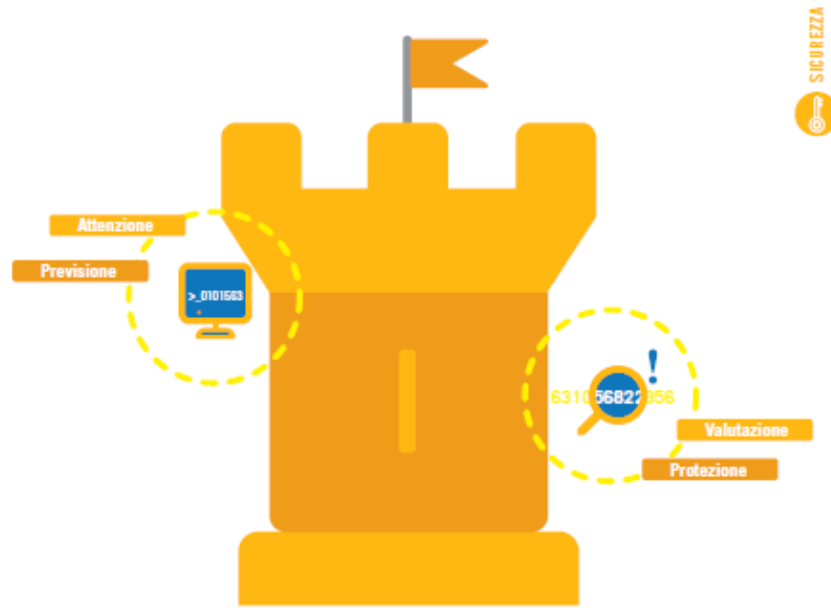




www.prb.it



Banche e Sicurezza

ABI - Roma – Palazzo Altieri – 28,29 Maggio 2012

Dematerializzazione documenti e sicurezza

una realizzazione sicura, attenta alla persona

Antonio Carbonera
Partner, Responsabile Tecnico PRB
antonio.carbonera@prb.it

Sicurezza

(secondo Wikipedia)

dal latino "sine cura": senza preoccupazione

"conoscenza che l'evoluzione di un sistema non produrrà stati indesiderati"

cioè:

«sapere che quello che faremo non provocherà danni»

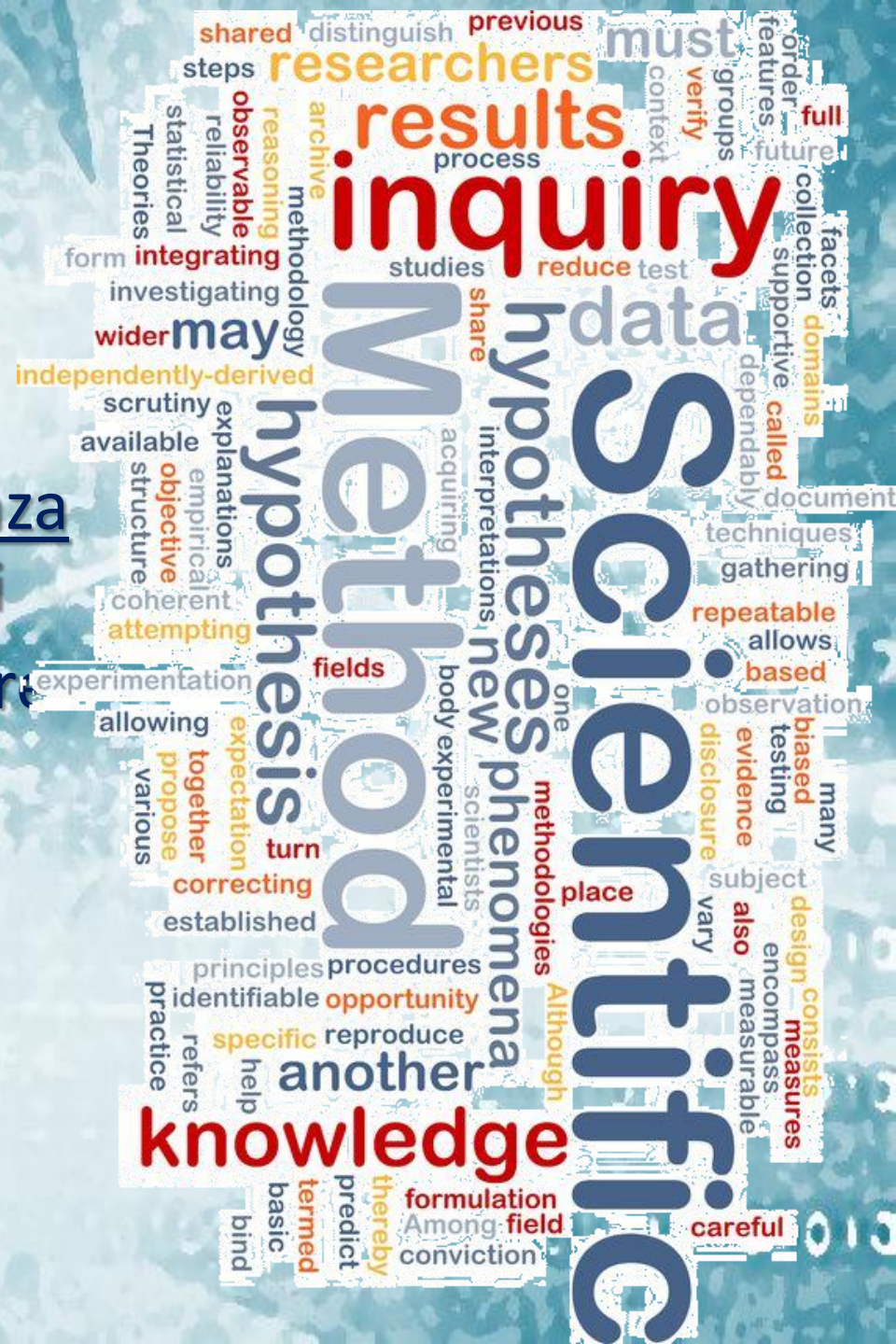


SICUREZZA

La conoscenza è
fondamentale:

Un sistema può evolversi senza
dar luogo a **stati indesiderati**
Ma non per questo può essere
ritenuto sicuro

Una conoscenza di tipo
scientifico, basata su
osservazioni ripetibili,
garantisce una valutazione
sensata della sicurezza



SICUREZZA e PERSONA

In un ambiente sicuro:

- La persona produce meglio e di più



**La sicurezza è essenziale per
aumentare produttività
e benessere**

OGGI

Per questo motivo, il centro di questa presentazione non sono gli *010011010101*.

Guarderemo:

- non solo la «macchina» (aspetto tecnico)
- ma la «persona» (aspetto umano)



Programma gestionale

Sistema Operativo

OGGI

Saremo guidati dall'esempio reale di una Tecnologia
sì innovativa
ma realizzata da anni
lungamente verificata «sul campo»

DDD DataPicker®

attraversando le logiche della «dematerializzazione»
e valutando qualche aspetto psicologico

La macchina è funzionale alla persona

VANTAGGI

2012 = DEMATERIALIZZARE



Il recente Forum ABILab
ha indicato il 2012 come

- “anno della dematerializzazione”

DEMATERIALIZZARE

Vuole dire (nella concezione più evoluta)

«**Far circolare digitalmente i documenti**»

- Fa trovare sempre i documenti
- Aumenta l'efficienza
- Riduce i tempi operativi
- Riduce i costi operativi (meno 70-90%)

Rende facile e immediato l'accesso ai documenti

EVENTI INDESIDERATI

La facile disponibilità dei documenti è un vantaggio
ma **espone a rischi:**



- Accesso non autorizzato
- Accesso di personale tecnico esperto
- Copia di documenti
- Comunicazione a persone malevoli
- Lavorazioni improprie (*fuori normative*)
- Contraffazione di contenuti

DEMATERIALIZZARE È ANCHE UTILE

- Bancomat esploso, filiale semidistrutta**
- Correntista presenta fax di accredito contraffatto**
- Impiegato invia all'esterno documenti riservati**

Sono alcuni «casi» vissuti da banche clienti PRB

PROCESSI ORGANIZZATIVI

La situazione è ancora più delicata se, oltre che “documenti”, si gestiscono “processi”:

- Selezione dei documenti più semplice



- Storia più completa
(le pratiche la raccontano nel dettaglio)
- Funzionalità più critica (se si ferma l'applicazione si ferma ogni attività della Banca)

CONFERME

Diversi relatori di questo convegno ieri hanno affermato che la «dematerializzazione comporta rischi»:

- *Andrea Agosti* di NTT DATA
- *Gianluigi Molinari* di Intesa San Paolo
 - *Romano Stasi* di ABI Lab

CRITICITÀ AGGIUNTIVA

Per PRB il problema è più critico, poiché dal 2007 propone:

- **L'accordo di "Success-Fee"**
 - Ogni onere e rischio assunto da PRB
 - Ritorno pari a una percentuale sul risparmio
 - Liquidazione dopo aver ottenuto il risparmio

Quindi, se la Banca non ottiene risparmio ma danno, per PRB non c'è ritorno

CONTROMISURE



applicazione
sicura
per gestire
documenti
dematerializzati
e processi organizzativi

alcune considerazioni con
un'ottica lato utente

SICUREZZA NELLA FUNZIONALITÀ

(SICUREZZA "BY DESIGN")

- Specifiche di progettazione
- Tracciatura puntuale delle fasi progettuali
- Verifiche e liste di riscontro rispetto specifiche
- Validazione accurata
- Business Continuity
- Test su campo
- Sistema di tracciatura automatica degli errori
- Statistica

(Criteri di sicurezza previsti all'inizio del progetto: modifiche successive rendono fragile l'architettura)

Impatto psicologico: mi posso fidare del sistema

SICUREZZA NELLA FUNZIONALITÀ

(SICUREZZA "BY DESIGN")

- Flow di progettazione



SICUREZZA NELLA FUNZIONALITÀ

(SICUREZZA “BY DESIGN”)

- **Specifiche di progettazione**

Linee guida per i commenti del codice sorgente

Buoni commenti e significativi, rendono il codice sorgente maggiormente manutenibile. Sempre.

Tutti i commenti devono essere scritti in lingua inglese.

Regola d'oro per i commenti: scrivere codice leggibile

Uno dei principi base per ogni sviluppatore è quello di far sì che il codice sia autoesplicativo. Questa regola non deve portare a non commentare il codice, bensì ad utilizzare i commenti in modo intelligente.

Commentare il codice mentre si scrive

Aggiungere i commenti mentre si scrive il codice e il suo significato è fresco in memoria. Lasciando i commenti alla fine, richiederà il doppio dell'impegno. “Non avevo tempo per i commenti”, “Avevo fretta”, “Il progetto era già in ritardo...” sono solo alcune delle scuse che ci troviamo per non commentare il codice. Il commento potrebbe addirittura anticipare la scrittura del codice, come promemoria di ciò che dovremo scrivere.

Ad esempio:

```
public void ProcessOrder()  
{  
    // Make sure the products are available  
    // Check that the customer is valid  
    // Send the order to the store  
    // Generate bill  
}
```

SICUREZZA NELLA FUNZIONALITÀ

(SICUREZZA "BY DESIGN")

- Tracciatura puntuale delle fasi progettuali

Visione struttura Processi - Fasi © Prb

Area Organizzativa con i *Processi* contenuti e relative Fasi.

- Area: **Progettazione**

- *Processo: Progettazione software*

- ❖ Idea prodotto
 - ❖ Approvazione R. Tecnico
 - ❖ Approvazione R. Sviluppo Clienti
- ❖ Macroanalisi
 - ❖ Approvazione R. Tecnico
- ❖ Bozza di Listino
 - ❖ Controllo R. Sviluppo software
 - ❖ Controllo R. Assistenza
- ❖ Assegnazione Progetto
 - ❖ Approvazione R. Tecnico
 - ❖ Assegnazione a più Progettisti
- ❖ Progettazione - documentazione utente
- ❖ Progettazione - documentazione master
- ❖ Progettazione - documentazione tecnica
- ❖ Proposta sviluppo Prodotto
 - ❖ Approvazione R. Tecnico e R. Sviluppo
- ❖ Controllo Qualità documentazione
- ❖ Ricerca e scelta dei Componenti
- ❖ Realizzazione sw
- ❖ Completamento liste di validazione
- ❖ Test di laboratorio
- ❖ Messa a punto delle Tracce diagnostiche
- ❖ Validazione sw
- ❖ Scelta dei Clienti di test

SICUREZZA NELLA FUNZIONALITÀ

(SICUREZZA "BY DESIGN")

- Liste di riscontro sul rispetto specifiche

Specifiche di progetto software

Data e ora di creazione

Oggetto Specifiche di progetto software

Il progettista verifica la completezza di tutte le attività necessarie alla chiusura del progetto.

Standard rispettati

- L'interfaccia utente rispetta le linee guida Microsoft (documento [UserInterfaceTextGuideLines](#)).
- Lo standard IQA per la digitalizzazione degli assegni è stato rispettato.
- 12207 *IS Software life cycle processes*
- Norma ISO 9000/3

Architettura dell'applicazione

- Le applicazioni sono compatibili per l'utilizzo sui sistemi operativi Microsoft Windows Vista e Windows 7 (gestione UAC).
- Le istruzioni di controllo di flusso *Switch (Select) ... Case* prevedono un'uscita di default.
- L'utente con cui è eseguita l'applicazione o il servizio è iscritto in GDD.
- L'applicazione gestisce in modo controllato e avvisa quando l'utente non è iscritto in GDD.
- Il progetto è concepito in modo modulare facendo uso delle tecniche di programmazione ad oggetti (in modo che i moduli possano essere riutilizzati in altri progetti).
- Il progetto è ottimizzato per l'esecuzione su reti lente e instabili.
- L'applicazione è progettata per elaborare solo i dati necessari (*ad esempio evitare query SELECT **).
- L'applicazione supporta la tracciatura della propria attività.
- L'applicazione gestisce in modo controllato (senza chiusure improvvisate) le eccezioni (errori non previsti).
- Le registrazioni diagnostiche sono in inglese.
- L'applicazione è concepita per essere scalabile.
- L'applicazione è concepita per supportare tecniche di [load-balancing](#).
- I moduli dell'applicazione sono concepiti per garantire un basso livello di accoppiamento (facilità di riuso).

SICUREZZA NELLA FUNZIONALITÀ

(SICUREZZA "BY DESIGN")

- Liste di validazione accurate

Lista di validazione

Funzione	Risultato Atteso	Risultato ottenuto
<i>Selezionare i processi da visualizzare nell'albero</i>		
Avviare l'applicazione	L'applicazione si avvia e l'albero DDD presenta solo il livello "Pausa".	2 Finestra Leggere Procedure e Istruzioni
	Automaticamente si apre la mappa per selezionare le Aree Funzionali. È presente una lista con le aree funzionali nello stesso ordine dei fogli nel documento di analisi di MS Excel. Nessun area funzionale è selezionata	OK
Premere Annulla	La mappa si chiude e resta attiva la mappa principale. Nell'albero è presente solo il Processo "Pausa"	OK
Premere il pulsante per selezionare le aree funzionali presente sulla barra degli strumenti	Si apre la mappa per selezionare le Aree Funzionali	Nella sezione pratiche, l'applicazione propone aree organizzative OK
Premere la X rossa presente sulla barra del titolo	La mappa si chiude e resta attiva la mappa principale. Nell'albero è presente solo il Processo "Pausa"	OK
Premere il pulsante per selezionare le aree funzionali presente sulla barra degli strumenti	Si apre la mappa per selezionare le Aree Funzionali	OK vedi sopra
Premere Conferma	Un messaggio indica che non sono state selezionate aree funzionali	OK
Premere No	Il messaggio scompare. La mappa si chiude e resta attiva la mappa principale. Nell'albero è presente solo il livello "Pausa"	NO. Il messaggio scompare ma la mappa principale risulta disattivata.
Premere il pulsante per selezionare le aree funzionali presente sulla barra degli strumenti	Si apre la mappa per selezionare le Aree Funzionali	OK vedi sopra
Premere Conferma	Un messaggio indica che non sono state	OK

SICUREZZA NELLA FUNZIONALITÀ

(SICUREZZA "BY DESIGN")

- **Business Continuity**
- **La sicurezza dell'applicazione dipende anche dall'architettura di rete nella quale il sistema è inserito**
- **BC prevede sistemi ridondati per garantire continuità nel servizio**



SICUREZZA NELLA FUNZIONALITÀ

(SICUREZZA "BY DESIGN")

- **Test effettivo sul campo**
(anni 2010 - 2011)

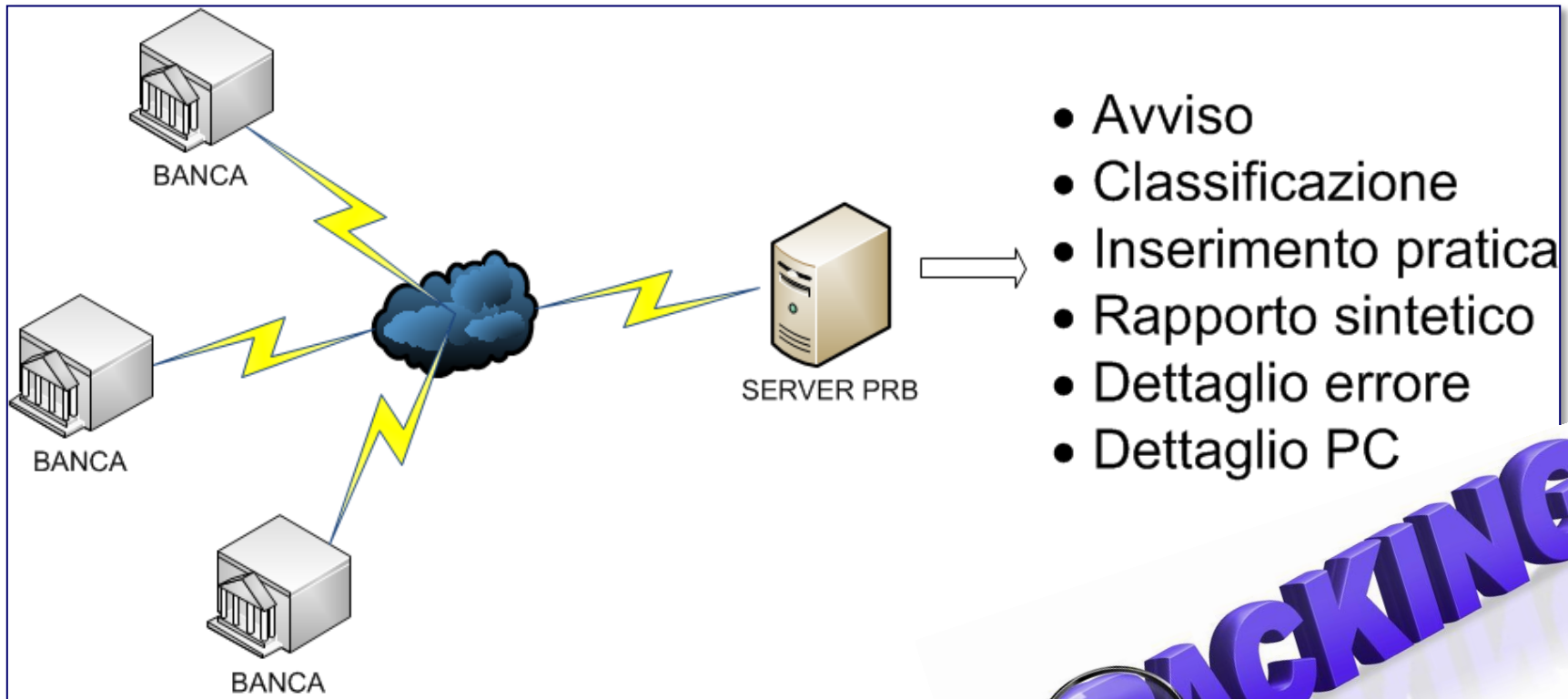
A laboratory setting with a rack of five test tubes containing blue liquid. A pipette is dispensing a drop of yellow liquid into the rightmost test tube. The background is a blurred laboratory environment.

***UniCredit
Intesa San Paolo
Banca di Inzago
Banca di Pistoia***

SICUREZZA NELLA FUNZIONALITÀ

(SICUREZZA "BY DESIGN")

- Tracciatura e inoltro automatico degli errori



TRACKING

*Impatto psicologico:
non perdo tempo, è tutto sotto controllo*

SICUREZZA NELLA FUNZIONALITÀ

(SICUREZZA "BY DESIGN")

Tracciatura e catalogazione automatica degli errori

*Impatto psicologico:
mi posso fidare del sistema*

ERROR

Report segnalazioni

Data e ora di creazione 15/05/2012 10:30
Oggetto 15/05/2012 - 10:30 - Report segnalazioni

Situazione generale
Sono state rilevate 1 anomalie che necessitano attenzione.

Elenco anomalie rilevate

Legenda:

- Procedura: procedura che ha sollevato l'anomalia;
- P: gravità della segnalazione;
- PG: peso giornaliero, indica la gravità della segnalazione per gli utenti;
- PM: peso mensile, indica la gravità della segnalazione per gli utenti;
- OS: Sistemi operativi installati sulle macchine che hanno inviato il .NET, Framework .NET installati sulle macchine che hanno inviato;
- Descrizione: Descrizione dell'anomalia;
- Clienti: Clienti presso cui si è verificata l'anomalia.

Applicazione: Editore GDD

Procedura	P	PG	PM	OS	.NET
Editore GDD - Applet.Main	22	1453	12312	Microsoft Windows 7 Professional - Service Pack 1 Microsoft Windows 7 Ultimate N - Service Pack 1 Microsoft Windows XP Professional - Service Pack 3 Microsoft Windows 7 Enterprise - Service Pack 1	3% 3.5.30729.01 2% 2.2.30729.01 95% 3.5.30729.5420 2% 3.0.30729.5420 2% 3.0.30729.01 99% 2.0.50727.01 420

Documento notificato a:
H.L.PDSK - Utente Virtuale Assistenza
GARAR0499 - Roberto Garavaglia

Questo modulo è inserito:

- Nel Processo Generazione Report
- Nella fase Generazione report
- Nella Pratica 2012 maggio - Report segnalazioni

Componenti della Pratica: PRB, PRB SMI

Tipo Documento REPORT - Report segnalazioni automatiche

Livello di riservatezza 20

Scopo del modulo: il servizio di generazione automatica dei report applicazioni PRB installate presso i Clienti

Report segnalazioni

Data e ora di creazione 15/05/2012 14:01
Oggetto 2012/05/15 - 14.01.15 - Segnalazione - Configuration

Dettagli della segnalazione

Nome dell'applicazione: DDD

Categoria dell'anomalia: Configuration
Procedura che ha generato l'anomalia: Updater.getObjectUpdates
Descrizione dell'anomalia: Update on WS fails: try to get updates from DB

Livello di priorità: 65
N° di segnalazioni nell'ultimo mese: 15

Sistemi operativi interessati:

- 47% Microsoft Windows 7 Professional - Service Pack 1
- 5% Microsoft Windows 7 Ultimate N - Service Pack 1
- 15% Microsoft Windows XP Professional - Service Pack 3
- 21% Microsoft Windows 7 Enterprise - Service Pack 1
- 10% Microsoft Windows Vista, Business - Service Pack 1

Framework .NET installati:

- 10% 3.0.30618.00
- 26% 3.5.30729.01
- 10% 2.0.50727.3053
- 15% 2.2.30729
- 73% 3.5.30729.5420
- 73% 2.0.50727.5420
- 15% 3.2.30729
- 73% 3.0.30729.5420

Clienti presso cui si è verificata:

██████████
██████████
██████████

Elenco segnalazioni

Informazioni complete della segnalazione	File di log della segnalazione
Log segnalazione 520196	Log segnalazione 520196
Log segnalazione 537725	Log segnalazione 537725
Log segnalazione 537477	Log segnalazione 537477
Log segnalazione 535592	Log segnalazione 535592
Log segnalazione 535572	Log segnalazione 535572
Log segnalazione 535211	Log segnalazione 535211
Log segnalazione 534953	Log segnalazione 534953
Log segnalazione 518383	Log segnalazione 518383
Log segnalazione 518334	Log segnalazione 518334
Log segnalazione 518966	Log segnalazione 518966

- Avviso cifrato
- Classificazione (tipologia)
- Rapporto sintetico
- Creazione/inserimento pratica

SICUREZZA NELL'ACCESSO

Alla procedura:
controllato con modalità
sicure

Ai documenti:
autorizzazioni di visibilità e
competenza nel profilo
utente



- *Tracciatura delle attività*
- *Allarmi real-time*

Particolare cautela se l'accesso avviene da utenti «esterni» (ad esempio clienti)

Deterrente psicologico: vengo subito individuato

SICUREZZA NELL'IDENTIFICAZIONE

La sicurezza del sistema informatico è legata alla sicurezza del sistema operativo con la quale si integra

Ma l'applicazione di gestione documenti può cadere in tranelli.....

- Identificazione dell'utente
 - ✓ login sicuro
- Identificazione utente esterno
 - ✓ protocolli sicuri

SICUREZZA NELLE AUTORIZZAZIONI



- Accesso limitato a insiemi di documenti e informazioni
- Consenso solo a utenti autorizzati
- Specifici privilegi utente

SICUREZZA NEI POTERI

La profilatura
garantisce visibilità:

Orizzontale per ambito

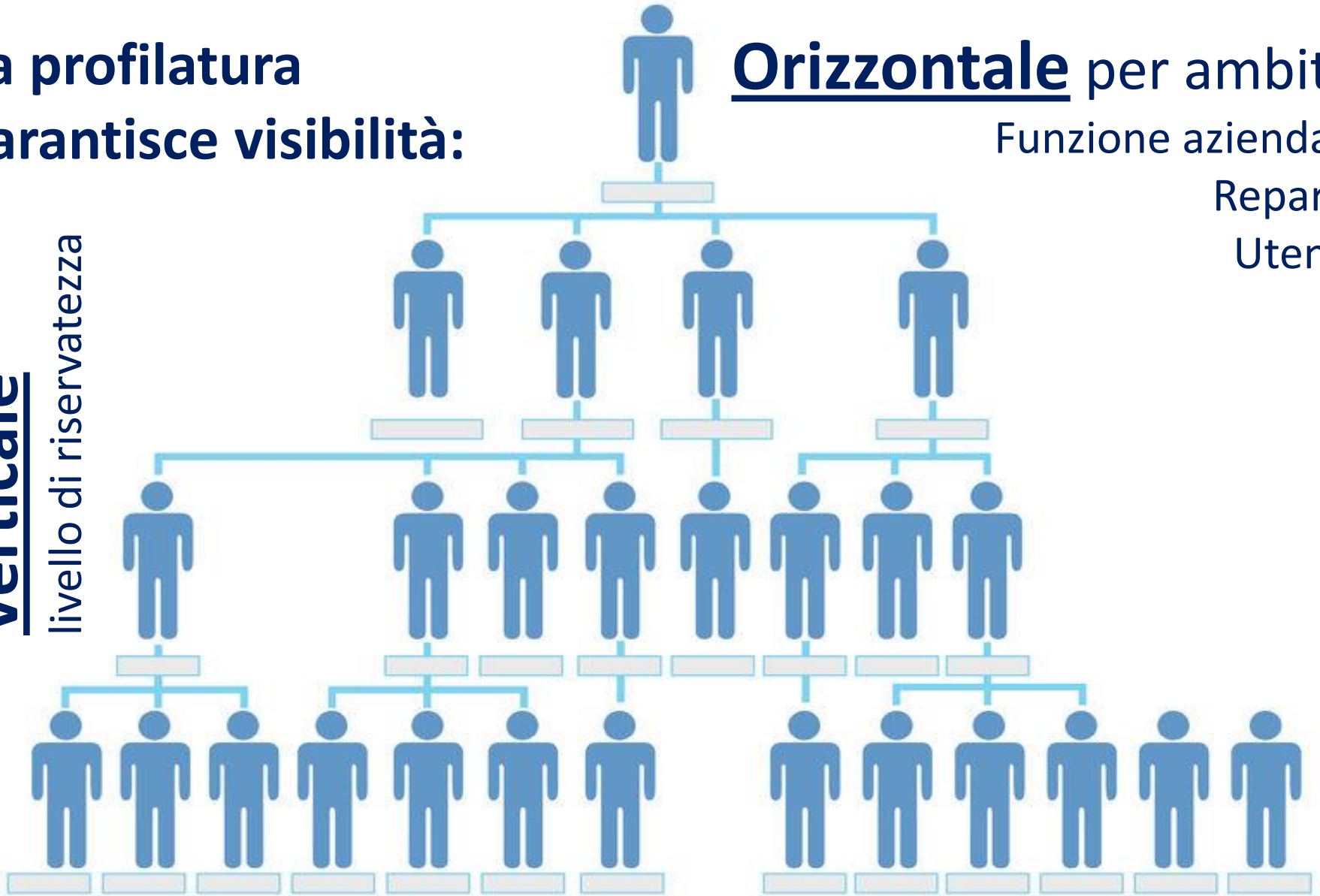
Funzione aziendale

Reparto

Utente

Verticale

livello di riservatezza



Impatto psicologico: so che ognuno vede solo quello che serve

SICUREZZA NEI PRIVILEGI

E anche privilegi operativi:

- Leggere e aggiornare informazioni e documenti
- Creare nuovi documenti
- Creare documenti aggiornabili
- Spedire messaggi all'esterno dell'organizzazione
- Avanzare le pratiche
- Fissare impegni sull'agenda
- Verificare le visibilità utente
- Estrarre statistiche e cruscotto direzionale
- Collegare/scollegare pratiche
- Estrarre i contenuti dei processi (procedure, moduli, istruzioni)










Impatto psicologico: ho quello che mi serve per lavorare bene

SICUREZZA NEL WORK-FLOW

DI DOCUMENTI E PRATICHE

- Non solo delle codifiche
- Tracciatura puntuale delle operazioni
- *Flessibilità operativa.....*
 - *Sicurezza di poter affrontare qualsiasi situazione imprevista*
- *ma possibilità di controllo (tracciatura attività)*

 **Storia**
Storia del documento ('Work-flow')
In grassetto gli indici aggiuntivi creati sul documento principale

▲	Data e Ora	Mittente	Destinatario	Stato
	13/01/2011 16:18...	XXXXXXXXXX - PRB	CONSORZIO ABI LAB	Nuovo (Pratica Portale ABILAB)
	13/01/2011 16:18...	XXXXXXXXXX - PRB	CONSORZIO ABI LAB	Spedito
	13/01/2011 16:26...	XXXXXXXXXX - PRB	CARBA0486 - PRB	Notificato
	13/01/2011 17:31...	XXXXXXXXXX - PRB	CONSORZIO ABI LAB	Collegato nella Pratica 'ABI LAB - PRB pa...
	13/01/2011 17:31...	XXXXXXXXXX - PRB	CARBA0486 - PRB	Vistato
	27/01/2011 15:43...	XXXXXXXXXX - PRB	PANCP0188 - PRB	Letto

Impatto psicologico: devo stare attento a quello che faccio

SICUREZZA NELL'INTEGRITÀ

Dei documenti

- ✓ Algoritmi di cifratura (*AES 256bit*)
- ✓ Firma digitale e marca temporale per i più importanti

Dei dati collegati

- ✓ Cifrati e con codici di controllo, per evitare manomissioni

Impatto psicologico: sono sicuro di quello che vedo

SICUREZZA SICURA®

nell'accesso ai documenti

- **Basata su più hardware che lavorano in collaborazione**

Rendono virtualmente impossibile ogni accesso illegale ai documenti

*Impatto psicologico:
sono sicuro anche per i
documenti più delicati*

A glass bottle with a cork, partially buried in sand, with a rolled-up document inside. The bottle is tilted, and the document is visible through the opening. The background is a clear blue sky.

**SICUREZZA
CHE UN
DOCUMENTO
NOTIFICATO
ALL'ESTERNO
RESTI
RISERVATO**

Quando si fornisce un documento
a una persona esterna
..... non si sa che «giro» farà.

Forse il giro del mondo!

La funzionalità di *Notifica Sicura*[®]
ottiene che solo la persona giusta
lo possa vedere.

(Brevetto PRB)

SICUREZZA NELLA COMPLIANCE

la Banca è come una “fabbrica”

- Tutti gli utenti fanno parte di un “ciclo” produttivo

Il ciclo deve essere:

facilitato

(istruzioni e procedure contestuali)

evidenziato

(processo organizzativo)

controllato

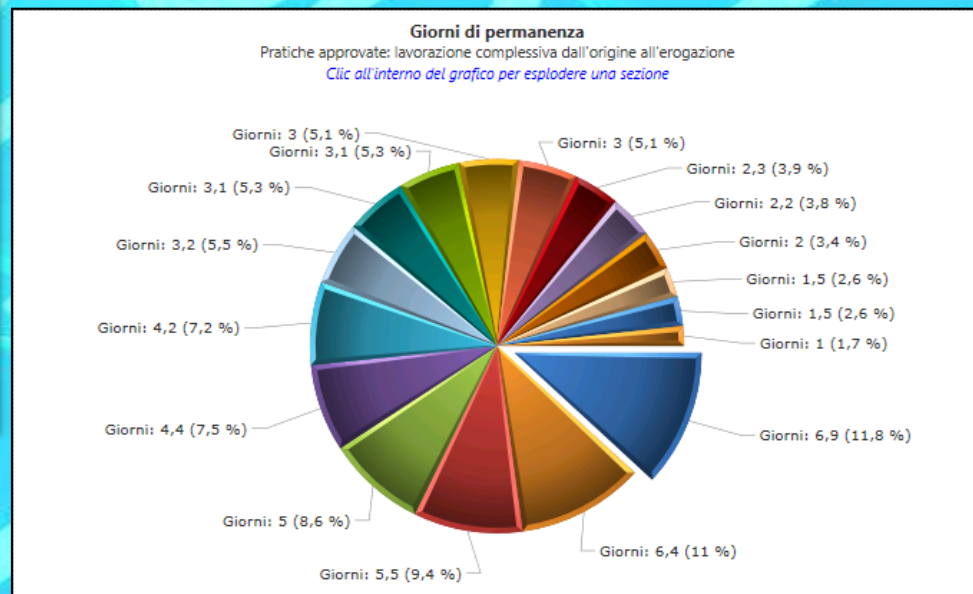
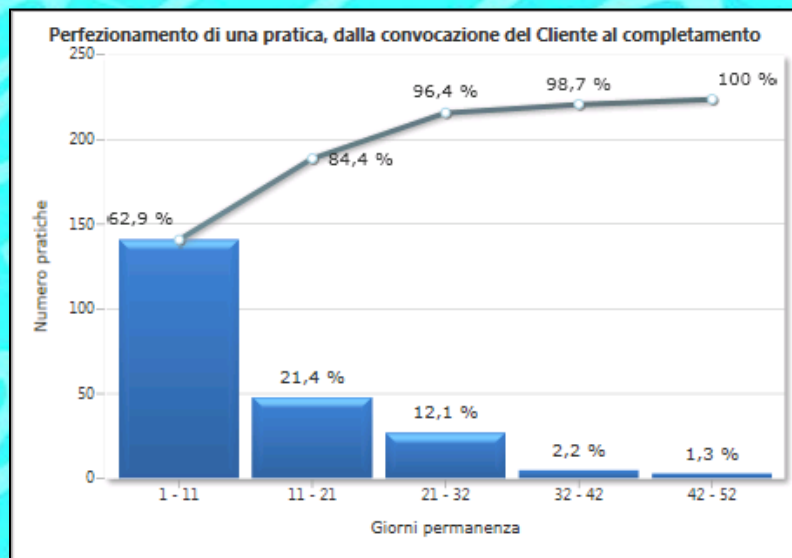
(tracciatura di tutte le attività svolte)

Impatti psicologico: sono aiutato dove e come mi serve



SICUREZZA NEL CONTROLLO

- Non solo controllo puntuale ma anche “statistico”
- Statistiche flessibili su dati “real-time”
- Estrazione dati delle attività per elaborazioni evolute (ad esempio *6-Sigma*)
- Allarmi automatici tempestivi (cruscotti di avviso, anche su *Smart-Phone*)



Impatto psicologico:

- *Devo curare la produttività*

SICUREZZA NELLA PREDIZIONE

Il gestore dei processi deve essere uno strumento predittivo

PAST

PRESENT

FUTURE

- **Sensibilità all'evento**
 - **Analisi degli eventi**
 - **Azioni autoprodotte**
 - **Avvisi predittivi**

Impatto psicologico: ho sotto controllo l'imprevisto

SICUREZZA NELL'IDENTIFICAZIONE

del cliente allo sportello

Metodi di identificazione:

- **Certificati**
- **Tavoletta di firma biometrica**
 - Identificazione firma, volto e voce
 - Tastierino PIN e OTP
- **Scanner per lettura:**
 - Smart-card/RFID
 - Tesserino magnetico
 - Carte ID/Passaporto/Patente



Impatto psicologico: so chi ho di fronte

SICUREZZA NELLE SCELTE PERSONALI

Quadro
chiaro delle
attività da
svolgere
(priorità evidente)

Statistica personale
e autocontrollo

Fotografia della
propria produttività

Spinta al
miglioramento
personale

Precedenza di
esecuzione alle
più importanti

Impatto psicologico: vedo quanto produco e posso migliorarlo



SICUREZZA NEL MIGLIORAMENTO

Evidenza delle
inefficienze

Statistiche e analisi
6-Sigma

Applicazione dei
Miglioramenti
rapida



il “miglioramento continuo” è un fatto quotidiano

Impatto psicologico: sento di collaborare al miglioramento complessivo

SICUREZZA PER L'AMBIENTE

Milioni di fogli di carta stampati ogni anno

4 litri di acqua per ogni foglio di carta

70.000 TIR per trasportarli

22.000.000 cartucce di toner

2.600.000 Pioppi abbattuti

Smaltimento di colle e coloranti necessari a produrli

Impatto psicologico: partecipo a creare un «ambiente pulito»

SICUREZZA NEL RISULTATO

per il cliente finale

- **Accordo di “Success-Fee”**
 - Ogni onere e rischio assunto da PRB
 - Costo pari a una percentuale sul risparmio
 - Liquidazione dopo aver ottenuto il risparmio

Io non rischio, è il Partner che rischia sul risultato

SICUREZZA NEL RISULTATO

per il gestore di servizi IT

- **Trasferimento di «tecnologia»**
 - Tempi di realizzazione brevi
 - Riduzione dei costi
 - Annullamento degli imprevisti
 - Copertura brevettuale

Meglio farsi aiutare da chi gli errori li ha commessi da tempo



**GRAZIE PER
L'ATTENZIONE**

spero che
questi
spunti

saranno utili
al vostro
lavoro

Antonio Carbonera
Partner, Responsabile Tecnico PRB
antonio.carbonera@prb.it

PRB

