Unità Didattica S
ISO 27001 SGSI

Docente: Ing. Rutilio Mazza

Cosa significa SGSI

- Sistema (modo di operare - metodo)
- Gestione (organizzazione - coordinamento di risorse in processi e attività)
- Sicurezza (**R**iservatezza – **I**ntegrità - **D**isponibilità)
- Informazioni (prescinde dalle modalità di archiviazione, dal supporto in cui l'informazione è riportata. Il supporto può essere elettronico, cartaceo, immateriale).

Stabilire il SGSI

- Campo di Applicazione e Limiti del SGSI
  (in riferimento al business, all'organizzazione ed ai processi, a beni e tecnologia adottata, alla localizzazione dell'organizzazione).
- Politica del SGSI
- Approccio alla valutazione del Rischio (metodo ripetibile, procedura)
- Identificare i rischi (per Riservatezza, Integrità e Disponibilità)
- Analizzare e ponderare i rischi (anche in relazione agli Incidenti)
- Identificare e ponderare le opzioni per il trattamento dei rischi
- Scegliere gli obiettivi di controllo e i controlli per il trattamento dei Rischi (Allegato A della ISO 27001)
- Ottenere l'approvazione della Direzione circa i rischi residui proposti
- Ottenere l'autorizzazione della Direzione per attuare e condurre il SGSI
- Predisporre una dichiarazione di Applicabilità (DdA o SoA)

Attuare e Condurre il SGSI

- Formulare e Attuare un piano di trattamento del rischio per conseguire gli obiettivi di controllo.
- Attuare i controlli per conseguire gli obiettivi di controllo.
- Misurare l'efficacia dei controlli
- Attuare programmi di formazione e addestramento
- Gestire Funzionamento e Risosrse del SGSI
- Attuare Procedure e controlli per individuare eventi relativi alla sicurezza e reagire agli incidenti.

Monitorare e Riesaminare il SGSI

a) Eseguire procedure di monitoraggio e di riesame;
b) Svolgere dei riesami regolari sull'efficacia del SGSI;
c) Misurare l'efficacia dei controlli;
d) Riesaminare le valutazioni del rischio a intervalli pianificati;
e) Condurre gli audit interni del SGSI a intervalli pianificati;
f) Effettuare un riesame da parte della direzione del SGSI;
g) Aggiornare i piani per la sicurezza;
h) Registrare le azioni e gli eventi che potrebbero avere un impatto sull'efficacia o sulle prestazioni del SGSI.

Mantenere attivo, aggiornato e migliorare il SGSI

a) Attuare i miglioramenti individuati.
b) Intraprendere le appropriate azioni correttive e preventive;
c) Applicare gli insegnamenti in materia di sicurezza acquisiti dalle esperienze di altre organizzazioni e dell'organizzazione stessa;
d) Comunicare le azioni e i miglioramenti a tutte le parti interessate;
e) Assicurarsi che i miglioramenti conseguano gli obiettivi prefissati.

Motori di un SGSI

- Inventario dei Beni e valorizzazione dei Beni
- Individuazione delle minacce ai beni
- Analisi dei Rischi per la Sicurezza delle Informazioni
- Analisi di BIA (Business Impact Analysis)
- BCP (Piano di Continuità del Business)
- Gestione degli Incidenti
- Conformità legislativa

Gestione dei Beni (Allegato A)

A.7.1 Responsabilità dei beni Obiettivo: Conseguire e mantenere attiva un'adeguata protezione dei beni dell'organizzazione.

A.7.1.1 Tutti i beni devono essere chiaramente identificati e deve essere compilato e mantenuto aggiornato un inventario di tutti i beni importanti.

A.7.1.2 Tutte le informazioni e i beni associati alle strutture di elaborazione delle informazioni devono essere sotto la "responsabilità"3) di una parte designata dell'organizzazione.

A.7.1.3 Le regole per un utilizzo accettabile delle informazioni e dei beni associati alle strutture di elaborazione delle informazioni, devono essere identificate, documentate e attuate.

A7.2 Classificazione delle informazioni Obiettivo: Assicurare che le informazioni ricevano un adeguato livello di protezione.

A.7.2.1 Le informazioni devono essere classificate in base al loro valore, alle prescrizioni legali, alla sensibilità e criticità nei confronti dell'organizzazione.

A.7.2.2 Deve essere sviluppato e attuato un appropriato insieme di procedure per l'etichettatura e il trattamento delle informazioni, in base allo schema di classificazione adottato dall'organizzazione.

Minacce

Accesso alla rete da parte di persone non autorizzate; Analisi dei traffici; Avaria dei componenti della rete; Avaria dei servizi di comunicazione; Avaria dei software; Avaria dell'impianto di condizionamento dell'aria; Avaria dell'hardware; Azioni industriali; Bombardamento; Carenza di personale; Contaminazione ambientale (e altre forme di disastro naturale o causato dall'uomo); Danni alle linee / ai cavi di comunicazione; Danni dolosi; Deterioramento dei dati memorizzati; Dirottamento di messaggi; Errore del personale operativo di supporto; Errore dell'utente; Errore di manutenzione; Errori di trasmissione; Estremi di temperatura e di umidità; Fluttuazioni di corrente; Fulmini; Furto; Import / export illegale di software; Incendio; Infiltrazione nelle comunicazioni; Inondazione; Mascheramento dell'identità dell'utente; Misconoscimento (per esempio di servizi, transazioni, messaggi inviati /ricevuti); Origliate; Particelle sospese / polvere; Software dolosi (come virus, Cavalli di Troia); Sospensione del rifornimento d'acqua; Sospensione del rifornimento di corrente; Sovraccarico dei traffici; Terremoto; Uragano; Uso di software da parte di utenti non autorizzat; Uso di software in modo non autorizzato; Uso illegale di software; Uso improprio delle risorse; Uso non autorizzato dei mezzi di memorizzazione; Uso non autorizzato della rete; Uso non autorizzato di software …

… naturalmente sono solo esempi.

Vulnerabilità

Assenza di personale; Avaria nell'anello debole; Carenza di controllo efficace dei cambienti; Carenza di documentazione; Carenza di meccanismi di identificazione e di autorizzazione come l'autenticazione dell'utente; Carenza di meccanismi di monitoraggio; Carenza di politiche per il corretto uso dei mezzi di telecomunicazione e di messaggeria; Carenza di programmi di sostituzione periodica delle attrezzature; Carenza di protezione fisica per gli edifici, le porte e le finestre; Carenza di prove dell'invio o della ricezione di un messaggio; Carenza di sensibilizzazione inerente la sicurezza; Carenza di tracce di audit; Cattiva gestione delle password (password facilmente indovinabili, memorizzazione di password, insufficiente frequenza di cambiamenti); Connessioni a reti pubbliche non protette; Copie non controllate; Distribuzione errata dei diritti di accesso; Gestione inadeguata della rete; Giunture difettose dei cavi; Griglia elettrica instabile; Insufficiente formazione per la sicurezza; Interfaccia utente complicata; Lavoro senza supervisione da parte del personale esterno per le pulizie; Linee a composizione automatica; Linee di comunicazione non protette; Magazzini non protetti; Mancato log-out quando si abbandona la postazione di lavoro; Mancato o insufficiente collaudo di software; Mantenimento insufficiente/ installazione difettosa di di mezzi di memorizzazione; Negligenza di smaltimento; Pecche ben note nel software; Procedure di reclutamento inadeguate; Scaricamento e uso non controllati di software; Smaltimento o riutilizzo di mezzi di memorizzazione senza appropriata cancellazione; Software con documentazione insufficiente; Specifiche per gli sviluppatori non chiare o incomplete; Suscettibilità delle attrezzature a umidità, polvere, sporcizia; Suscettibilità delle attrezzature a variazioni di voltaggio; Suscettibilità delle attrezzature alle variazioni di temperatura; Tabelle delle password non protette; Traffico delicato non protetto; Trasferimento delle password in chiaro; Ubicazione in area suscettibile a inondazioni; Uso inadeguato o negligente del controllo accessi agli edifici, alle stanze e agli uffici …

… naturalmente sono solo esempi.

Impatti, Incidenti potenziali

Cambiamenti accidentali o non voluti a software e dati condivisi in ambiente informatico; Infrazione della sicurezza dovuta a non conformità alle procedure operative; Infrazione della sicurezza dovuta a procedure operative imprecise, incomplete o inappropriate o alla definizione delle responsabilità o a insufficienti aggiornamenti di tali procedure; Infrazione della sicurezza dovuta a non conformità con le procedure per il trattamento degli incidenti; Compromesso, danno o perdita di dati presso un contraente; Danni dovuti a piani per la continuità imprecisi, incompleti o inappropriati, a collaudi insufficienti o ad aggiornamenti insufficienti dei piani; Negazione del servizio, di risorse per il sistema, di informazioni; Bombardamento via e-mail; Falsificazione; Frode; Uso improprio negligente o deliberato degli impianti dovuto a carenza di segregazione e di esecuzione dei doveri; Divulgazione non autorizzata dell'ubicazione di siti / edifici/ uffici contenenti impianti di elaborazione e informatici critici e/o delicati; Divulgazione non autorizzata delle informazioni …

… naturalmente …

Analisi dei Rischi

Identificare i rischi:

1. i beni e i responsabili dei beni;
2. le minacce;
3. le vulnerabilità;
4. gli impatti o incidenti potenziali (per Riservatezza Integrità Disponibilità).

Analizzare e ponderare i rischi:

1. valutare l'impatto sul Business di malfunzionamenti della sicurezza (RID);
2. valutare la probabilità di accadimento di malfunzionamenti della sicurezza;
3. stimare i livelli dei rischi;
4. stabilire se i rischi siano accettabili o se richiedano un trattamento.

Identificare e ponderare le opzioni per il trattamento dei rischi:

1. applicare controlli;
2. accettare i rischi in modo consapevole e obiettivo;
3. evitare i rischi;
4. trasferire i rischi associati al business ad altre parti.

BIA e BCP (Allegato A)

Business Impact Analysis e Business Continuity Plan

A.14 GESTIONE DELLA CONTINUITÀ OPERATIVA

A.14.1 Aspetti di sicurezza delle informazioni relativi alla gestione della continuità operativa Obiettivo: Contrastare le interruzioni delle attività relative al business, proteggerne i processi critici dagli effetti di malfunzionamenti significativi dei sistemi informativi o da disastri e assicurare il loro tempestivo ripristino.

A.14.1.1 Deve essere sviluppato e mantenuto attivo un processo per la gestione della continuità operativa in tutta l'organizzazione, che prenda in considerazione i requisiti di sicurezza delle informazioni necessari per la continuità operativa dell'organizzazione.

A.14.1.2 Si devono identificare gli eventi che possono causare interruzioni ai processi relativi al business, unitamente alle probabilità e agli impatti di tali interruzioni e alle loro conseguenze per la sicurezza delle informazioni.

A.14.1.3 A seguito di interruzioni o malfunzionamenti nei processi critici relativi al business, devono essere sviluppati e attuati piani per mantenere o ripristinare il funzionamento e per assicurare la disponibilità delle informazioni al livello e nei tempi richiesti,

A.14.1.4 Deve essere mantenuta una singola struttura metodologica di supporto per piani di continuità operativa al fine di assicurare che tutti i piani siano coerenti, considerare in maniera coerente i requisiti di sicurezza delle informazioni e identificare le priorità ai fini dei test e della manutenzione.

A.14.1.5 I piani di continuità operativa devono essere testati e aggiornati regolarmente, per assicurare che siano aggiornati ed efficaci.

Gestione degli Incidenti (Allegato A)

A.13 GESTIONE DEGLI INCIDENTI RELATIVI ALLA SICUREZZA DELLE INFORMAZIONIA.

13.1 Segnalazione degli eventi e dei punti di debolezza relativi alla sicurezza delle informazioni Obiettivo: Assicurare che gli eventi relativi alla sicurezza delle informazioni e i punti di debolezza dei sistemi informativi siano segnalati in modo da permettere tempestive azioni correttive.

A.13.1.1 Gli eventi relativi alla sicurezza delle informazioni devono essere segnalati il più velocemente possibile attraverso appropriati canali direzionali.

A.13.1.2 A tutti i dipendenti, collaboratori e utenti di terze parti dei sistemi e servizi informativi, deve essere richiesto di registrare e segnalare ogni debolezza osservata o sospettata nei sistemi o nei servizi.

A.13.2 Gestione degli incidenti relativi alla sicurezza delle informazioni e dei miglioramenti Obiettivo: Assicurare l'applicazione di un approccio coerente ed efficace per la gestione degli incidenti relativi alla sicurezza delle informazioni.

A.13.2.1 Devono essere stabilite le responsabilità di gestione e le procedure per assicurare una risposta rapida, efficace e ordinata agli incidenti relativi alla sicurezza delle informazioni.

A.13.2.2 Devono essere attivati dei meccanismi per quantificare e monitorare le tipologie, i volumi e i costi degli incidenti relativi alla sicurezza delle informazioni.

A.13.2.3 Qualora, a seguito di un incidente relativo alla sicurezza delle informazioni, risulti necessario intraprendere un'azione legale (civile o penale) contro una persona fisica o giuridica, le evidenze oggettive devono essere raccolte, conservate e presentate, al fine di conformarsi ai requisiti di legge applicabili nella/e giurisdizione/i pertinente/i.

Conformità legislativa

- **Proprietà intellettuale**, in particolare software originale, licenze d'uso… (L. 633/41, artt. 1, 12 ss., 171 ss.; d.lgs. 196/03);
- **Gestione delle registrazione contabili:** in particolare per conservazione sostitutiva e fatturazione elettronica … (D.p.r. 600/73, Codice civile art. 2220, D.lgs. 52/2004, D.lgs. 82/2005 artt. 39 e 71, Deliberazione CNIPA 11/2004, Circolare dell'Agenzia delle entrate n. 36/2006, Risoluzioni dell'Agenzia delle entrate nn. 158/E/09, 194/E/09, 195/E/09, 196/E/09);
- **Misure Minime di Sicurezza (strumenti non elettronici):** … (D.lgs. 196/03, artt. 33-36 e all. B, 27-29);
- **Misure Minime di Sicurezza (strumenti elettronici):** in particolare: accesso agli strumenti informatici protetto; credenziali strettamente individuali; parole chiave di lunghezza non inferiore a 8 caratteri e cambiate ogni 6 mesi; sistemi di autenticazione e di autorizzazione; presenza di strumenti di protezione (es. firewall e antivirus), aggiornati con cadenza almeno semestrale; aggiornamenti periodici dei programmi per risolvere le vulnerabilità … (D.lgs. 196/03, artt. 33-36 e all. B, 1-26);
- **Dati sensibili e giudiziari:** autorizzazione al trattamento, del Garante Privacy, anche a carattere generale; **Redazione del DPS** entro il 31 marzo di ogni anno, tecniche di cifratura ... (D.lgs. 196/03, artt. 33-36 e all. B)
- **Prevenzione per l'utilizzo non appropriato degli elaboratori:** … per scopi non autorizzati, Policy adeguate, comunicate… (D.lgs. 196/03, Linee guida Garante privacy per posta elettronica e Internet del 01/03/2007, l. 300/70 artt. 4 e 8, Provvedimento generale Garante privacy sulla videosorveglianza del 29/04/2004).
- **Attribuzioni delle funzioni di amministratore di sistema**: Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici … (Provvedimento del Garante del 27 novembre 2008 e successive modifiche (25 giugno 2009) e precisazioni (10 dicembre 2009) e comunicati (14 gennaio 2009))

SANS

Il sito di SANS (SysAdmin, Audit, Network, Security) fornisce gratuitamente:

- "Top Security Risks";
- "Top 25 programming errors";
- "Top 10 security Trends";
- "Top 5 essential log report";
- ed altro …;

http://www.sans.org/

Altri links utili

- ENISA (European Network and Information Security Agency)
  http://www.enisa.europa.eu/
- PILAR in Italia (SW libero per la gestione della Analisi dei Rischi)
  http://www.sgsi.net/
- Forum sulla ISO/IEC 27000
  http://www.iso27001security.com/
- IT Governance Institute (IS0/IEC 38500:2008)
  http://www.itgi.org/

Altri riferimenti normativi

ISO/IEC 27002: 2005
Information technology — Security techniques — Code of practice for information security management

ISO IEC 27005:2008
Information technology — Security techniques — Information security risk management

ISO/IEC TR 18044:2004
Information technology — Security techniques — Information security incident management

ISO/IEC TR 13335-5
Information technology — Guidelines for the management of IT Security — Part 5: Management guidance on network security

BS 25999-1:2006
Business continuity management. Code of practice

BS 25999-2:2007
Business continuity management. Specification