

INDICE

INDICE

PRESENTAZIONE

INTRODUZIONE

GUIDA ALLA LETTURA DI QUESTO LIBRO

DEFINIZIONI

Di cosa stiamo parlando

Normativa

Standard

Altre definizioni

DORA (Digital Operational Resilience Act)

Perché DORA

Aree di intervento

Ambito di applicazione

Le sanzioni

Articolazione della norma

LA RACCOLTA DELLE INFORMAZIONI

Tecniche di raccolta dei dati

La verifica documentale

Fonti dati sulle risorse

I RISCHI

Il concetto di rischio

Tipologia di rischi

I rischi di soggetti terzi in carico all'organizzazione

Il rischio di terza e quarta parte

I limiti dei modelli

ASSET – PROCESSI - SERVIZI

Identificazione

Gli asset dal punto di vista dell'azienda

La conoscenza

La classificazione delle informazioni

I documenti

I documenti elettronici

Il sistema informativo

Il ciclo di vita delle informazioni

Il capitale umano

Competenze/Conoscenze

Altri asset immateriali

La collocazione degli asset aziendali

Correlazione fra gli asset

Struttura gerarchica

Cataloghi di asset

Le informazioni da raccogliere in ambito ICT
Mappatura del sistema informativo
Il livello di analiticità nella mappatura degli asset
I servizi
I processi
Cataloghi di processi
Le finalità di trattamento
Cataloghi delle finalità
La rilevazione dei flussi documentali
La mappatura funzionale
Strumenti

LE MINACCE E LE VULNERABILITÀ

Gli eventi di minaccia
Classificazione delle fonti di minacce
Le Vulnerabilità
Cataloghi delle minacce e delle vulnerabilità

GLI SCENARI DI RISCHIO PER LA CONTINUITÀ OPERATIVA

Normativa banche
Pubblica amministrazione
Esempi di scenari, eventi ed asset coinvolti
Nuovi rischi – i rischi climatici

LA GESTIONE DEL RISCHIO

Standard per la gestione del rischio
Metodologie per la gestione del rischio
I ruoli nella gestione dei rischi

LA VALUTAZIONE DEGLI IMPATTI

Esempi di scale di impatto

LA BIA (BUSINESS IMPACT ANALYSIS)

Definizione della metodologia con cui eseguire una BIA
Individuare i servizi/prodotti
La valutazione dell'rpo
Punti di attenzione
Analisi del rischio e bia

LA VALUTAZIONE DELLA PROBABILITÀ

L'ANALISI DEI RISCHI

Un approccio all'analisi del rischio a più livelli
Terminologia dell'analisi dei rischi
Metodologie per l'analisi dei rischi
Aspetti trasversali nella analisi dei rischi
Fasi dell'analisi dei rischi

AGGREGAZIONI E CORRELAZIONI DEI RISCHI

Somma dei rischi e Calcolo della rischiosità totale
Rischi indipendenti
Rischi correlati

IL TRATTAMENTO DEL RISCHIO

L'attivazione delle contromisure
Il trasferimento del rischio
Il ciclo dell'analisi del rischio

LE MISURE DI SICUREZZA

[Classificazione delle Misure di Sicurezza](#)

[Ciclo di vita delle misure di sicurezza](#)

[Coerenza nelle contromisure](#)

[Differenza nelle contromisure](#)

[Framework di sicurezza](#)

Quadro per la gestione dei rischi informatici

[Cataloghi delle misure di sicurezza](#)

[Misure di sicurezza - Policy e Procedure](#)

[Costi delle misure di sicurezza](#)

MISURARE

[Metriche e misure](#)

[Tipologia di misure di sicurezza](#)

[Lead e Lag indicators](#)

[Metriche di resilienza](#)

[Misurare i processi ICT](#)

[CIRCOLARE N. 3 del 9 aprile 2018](#)

[Criteri per la qualificazione di servizi SaaS per il Cloud della PA](#)

[Maturity Model](#)

[Cataloghi di misure in ambito sicurezza](#)

[MITRE - Cyber Resiliency Metrics, Version 1.0, Rev. 1 - Appendix B Representative](#)

[Set of Cyber Resiliency Metrics](#)

[Software Engineering Institute - Measures for Managing Operational Resilience -](#)

[Appendix](#)

[Resilience Measures](#)

[Basel Committee on Banking Supervision December 2018 Cyber-resilience: Range of practices](#)

[Service level agreement](#)

[Security maturity model](#)

[FFIEC - Cybersecurity Assessment Tool](#)

INCIDENTI

[Normativa in ambito ICT](#)

[Gli incidenti nell'ambito della resilienza operativa](#)

[Perimetro di applicazione Degli incidenti ICT](#)

[Esempi di incidenti](#)

[Procedura di gestione degli incidenti](#)

[I ruoli nella gestione degli incidenti](#)

[Livello di maturità nella gestione degli incidenti](#)

RUOLI

[Normativa in ambito BC](#)

[Normativa in ambito cybersecurity](#)

IL PIANO DI BC

[Normativa banche](#)

[I contenuti del piano](#)

[Intervallo temporale di riferimento](#)

[Piani alternativi](#)

[L'organizzazione della documentazione a supporto del piano](#)

[La gestione dei documenti del piano di bc](#)

[L'aggiornamento del piano di BC](#)

[Resilienza by design](#)

[I piani per l'indisponibilità del sistema informativo](#)

Disponibilità della documentazione in caso di crisi

Punti di attenzione: bc

Rischi residui

Esempi di indici di piani

Esempi piano di dr

LA GESTIONE DELLA CRISI

Dall'incidente alla gestione della emergenza e della crisi

Lo stato di crisi

Piano di bc: comunicazioni

LE SOLUZIONI PER IL SISTEMA INFORMATIVO

Normativa banche

Indisponibilità del sistema informativo

Alcuni parametri

Punti di attenzione

Alta affidabilità (alta disponibilità)

Punti di attenzione

Soluzioni: DR

Punti di attenzione: dr

Possibili requisiti del sito di dr

Attacco cyber

Normativa

Individuazione

Effetti di un attacco Ransomware

Fasi di un attacco ransomware

Azioni preventive e successive

Policy per il backup

LE SOLUZIONI

Normative banche

Le soluzioni per essere resilienti

FORNITORI E OUTSOURCER

PRINCIPALI DISPOSIZIONI CONTRATTUALI

I rischi fornitori

I fornitori in ambito CLOUD

I rischi dei fornitori

La valutazione puntuale del fornitore

La valutazione del fornitore da parte di enti XXXXX

La valutazione volontaria

Azioni da svolgere nella relazione con i fornitori

Gli aspetti contrattuali

La scelta del fornitore

TEST

I test di resilienza

Tipologie di test di resilienza

Test e le verifiche della continuità operativa

Test e verifiche

Guida all'esecuzione dei test

Check list di spunta dei test

LA FORMAZIONE

Normativa bancaria

GLI STANDARD

Standard - ISO

LE NORMATIVE