzione non sono mai troppe.**
  - essere sufficientemente diffidenti e ragionevolmente prudenti nei confronti di situazioni anomale (comunicare a chi di dovere ogni situazione sospetta)
- **Identificare l'interlocutore (richiedente/destinatario)**
  - non comunicare informazioni aziendali (anche se non riservate) a sconosciuti
  - verificare che colleghi che vi richiedono informazioni siano autorizzati a riceverle
- **Adottare il principio che "E' vietato tutto quello che non è permesso".**
  - spesso invece si lavora con il presupposto che "E' permesso tutto quello che non è vietato"

Formazione / informazione / consapevolezza

- **Essere prudenti e attenti in ogni circostanza.**
- **Tenere in debito conto il rischio effettivamente assunto.**
- (valutare le possibili conseguenze nel dire e nel fare, nei comportamenti assunti, nell'utilizzo quotidiano del telefono, del telefonino, del fax, del PC, del portatile, delle agende elettroniche, di Internet e della posta elettronica, ...)
- **Evitare lo "voci di corridoio" e le "chiacchiere da bar".**
- **Conoscere e rispettate la normativa in vigore.**
- **Tenersi informati / Richiedere informazioni.**

Domande?

- **Domande?**

If you think education is expensive, try ignorance.

Anonimo

Un insegnante
può aprirvi la porta,
ma sta a voi varcarne la soglia.

Proverbio latino

L'uomo che non fa errori
di solito non fa niente.

E. Phelps