Gestione della sicurezza

Gregorio D'Agostino

1 giugno 2021

Agenda

Revoca Certificati

Penetration Tests

Accordi per i contratti di gestione

La politica organizzativa per la sicurezza

Classificazione Sicurezza

Revoca certificati

- Se avvengono variazioni sullo stato giuridico o sulla legittimità dell'uso del name o dell'IP, i certificati possono essere revocati.

Revoca certificati

- Se avvengono variazioni sullo stato giuridico o sulla legittimità dell'uso del name o dell'IP, i certificati possono essere revocati.
- Per revocare i certificati vengono redatte delle liste di revoca che si scaricano dal sito della autorità certificante con il protocollo Certificate Revocation Lists (CRL).

Revoca certificati

- Se avvengono variazioni sullo stato giuridico o sulla legittimità dell'uso del name o dell'IP, i certificati possono essere revocati.
- Per revocare i certificati vengono redatte delle liste di revoca che si scaricano dal sito della autorità certificante con il protocollo Certificate Revocation Lists (CRL).
- Anziché scaricare questi file è stato definito un protocollo con cui si interrogano le autorità di certificazione in tempo reale tramite: Online Certificate Status Protocol

Revoca certificati

- Se avvengono variazioni sullo stato giuridico o sulla legittimità dell'uso del name o dell'IP, i certificati possono essere revocati.
- Per revocare i certificati vengono redatte delle liste di revoca che si scaricano dal sito della autorità certificante con il protocollo Certificate Revocation Lists (CRL).
- Anziché scaricare questi file è stato definito un protocollo con cui si interrogano le autorità di certificazione in tempo reale tramite: Online Certificate Status Protocol
- Tutti i browser hanno la loro gestione dei certificati. In firefox bisogna andare in preference "privacy & security".

Revoca certificati

- Se avvengono variazioni sullo stato giuridico o sulla legittimità dell'uso del name o dell'IP, i certificati possono essere revocati.
- Per revocare i certificati vengono redatte delle liste di revoca che si scaricano dal sito della autorità certificante con il protocollo Certificate Revocation Lists (CRL).
- Anziché scaricare questi file è stato definito un protocollo con cui si interrogano le autorità di certificazione in tempo reale tramite: Online Certificate Status Protocol
- Tutti i browser hanno la loro gestione dei certificati. In firefox bisogna andare in preference "privacy & security".
- In tutti i sistemi operativi moderni il controllo delle certificazioni è gestito da appositi programmi. Nei sistemi apple l'applicativo Keychain Access si interfaccia automaticamente con il browser safari.

Penetration Test

- Prima di rendere attiva una piattaforma si effettuano dei controlli sulla sicurezza informatica. Il più comune è il penetration test.

Penetration Test

- Prima di rendere attiva una piattaforma si effettuano dei controlli sulla sicurezza informatica. Il più comune è il penetration test.
- Il penetration test si avvale di strumenit informatici automatizzati ed altri che aiutano l'indagine umana. Esistono versioni anche open source ad esempio dall'organizzazione non profit "OWASP" www.owasp.org.

Penetration Test

- Prima di rendere attiva una piattaforma si effettuano dei controlli sulla sicurezza informatica. Il più comune è il penetration test.
- Il penetration test si avvale di strumenit informatici automatizzati ed altri che aiutano l'indagine umana. Esistono versioni anche open source ad esempio dall'organizzazione non profit "OWASP" www.owasp.org.
- I test verificano le principali vulnerabilità note (e quelle di conoscenza esclusiva del tester) e producono dei rapporti sulle vulnerabilità con eventuali soluzioni di migrazione di piattaforma o attuazione di dispositivi suppletivi di sicurezza.

Penetration Test

- Prima di rendere attiva una piattaforma si effettuano dei controlli sulla sicurezza informatica. Il più comune è il penetration test.
- Il penetration test si avvale di strumenit informatici automatizzati ed altri che aiutano l'indagine umana. Esistono versioni anche open source ad esempio dall'organizzazione non profit "OWASP" www.owasp.org.
- I test verificano le principali vulnerabilità note (e quelle di conoscenza esclusiva del tester) e producono dei rapporti sulle vulnerabilità con eventuali soluzioni di migrazione di piattaforma o attuazione di dispositivi suppletivi di sicurezza.
- Si indagano sia eventuali vunerabilità locali che quelle legate alla rete.

Ethical Hacking

- Gli ethical hacker sono esperti informatici che attuano le strategie di attacco sulle piattaforme con il consenso dei proprietari e con il fine di evidenziare le vulnerabilità per suggerire azioni di miglioramento della sicurezza.

Ethical Hacking

- Gli ethical hacker sono esperti informatici che attuano le strategie di attacco sulle piattaforme con il consenso dei proprietari e con il fine di evidenziare le vulnerabilità per suggerire azioni di miglioramento della sicurezza.
- Al termine dell'ispezione l'esperto fornisce un rapporto delle vulnerablità riscontrate e suggerimenti per blindare il sistema.

Ethical Hacking

- Gli ethical hacker sono esperti informatici che attuano le strategie di attacco sulle piattaforme con il consenso dei proprietari e con il fine di evidenziare le vulnerabilità per suggerire azioni di miglioramento della sicurezza.
- Al termine dell'ispezione l'esperto fornisce un rapporto delle vulnerablità riscontrate e suggerimenti per blindare il sistema.
- Sono nate delle società che forniscono queste prestazioni qualificate, ma ancora non esiste un albo degli esperti o delle società che dia una garanzia di affidabilità.

Ethical Hacking

- Gli ethical hacker sono esperti informatici che attuano le strategie di attacco sulle piattaforme con il consenso dei proprietari e con il fine di evidenziare le vulnerabilità per suggerire azioni di miglioramento della sicurezza.
- Al termine dell'ispezione l'esperto fornisce un rapporto delle vulnerablità riscontrate e suggerimenti per blindare il sistema.
- Sono nate delle società che forniscono queste prestazioni qualificate, ma ancora non esiste un albo degli esperti o delle società che dia una garanzia di affidabilità.
- Stanno nascendo scuole gestite da società private che formano e cetificano la profesionalità degli esperti che eseguono i test detti certified ethical hacker .

Gestione interna ed a contratto

- In molti casi si preferisce gestire la sicurezza all'interno di una organizzazione. Questo implica diversi concetti:

Gestione interna ed a contratto

- In molti casi si preferisce gestire la sicurezza all'interno di una organizzazione. Questo implica diversi concetti:
  - La definizione della politica di sicurezza: obiettivi (cosa tutelare), dispositivi (come tutelare) e la redazione del "piano di sicurezza" (preparation cycle e contingency plans)

Gestione interna ed a contratto

- In molti casi si preferisce gestire la sicurezza all'interno di una organizzazione. Questo implica diversi concetti:
  - La definizione della politica di sicurezza: obiettivi (cosa tutelare), dispositivi (come tutelare) e la redazione del "piano di sicurezza" (preparation cycle e contingency plans)
  - l'allocazione di personale e delle piattaforme fisiche.

Gestione interna ed a contratto

- In molti casi si preferisce gestire la sicurezza all'interno di una organizzazione. Questo implica diversi concetti:
  - La definizione della politica di sicurezza: obiettivi (cosa tutelare), dispositivi (come tutelare) e la redazione del "piano di sicurezza" (preparation cycle e contingency plans)
  - l'allocazione di personale e delle piattaforme fisiche.
  - La definizione dei dispositivi di sicurezza e la loro "implementazione".

Gestione interna ed a contratto

- In molti casi si preferisce gestire la sicurezza all'interno di una organizzazione. Questo implica diversi concetti:
  - La definizione della politica di sicurezza: obiettivi (cosa tutelare), dispositivi (come tutelare) e la redazione del "piano di sicurezza" (preparation cycle e contingency plans)
  - l'allocazione di personale e delle piattaforme fisiche.
  - La definizione dei dispositivi di sicurezza e la loro "implementazione".
  - L'allocazione di risorse per la manutenzione

Gestione interna ed a contratto

- In molti casi si preferisce gestire la sicurezza all'interno di una organizzazione. Questo implica diversi concetti:
  - La definizione della politica di sicurezza: obiettivi (cosa tutelare), dispositivi (come tutelare) e la redazione del "piano di sicurezza" (preparation cycle e contingency plans)
  - l'allocazione di personale e delle piattaforme fisiche.
  - La definizione dei dispositivi di sicurezza e la loro "implementazione".
  - L'allocazione di risorse per la manutenzione
  - Il monitoraggio delle attività

Gestione interna ed a contratto

- In molti casi si preferisce gestire la sicurezza all'interno di una organizzazione. Questo implica diversi concetti:
  - La definizione della politica di sicurezza: obiettivi (cosa tutelare), dispositivi (come tutelare) e la redazione del "piano di sicurezza" (preparation cycle e contingency plans)
  - l'allocazione di personale e delle piattaforme fisiche.
  - La definizione dei dispositivi di sicurezza e la loro "implementazione".
  - L'allocazione di risorse per la manutenzione
  - Il monitoraggio delle attività
  - La revisione periodica e straordinaria dei piani.

Gestione interna ed a contratto

- In molti casi si preferisce gestire la sicurezza all'interno di una organizzazione. Questo implica diversi concetti:
  - La definizione della politica di sicurezza: obiettivi (cosa tutelare), dispositivi (come tutelare) e la redazione del "piano di sicurezza" (preparation cycle e contingency plans)
  - l'allocazione di personale e delle piattaforme fisiche.
  - La definizione dei dispositivi di sicurezza e la loro "implementazione".
  - L'allocazione di risorse per la manutenzione
  - Il monitoraggio delle attività
  - La revisione periodica e straordinaria dei piani.
  - Predisposizione di eventuali unità di crisi.

Gestione interna ed a contratto

- In molti casi si preferisce gestire la sicurezza all'interno di una organizzazione. Questo implica diversi concetti:
  - La definizione della politica di sicurezza: obiettivi (cosa tutelare), dispositivi (come tutelare) e la redazione del "piano di sicurezza" (preparation cycle e contingency plans)
  - l'allocazione di personale e delle piattaforme fisiche.
  - La definizione dei dispositivi di sicurezza e la loro "implementazione".
  - L'allocazione di risorse per la manutenzione
  - Il monitoraggio delle attività
  - La revisione periodica e straordinaria dei piani.
  - Predisposizione di eventuali unità di crisi.
- Per ridurre il carico interno di tali attività spesso si ricorre a contratti di gestione in cui si definiscono le modalità con cui alcune delle attività vengono svolte da soggetti esterni. In molte multinazionali i contratti si fanno anche tra società controllate dalla stessa case madre (holding).

Contratti di Gestione

- Nella definizione dei contratti si dovrebbe raggiungere un equilibrio tra le risorse economiche allocate e la qualità del servizio fornita.

Contratti di Gestione

- Nella definizione dei contratti si dovrebbe raggiungere un equilibrio tra le risorse economiche allocate e la qualità del servizio fornita.
- La qualità del servizio viene spesso "garantita" tramite gli accordi sui livelli di servizio SLA (Service Level Agreement).

Contratti di Gestione

- Nella definizione dei contratti si dovrebbe raggiungere un equilibrio tra le risorse economiche allocate e la qualità del servizio fornita.
- La qualità del servizio viene spesso "garantita" tramite gli accordi sui livelli di servizio SLA (Service Level Agreement).
- Il meccanismo delle penali:
  Per ogni indicatore di prestazione (abbiamo visto la definizione di Performance Indicator) viene previsto un livello da rispettare (che può essere medio, di picco o sostenuto) e delle penali legate all'entità del disservizio ed alla sua durata.

Contratti di Gestione

- Nella definizione dei contratti si dovrebbe raggiungere un equilibrio tra le risorse economiche allocate e la qualità del servizio fornita.
- La qualità del servizio viene spesso "garantita" tramite gli accordi sui livelli di servizio SLA (Service Level Agreement).
- Il meccanismo delle penali:
  Per ogni indicatore di prestazione (abbiamo visto la definizione di Performance Indicator) viene previsto un livello da rispettare (che può essere medio, di picco o sostenuto) e delle penali legate all'entità del disservizio ed alla sua durata.
- In totale per definire correttamente un accordo di gestione occorrerebbe valutare l'impatto del mancato servizio e richiedere delle penali economicamente equivalenti al danno eventuale. Molto spesso invece si lavora a budget prefissato e si definisce il massimo livello ottenibile dal fornitore di servizio fissate le SLA e le relative penali.

Principali servizi su cui concordare i livelli minimali garantiti

Si possono distinguere elementi strettamente informatici ed elementi con intervento umano.

- Principali elementi che coinvolgono in maniera attiva gli operatori:

Principali servizi su cui concordare i livelli minimali garantiti

Si possono distinguere elementi strettamente informatici ed elementi con intervento umano.

- Principali elementi che coinvolgono in maniera attiva gli operatori:
- Tempi di intervento in caso di interruzione o impoverimento del servizio

Principali servizi su cui concordare i livelli minimali garantiti

Si possono distinguere elementi strettamente informatici ed elementi con intervento umano.

- Principali elementi che coinvolgono in maniera attiva gli operatori:
- Tempi di intervento in caso di interruzione o impoverimento del servizio
- Tempi di ripristino dei livelli garantiti di servizio (o di altri livelli minimali temporanei) per i principali eventi indesiderati prevedibili.

Principali servizi su cui concordare i livelli minimali garantiti

Si possono distinguere elementi strettamente informatici ed elementi con intervento umano.

- Principali elementi che coinvolgono in maniera attiva gli operatori:
- Tempi di intervento in caso di interruzione o impoverimento del servizio
- Tempi di ripristino dei livelli garantiti di servizio (o di altri livelli minimali temporanei) per i principali eventi indesiderati prevedibili.
- Orari di assistenza, Assistenza straordinaria (fuori orario)

Principali servizi su cui concordare i livelli minimali garantiti

Si possono distinguere elementi strettamente informatici ed elementi con intervento umano.

- Principali elementi che coinvolgono in maniera attiva gli operatori:
- Tempi di intervento in caso di interruzione o impoverimento del servizio
- Tempi di ripristino dei livelli garantiti di servizio (o di altri livelli minimali temporanei) per i principali eventi indesiderati prevedibili.
- Orari di assistenza, Assistenza straordinaria (fuori orario)
- Procedure d'urgenza e di emergenza;

Principali servizi su cui concordare i livelli minimali garantiti

Si possono distinguere elementi strettamente informatici ed elementi con intervento umano.

- Principali elementi che coinvolgono in maniera attiva gli operatori:
- Tempi di intervento in caso di interruzione o impoverimento del servizio
- Tempi di ripristino dei livelli garantiti di servizio (o di altri livelli minimali temporanei) per i principali eventi indesiderati prevedibili.
- Orari di assistenza, Assistenza straordinaria (fuori orario)
- Procedure d'urgenza e di emergenza;
- Procedure di recovery e restauration post emergenza

Principali servizi su cui concordare i livelli minimali garantiti

Si possono distinguere elementi strettamente informatici ed elementi con intervento umano.

- Principali elementi che coinvolgono in maniera attiva gli operatori:
- Tempi di intervento in caso di interruzione o impoverimento del servizio
- Tempi di ripristino dei livelli garantiti di servizio (o di altri livelli minimali temporanei) per i principali eventi indesiderati prevedibili.
- Orari di assistenza, Assistenza straordinaria (fuori orario)
- Procedure d'urgenza e di emergenza;
- Procedure di recovery e restauration post emergenza
- Numero di addetti e responsabili dei servizi e degli interventi.

Principali servizi su cui concordare i livelli minimali garantiti

Si possono distinguere elementi strettamente informatici ed elementi con intervento umano.

- Principali elementi che coinvolgono in maniera attiva gli operatori:
- Tempi di intervento in caso di interruzione o impoverimento del servizio
- Tempi di ripristino dei livelli garantiti di servizio (o di altri livelli minimali temporanei) per i principali eventi indesiderati prevedibili.
- Orari di assistenza, Assistenza straordinaria (fuori orario)
- Procedure d'urgenza e di emergenza;
- Procedure di recovery e restauration post emergenza
- Numero di addetti e responsabili dei servizi e degli interventi.
- Accordi sulle modalità di reperibilità

Principali servizi su cui concordare i livelli minimali garantiti

Si possono distinguere elementi strettamente informatici ed elementi con intervento umano.

- Principali elementi che coinvolgono in maniera attiva gli operatori:
- Tempi di intervento in caso di interruzione o impoverimento del servizio
- Tempi di ripristino dei livelli garantiti di servizio (o di altri livelli minimali temporanei) per i principali eventi indesiderati prevedibili.
- Orari di assistenza, Assistenza straordinaria (fuori orario)
- Procedure d'urgenza e di emergenza;
- Procedure di recovery e restauration post emergenza
- Numero di addetti e responsabili dei servizi e degli interventi.
- Accordi sulle modalità di reperibilità
- Regole per l'evoluzione degli accordi (per evitare dipendenze)

Principali procedure automatizzate (coinvolgono gli operatori solo per manutenzione o malfunzionamento)

- Livelli di servizio minimo, sostenuto, medio e di picco (può prevedere aumenti di costo).

Principali procedure automatizzate (coinvolgono gli operatori solo per manutenzione o malfunzionamento)

- Livelli di servizio minimo, sostenuto, medio e di picco (può prevedere aumenti di costo).
- Procedure di monitoraggio (log delle attività nei server ed in rete) accountability

Principali procedure automatizzate (coinvolgono gli operatori solo per manutenzione o malfunzionamento)

- Livelli di servizio minimo, sostenuto, medio e di picco (può prevedere aumenti di costo).
- Procedure di monitoraggio (log delle attività nei server ed in rete) accountability
- Procedure di backup dei dati e di cancellazione.

Principali procedure automatizzate (coinvolgono gli operatori solo per manutenzione o malfunzionamento)

- Livelli di servizio minimo, sostenuto, medio e di picco (può prevedere aumenti di costo).
- Procedure di monitoraggio (log delle attività nei server ed in rete) accountability
- Procedure di backup dei dati e di cancellazione.
- Procedure di backup del traffico sulle linee di comunicazione

Principali procedure automatizzate (coinvolgono gli operatori solo per manutenzione o malfunzionamento)

- Livelli di servizio minimo, sostenuto, medio e di picco (può prevedere aumenti di costo).
- Procedure di monitoraggio (log delle attività nei server ed in rete) accountability
- Procedure di backup dei dati e di cancellazione.
- Procedure di backup del traffico sulle linee di comunicazione
- Qualità dell'hardware e dispositivi di sicurezza istallati (certificazione ed eventuali standard)

Principali procedure automatizzate (coinvolgono gli operatori solo per manutenzione o malfunzionamento)

- Livelli di servizio minimo, sostenuto, medio e di picco (può prevedere aumenti di costo).
- Procedure di monitoraggio (log delle attività nei server ed in rete) accountability
- Procedure di backup dei dati e di cancellazione.
- Procedure di backup del traffico sulle linee di comunicazione
- Qualità dell'hardware e dispositivi di sicurezza istallati (certificazione ed eventuali standard)
- Gestione della Fine contratto: tempo di custodia, modalità di transizione e cancellazione dei dati.

Responsabilità

- Il termine si usa in senso lato nelle organizzazione riferendosi a chi risponde delle conseguenze degli eventuali errori di pianificazione o gestione.

Responsabilità

- Il termine si usa in senso lato nelle organizzazione riferendosi a chi risponde delle conseguenze degli eventuali errori di pianificazione o gestione.
- Uno dei problemi fondamentali per ogni organizzazione è definire delle modalità operative che consentano sempre la tracciabilità della responsabilità per ciascun atto.

Responsabilità giuridica

- La responsabilità giuridica è suddivisa in responsabilità penale e civile (cioè economica). Le eventuali vertenze sono risolte nei tribunali civili e amministrativi e le corti penali.

Responsabilità giuridica

- La responsabilità giuridica è suddivisa in responsabilità penale e civile (cioè economica). Le eventuali vertenze sono risolte nei tribunali civili e amministrativi e le corti penali.
- La responsabilità penale è sempre individuale (tranne reato di associazione a delinquere) ed è quindi in prima istanza attribuita all'operatore che deliberatamente commette la violazione. Si estende ai datori di lavoro qualora vi sia una specifica richiesta (mandanti) o una grave negligenza (mancata vigilanza (mancanza di controlli) o inappropriata allocazione di risorse).

Responsabilità giuridica

- La responsabilità giuridica è suddivisa in responsabilità penale e civile (cioè economica). Le eventuali vertenze sono risolte nei tribunali civili e amministrativi e le corti penali.
- La responsabilità penale è sempre individuale (tranne reato di associazione a delinquere) ed è quindi in prima istanza attribuita all'operatore che deliberatamente commette la violazione. Si estende ai datori di lavoro qualora vi sia una specifica richiesta (mandanti) o una grave negligenza (mancata vigilanza (mancanza di controlli) o inappropriata allocazione di risorse).
- La responsabiltà civile cioè la condivisione in solido dei danni, di solito non viene accettata dai fornitori di servizio e rimane sempre esclusivamente del soggetto che sia avvale dei servizi. Esempio classico: un internet service provider (ISP) non fornisce il servizio per un tempo assegnato. Qualunque sia l'ammontare del danno Il'ISP pagherà solo le panali previste per l'interruzione di servizio. In molti casi (e.g. operazioni bancarie) il danno è notevolmente superiore.

Condivisione del Rischio

- Il termine risk sharing, cioè condivisione del rischio è una modalità che le aziende vorrebbero introdurre, ma attualmente i fornitori di servizio non accettano. Significa che il fornitore di servizio dovrebbe rispondere in solido di eventuali perdite legate all'interruzione (o impoverimento) del servizio, ma nel contempo beneficiare di percentuali sui guadagni (o sui ricavi) dello stesso.

Condivisione del Rischio

- Il termine risk sharing, cioè condivisione del rischio è una modalità che le aziende vorrebbero introdurre, ma attualmente i fornitori di servizio non accettano. Significa che il fornitore di servizio dovrebbe rispondere in solido di eventuali perdite legate all'interruzione (o impoverimento) del servizio, ma nel contempo beneficiare di percentuali sui guadagni (o sui ricavi) dello stesso.
- I rischi che rendono difficile accettare la condivisione sono legati alle azioni terroristiche ed alle grandi calamità naturali. Le grandi società di assicurazione di solito escludono dalla copertura questo genere di eventi. Per tale ragione esiste una componente del rischio che nessuno vuole condividere (o lo farebbe a costi insostenibili).

Condivisione del Rischio

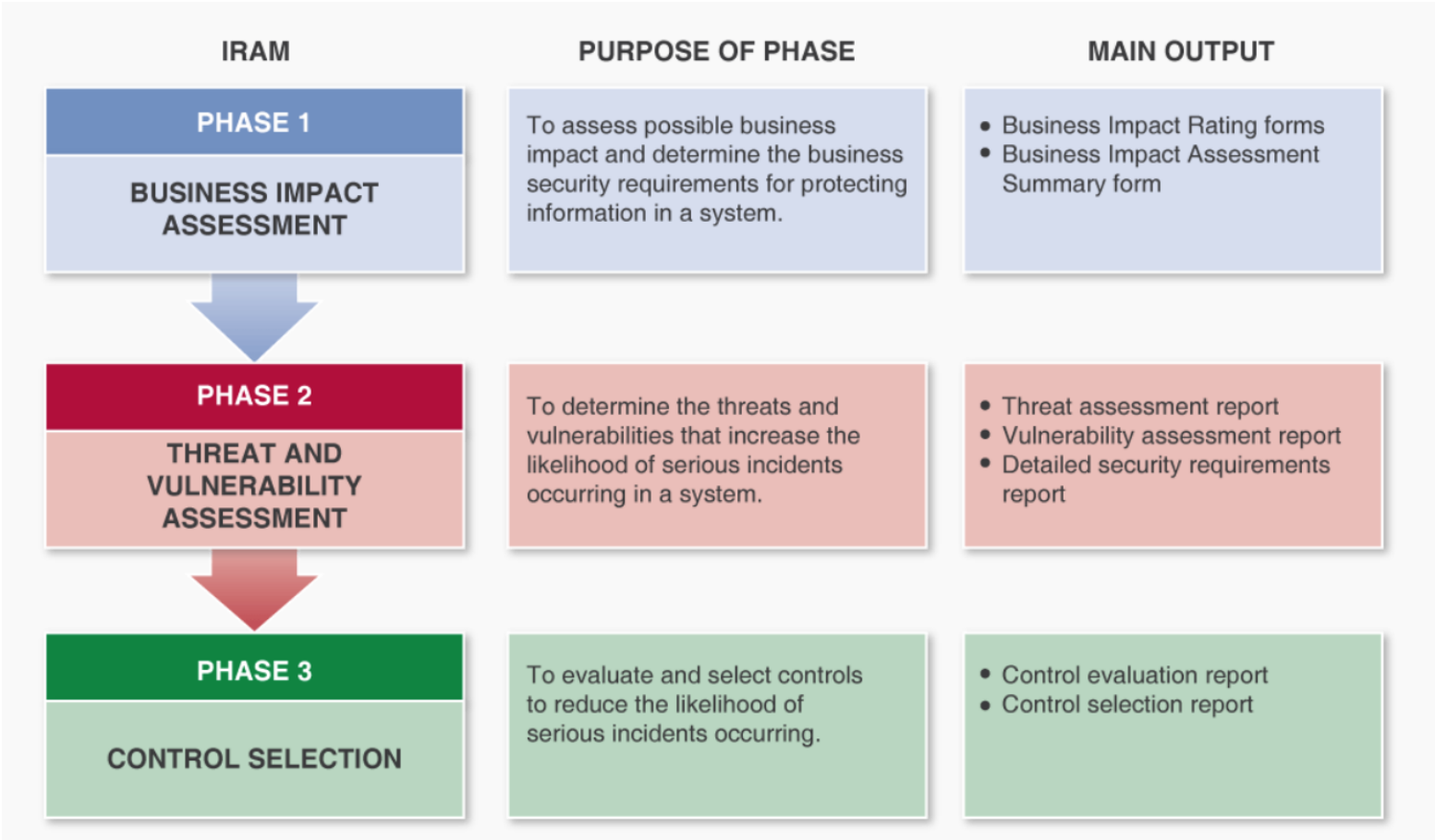
- Il termine risk sharing, cioè condivisione del rischio è una modalità che le aziende vorrebbero introdurre, ma attualmente i fornitori di servizio non accettano. Significa che il fornitore di servizio dovrebbe rispondere in solido di eventuali perdite legate all'interruzione (o impoverimento) del servizio, ma nel contempo beneficiare di percentuali sui guadagni (o sui ricavi) dello stesso.
- I rischi che rendono difficile accettare la condivisione sono legati alle azioni terroristiche ed alle grandi calamità naturali. Le grandi società di assicurazione di solito escludono dalla copertura questo genere di eventi. Per tale ragione esiste una componente del rischio che nessuno vuole condividere (o lo farebbe a costi insostenibili).
- Nelle istituzioni pubbliche lo Stato di solito risponde in solido con i suoi Enti (public bodies) e indirettamente quando soggetti terzi gestiscono per suo conto attività istituzionali. Ovviamente la responsabilità in solido in questi casi è squisitamente finanziaria.

Standard e certificazioni

- Gli standard per la sicurezza sono in continua evoluzione. Ecco un esempio di organizzazione non profit e non governativa:

Standard e certificazioni

- Gli standard per la sicurezza sono in continua evoluzione. Ecco un esempio di organizzazione non profit e non governativa:
- Information Security Forum (https://www.securityforum.org) è una organizzazione non profit a cui aderiscono molte aziende: IBM, NOKIA, SWISCOM, Telefonica, etc. Fornisce uno schema per la sicurezza.



Standard sicurezza

- Lo standard in vigore (ma come detto sono in continua evoluzione) è lo ISO/IEC 27000:2018 della Organizzazione Internazionale per la standardizzazione https://www.iso.org/standard/73906.html, si può scaricare qui: *http://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip*

Standard sicurezza

- Lo standard in vigore (ma come detto sono in continua evoluzione) è lo ISO/IEC 27000:2018 della Organizzazione Internazionale per la standardizzazione https://www.iso.org/standard/73906.html, si può scaricare qui: *http://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip*
- L'adozione di uno standard può per una società essere certificato da una società di audit che osserva il funzionamento di un fornitore di servizi informatici.

Standard sicurezza

- Lo standard in vigore (ma come detto sono in continua evoluzione) è lo ISO/IEC 27000:2018 della Organizzazione Internazionale per la standardizzazione https://www.iso.org/standard/73906.html, si può scaricare qui: *http://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip*
- L'adozione di uno standard può per una società essere certificato da una società di audit che osserva il funzionamento di un fornitore di servizi informatici.
- Le società certificanti sono tutti soggetti privati. La vigilanza sulle società di certificazione in Italia è svolta dall' Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCOM)

Standard sicurezza

- Lo standard in vigore (ma come detto sono in continua evoluzione) è lo ISO/IEC 27000:2018 della Organizzazione Internazionale per la standardizzazione https://www.iso.org/standard/73906.html, si può scaricare qui: *http://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip*
- L'adozione di uno standard può per una società essere certificato da una società di audit che osserva il funzionamento di un fornitore di servizi informatici.
- Le società certificanti sono tutti soggetti privati. La vigilanza sulle società di certificazione in Italia è svolta dall' Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCOM)
- In ogni caso è sempre opportuno che l'azienda committente sia in grado verificare i contratti di gestione e le reali sicurezze attuate dal gestore, non è sufficiente basarsi sugli standard e le certificazioni del gestore.

Certificazione professionalità

- Anche la professionalità degli operatori può essere certificata; ad esempio:

Certificazione professionalità

- Anche la professionalità degli operatori può essere certificata; ad esempio:
  - Il "Certified Information Security Manager" è rilasciato da Information Systems Audit and Control Association, *ISACA*

Certificazione professionalità

- Anche la professionalità degli operatori può essere certificata; ad esempio:
  - Il "Certified Information Security Manager" è rilasciato da Information Systems Audit and Control Association, *ISACA*
  - Il "Certified Information Systems Security Professional" è rilasciato da International Information System Security Certification Consortium $(ICS)^2$

Certificazione professionalità

- Anche la professionalità degli operatori può essere certificata; ad esempio:
  - Il "Certified Information Security Manager" è rilasciato da Information Systems Audit and Control Association, *ISACA*
  - Il "Certified Information Systems Security Professional" è rilasciato da International Information System Security Certification Consortium $(ICS)^2$
  - Cisco rilascia il "Certified Network Associate - Security" professionalità per la gestione delle reti.

Certificazione professionalità

- Anche la professionalità degli operatori può essere certificata; ad esempio:
  - Il "Certified Information Security Manager" è rilasciato da Information Systems Audit and Control Association, *ISACA*
  - Il "Certified Information Systems Security Professional" è rilasciato da International Information System Security Certification Consortium $(ICS)^2$
  - Cisco rilascia il "Certified Network Associate - Security" professionalità per la gestione delle reti.
- La certificazione della professionalità può essere un elemento di valutazione per la scelta degli addetti alla sicurezza o degli operatori esterni ad essa assegnati.

Politica organizzativa per la sicurezza informatica

- Nella definizione della Policy il primo passo è la definizione del bene da tutelare. In particolare definire quali sono attività essenziali che richiedono necessariamente l'uso di applicazioni informatiche. Anche questa attività può essere commissionata all'esterno dell'organizzazione, ma un minimo di competenza interno è necessario.

Politica organizzativa per la sicurezza informatica

- Nella definizione della Policy il primo passo è la definizione del bene da tutelare. In particolare definire quali sono attività essenziali che richiedono necessariamente l'uso di applicazioni informatiche. Anche questa attività può essere commissionata all'esterno dell'organizzazione, ma un minimo di competenza interno è necessario.
- In secondo ordine occorre valutare quali attività possono migliorare con l'introduzione del trattamento informatico.

Politica organizzativa per la sicurezza informatica

- Nella definizione della Policy il primo passo è la definizione del bene da tutelare. In particolare definire quali sono attività essenziali che richiedono necessariamente l'uso di applicazioni informatiche. Anche questa attività può essere commissionata all'esterno dell'organizzazione, ma un minimo di competenza interno è necessario.
- In secondo ordine occorre valutare quali attività possono migliorare con l'introduzione del trattamento informatico.
- Valutare quali decisioni operative dipendono dalla integrità (accuratezza) , disponibilità e confidenzialità dei dati.

Politica organizzativa per la sicurezza informatica

- Nella definizione della Policy il primo passo è la definizione del bene da tutelare. In particolare definire quali sono attività essenziali che richiedono necessariamente l'uso di applicazioni informatiche. Anche questa attività può essere commissionata all'esterno dell'organizzazione, ma un minimo di competenza interno è necessario.
- In secondo ordine occorre valutare quali attività possono migliorare con l'introduzione del trattamento informatico.
- Valutare quali decisioni operative dipendono dalla integrità (accuratezza) , disponibilità e confidenzialità dei dati.
- Valutare quali dati creati, immagazzinati, manipolati, gestiti o elaborati nei dispositivi informatici devono essere protetti e difesi?

Politica organizzativa per la sicurezza informatica - cont.

- Valutare qual è l'impatto economico, di immagine ed eventualmente penale legato ad un potenziale fallimento della gestione informatica.

Politica organizzativa per la sicurezza informatica - cont.

- Valutare qual è l'impatto economico, di immagine ed eventualmente penale legato ad un potenziale fallimento della gestione informatica.
- Questi elementi consentono di definire le necessità informatiche di una organizzazione aziendale o un soggetto fornitore di servizi pubblici.

Politica organizzativa per la sicurezza informatica - cont.

- Valutare qual è l'impatto economico, di immagine ed eventualmente penale legato ad un potenziale fallimento della gestione informatica.
- Questi elementi consentono di definire le necessità informatiche di una organizzazione aziendale o un soggetto fornitore di servizi pubblici.
- Una delle maggiori difficoltà per un manager della sicurezza è convincere i decisori aziendali ad allocare fondi specifici per la sicurezza. Spesso le spese per la sicurezza vengono considerate inutili.

Politica organizzativa per la sicurezza informatica - cont.

- Valutare qual è l'impatto economico, di immagine ed eventualmente penale legato ad un potenziale fallimento della gestione informatica.
- Questi elementi consentono di definire le necessità informatiche di una organizzazione aziendale o un soggetto fornitore di servizi pubblici.
- Una delle maggiori difficoltà per un manager della sicurezza è convincere i decisori aziendali ad allocare fondi specifici per la sicurezza. Spesso le spese per la sicurezza vengono considerate inutili.
- Il problema è gli eventi o le contingenze scongiurati dalla prevenzione e dai dispositivi di sicurezza informatica non si osservano.

Pianificazione della sicurezza informatica - vincoli e finalità

Nel definire la pianificazione (in inglese è più chiaro il termine security policy), occorre tenere conto di moltissimi elementi:

- lo scopo della pianificazione

Pianificazione della sicurezza informatica - vincoli e finalità

Nel definire la pianificazione (in inglese è più chiaro il termine security policy), occorre tenere conto di moltissimi elementi:

- lo scopo della pianificazione
- Le relazioni tre gli obiettivi prefissati e le normative legali, regolatorie e gli obiettivi finanziari.

Pianificazione della sicurezza informatica - vincoli e finalità

Nel definire la pianificazione (in inglese è più chiaro il termine security policy), occorre tenere conto di moltissimi elementi:

- lo scopo della pianificazione
- Le relazioni tre gli obiettivi prefissati e le normative legali, regolatorie e gli obiettivi finanziari.
- Vincoli di disponibilità, confidenzialità ed integrità; ma anche di accoutability, authenticità, affibdabilità.

Pianificazione della sicurezza informatica - vincoli e finalità

Nel definire la pianificazione (in inglese è più chiaro il termine security policy), occorre tenere conto di moltissimi elementi:

- lo scopo della pianificazione
- Le relazioni tre gli obiettivi prefissati e le normative legali, regolatorie e gli obiettivi finanziari.
- Vincoli di disponibilità, confidenzialità ed integrità; ma anche di accoutability, authenticità, affibdabilità.
- La suddivisione delle reponsabilità all'interno dell'organizzazione.

Pianificazione della sicurezza informatica - vincoli e finalità

Nel definire la pianificazione (in inglese è più chiaro il termine security policy), occorre tenere conto di moltissimi elementi:

- lo scopo della pianificazione
- Le relazioni tre gli obiettivi prefissati e le normative legali, regolatorie e gli obiettivi finanziari.
- Vincoli di disponibilità, confidenzialità ed integrità; ma anche di accoutability, authenticità, affibdabilità.
- La suddivisione delle reponsabilità all'interno dell'organizzazione.
- L'approccio al rischio deciso dai vertici dell'organizzazione

Pianificazione della sicurezza informatica - vincoli e finalità

Nel definire la pianificazione (in inglese è più chiaro il termine security policy), occorre tenere conto di moltissimi elementi:

- lo scopo della pianificazione
- Le relazioni tre gli obiettivi prefissati e le normative legali, regolatorie e gli obiettivi finanziari.
- Vincoli di disponibilità, confidenzialità ed integrità; ma anche di accoutability, authenticità, affibdabilità.
- La suddivisione delle reponsabilità all'interno dell'organizzazione.
- L'approccio al rischio deciso dai vertici dell'organizzazione
- Gestione della consapevolezza informatica e addestramento del personale (eventuali sanzioni penali ed economiche del personale coinvolto)

Pianificazione della sicurezza informatica - vincoli e finalità - cont.

- Armonizzazione con le politiche di sviluppo dell'organizzazione (miglioramento ed acquisizione mercati).

Pianificazione della sicurezza informatica - vincoli e finalità - cont.

- Armonizzazione con le politiche di sviluppo dell'organizzazione (miglioramento ed acquisizione mercati).
- Classificazione delle informazioni e dei livelli di accesso.

Pianificazione della sicurezza informatica - vincoli e finalità - cont.

- Armonizzazione con le politiche di sviluppo dell'organizzazione (miglioramento ed acquisizione mercati).
- Classificazione delle informazioni e dei livelli di accesso.
- Meccanismi per il rilevamento degli incidenti o altri eventi indesiderati

Pianificazione della sicurezza informatica - vincoli e finalità - cont.

- Armonizzazione con le politiche di sviluppo dell'organizzazione (miglioramento ed acquisizione mercati).
- Classificazione delle informazioni e dei livelli di accesso.
- Meccanismi per il rilevamento degli incidenti o altri eventi indesiderati
- Periodicità e modalità di revisione della pianificazione

Classificazione segretezza

- Le attività di una organizzazione ed i relativi documenti vengono spesso organizzate secondo dei livelli gerarchici di segretezza. La classificazione può essere arbitraria, ma di solito si utilizza quella standard.

Classificazione segretezza

- Le attività di una organizzazione ed i relativi documenti vengono spesso organizzate secondo dei livelli gerarchici di segretezza. La classificazione può essere arbitraria, ma di solito si utilizza quella standard.
- Il livelli standard sono quattro: in Italia vengono denominati: riservato (R), riservatissimo (RR), segreto (S), segretissimo (SS). Oltre ovviamente al livello pubblico cioè non classificato.

Classificazione segretezza

- Le attività di una organizzazione ed i relativi documenti vengono spesso organizzate secondo dei livelli gerarchici di segretezza. La classificazione può essere arbitraria, ma di solito si utilizza quella standard.
- Il livelli standard sono quattro: in Italia vengono denominati: riservato (R), riservatissimo (RR), segreto (S), segretissimo (SS). Oltre ovviamente al livello pubblico cioè non classificato.
- I livelli internazionali vengono invece denominati: Restricted, Confidential, Secret e Top secret; oltre agli "unclassified".

Classificazione segretezza

- Le attività di una organizzazione ed i relativi documenti vengono spesso organizzate secondo dei livelli gerarchici di segretezza. La classificazione può essere arbitraria, ma di solito si utilizza quella standard.
- Il livelli standard sono quattro: in Italia vengono denominati: riservato (R), riservatissimo (RR), segreto (S), segretissimo (SS). Oltre ovviamente al livello pubblico cioè non classificato.
- I livelli internazionali vengono invece denominati: Restricted, Confidential, Secret e Top secret; oltre agli "unclassified".
- Un documento non classificato potrebbe contenere delle informazioni protette e quindi tale condizione non esime dalla cautela nella diffusione.

Classificazione segretezza

- Le attività di una organizzazione ed i relativi documenti vengono spesso organizzate secondo dei livelli gerarchici di segretezza. La classificazione può essere arbitraria, ma di solito si utilizza quella standard.
- Il livelli standard sono quattro: in Italia vengono denominati: riservato (R), riservatissimo (RR), segreto (S), segretissimo (SS). Oltre ovviamente al livello pubblico cioè non classificato.
- I livelli internazionali vengono invece denominati: Restricted, Confidential, Secret e Top secret; oltre agli "unclassified".
- Un documento non classificato potrebbe contenere delle informazioni protette e quindi tale condizione non esime dalla cautela nella diffusione.
- Quando un documento può essere diffuso liberamente si effettua una liberatoria (disclaimer) che ne garantisce l'innoquità.

Nulla Osta Sicurezza NOS

- In inglese security clearance è un attestato che consente agli individui di accedere alle informazioni classificate.

Nulla Osta Sicurezza NOS

- In inglese security clearance è un attestato che consente agli individui di accedere alle informazioni classificate.
- I livelli di nulla osta sono i medesimi della sicurezza.

Nulla Osta Sicurezza NOS

- In inglese security clearance è un attestato che consente agli individui di accedere alle informazioni classificate.
- I livelli di nulla osta sono i medesimi della sicurezza.
- Il rilascio di tale attestato avviene in Italia da parte del Dipartimento delle informazioni per la sicurezza della presidenza del Consiglio dei Ministri.

Nulla Osta Sicurezza NOS

- In inglese security clearance è un attestato che consente agli individui di accedere alle informazioni classificate.
- I livelli di nulla osta sono i medesimi della sicurezza.
- Il rilascio di tale attestato avviene in Italia da parte del Dipartimento delle informazioni per la sicurezza della presidenza del Consiglio dei Ministri.
- In altri Paesi vi sono altri soggetti istituzionali preposti al rilascio del nulla osta sicurezza.

Nulla Osta Sicurezza NOS

- In inglese security clearance è un attestato che consente agli individui di accedere alle informazioni classificate.
- I livelli di nulla osta sono i medesimi della sicurezza.
- Il rilascio di tale attestato avviene in Italia da parte del Dipartimento delle informazioni per la sicurezza della presidenza del Consiglio dei Ministri.
- In altri Paesi vi sono altri soggetti istituzionali preposti al rilascio del nulla osta sicurezza.
- 19 March 2001 Il consiglio della Comunità Europea (collegio dei ministri degli stati membri) ha adottato "The Council's security regulations" (2001/264/EC). In tale documento si definiscono le politiche comuni sulla sicurezza.

Livello di accesso alla segretezza

- Nelle organizzazioni ogni individuo ha un suo livello massimo di accesso alla sicurezza.

Livello di accesso alla segretezza

- Nelle organizzazioni ogni individuo ha un suo livello massimo di accesso alla sicurezza.
- Di solito si definiscono delle strutture settoriali per cui allo stesso individuo possono essere attribuiti livelli di accesso in base alla tematica.

Livello di accesso alla segretezza

- Nelle organizzazioni ogni individuo ha un suo livello massimo di accesso alla sicurezza.
- Di solito si definiscono delle strutture settoriali per cui allo stesso individuo possono essere attribuiti livelli di accesso in base alla tematica.
- I sistemi informatici che gestiscono la sicurezza dei dati devono rispettare tale struttura. In particolare il system manager deve essere in grado di manipolare il sistema senza superare il proprio livello di sicurezza.

Livello di accesso alla segretezza

- Nelle organizzazioni ogni individuo ha un suo livello massimo di accesso alla sicurezza.
- Di solito si definiscono delle strutture settoriali per cui allo stesso individuo possono essere attribuiti livelli di accesso in base alla tematica.
- I sistemi informatici che gestiscono la sicurezza dei dati devono rispettare tale struttura. In particolare il system manager deve essere in grado di manipolare il sistema senza superare il proprio livello di sicurezza.
- La gestione delle banche dati consente di rispettare i livelli di sicurezza assegnati con meccanismi analoghi alle passwd e meccanismi di crittazione asimmetrica.

Modello di Bell-La Padula

- Il modello è basato su una gerarchia di livelli di segretezza (o sensibilità) decrescente.

Modello di Bell-La Padula

- Il modello è basato su una gerarchia di livelli di segretezza (o sensibilità) decrescente.
- Ad ogni utente è assegnata una Classe ovvero un livello massimo di accessibilità in un dato settore.

Modello di Bell-La Padula

- Il modello è basato su una gerarchia di livelli di segretezza (o sensibilità) decrescente.
- Ad ogni utente è assegnata una Classe ovvero un livello massimo di accessibilità in un dato settore.
- Per tutelare la confidenzialità il modello richiede due principi:

Modello di Bell-La Padula

- Il modello è basato su una gerarchia di livelli di segretezza (o sensibilità) decrescente.
- Ad ogni utente è assegnata una Classe ovvero un livello massimo di accessibilità in un dato settore.
- Per tutelare la confidenzialità il modello richiede due principi:
  - Si possono leggere solo documenti classificati al livello inferiore al proprio rango.

Modello di Bell-La Padula

- Il modello è basato su una gerarchia di livelli di segretezza (o sensibilità) decrescente.
- Ad ogni utente è assegnata una Classe ovvero un livello massimo di accessibilità in un dato settore.
- Per tutelare la confidenzialità il modello richiede due principi:
  - Si possono leggere solo documenti classificati al livello inferiore al proprio rango.
  - Si possono scrivere (modalità addizionale senza leggere) solo documenti classificati al livello superiore al proprio rango.

Modello di Bell-La Padula

- Il modello è basato su una gerarchia di livelli di segretezza (o sensibilità) decrescente.
- Ad ogni utente è assegnata una Classe ovvero un livello massimo di accessibilità in un dato settore.
- Per tutelare la confidenzialità il modello richiede due principi:
  - Si possono leggere solo documenti classificati al livello inferiore al proprio rango.
  - Si possono scrivere (modalità addizionale senza leggere) solo documenti classificati al livello superiore al proprio rango.
- Applicando entrambi i criteri si evita il rilascio di informazioni alle gerarchie inferiori.

Modello di Bell-La Padula

- Il modello è basato su una gerarchia di livelli di segretezza (o sensibilità) decrescente.
- Ad ogni utente è assegnata una Classe ovvero un livello massimo di accessibilità in un dato settore.
- Per tutelare la confidenzialità il modello richiede due principi:
  - Si possono leggere solo documenti classificati al livello inferiore al proprio rango.
  - Si possono scrivere (modalità addizionale senza leggere) solo documenti classificati al livello superiore al proprio rango.
- Applicando entrambi i criteri si evita il rilascio di informazioni alle gerarchie inferiori.
- I livelli rwx dei privilegi attribuiti a root, gruppi e utenti in linux e le Proprietà dei file in windows rispecchiano lo schema. Lo stesso vale per la gestione delle banche dati.

Messaggio

- La sicurezza (in particolare informatica) richiede una pianificazione (policy) e la definizione delle regole generali.

Messaggio

- La sicurezza (in particolare informatica) richiede una pianificazione (policy) e la definizione delle regole generali.
- La gestione dei sistemi informativi puó essere realizzata dal personale autorizzato o essere commissionata all'esterno.

Messaggio

- La sicurezza (in particolare informatica) richiede una pianificazione (policy) e la definizione delle regole generali.
- La gestione dei sistemi informativi puó essere realizzata dal personale autorizzato o essere commissionata all'esterno.
- Nel caso di una gestione esterna della sicurezza informatica occorre concordare gli indici di prestazione (KPI), I livelli minimi di qualità del servizio fornito (SLA) e le penalità da applicare nel caso di mancata fornitura.

Messaggio

- La sicurezza (in particolare informatica) richiede una pianificazione (policy) e la definizione delle regole generali.
- La gestione dei sistemi informativi puó essere realizzata dal personale autorizzato o essere commissionata all'esterno.
- Nel caso di una gestione esterna della sicurezza informatica occorre concordare gli indici di prestazione (KPI), I livelli minimi di qualità del servizio fornito (SLA) e le penalità da applicare nel caso di mancata fornitura.
- Per la stipula di contratti convenienti occorre una corretta valutazione dei costi e benefici. Analisi del Rischio.

Messaggio

- La sicurezza (in particolare informatica) richiede una pianificazione (policy) e la definizione delle regole generali.
- La gestione dei sistemi informativi puó essere realizzata dal personale autorizzato o essere commissionata all'esterno.
- Nel caso di una gestione esterna della sicurezza informatica occorre concordare gli indici di prestazione (KPI), I livelli minimi di qualità del servizio fornito (SLA) e le penalità da applicare nel caso di mancata fornitura.
- Per la stipula di contratti convenienti occorre una corretta valutazione dei costi e benefici. Analisi del Rischio.
- Il metodo migliore per garantire la qualità della fornitura è la condivisione delle perdite (risk sharing) ma le compagnie che forniscono i servizi informatici normalmente non accettano questo genere di accordo.