Prime

ISF – GERENCIAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Definições de Incidentes

Incidente de Segurança da Informação:

- Ocorre quando fere o elemento de confiabilidade da informação: Confidencialidade, Integridade e Disponibilidade;
- É indicado por um único ou uma série de eventos indesejados ou inesperados de Segurança da Informação;
- Possui uma probabilidade significativa de comprometer a operação do negócio e ameaça a Segurança da Informação;
- Ocorre quando uma ameaça se manifesta. Exemplo: Um hacker consegue invadir a rede da empresa.

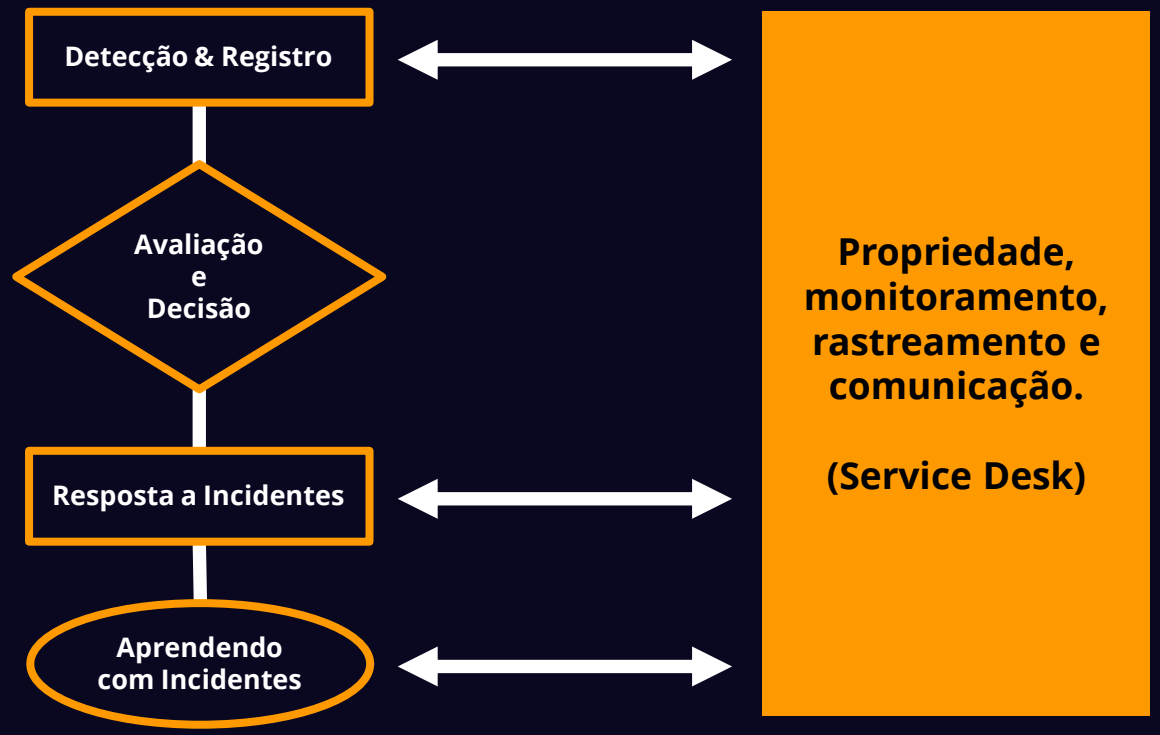
Desastre de Segurança da Informação:

- Um ou mais incidentes ameaçam a continuidade de Segurança da Informação da empresa;
- Exemplo: Um ou mais hackers apagam ou destroem ativos críticos da segurança da informação, causando uma grande perda de acesso à informação.

Gerenciamento de Incidentes da Segurança da Informação

- Garantir uma abordagem coerente e eficaz para a gestão de incidentes da informação da segurança, incluindo comunicação dos eventos de segurança e das fraquezas.

Macro Etapas do **Processo de Gestão de Incidentes**



Controle: Planejamento e Preparação do Gerenciamento de Incidentes de Segurança da Informação

Objetivo:

Garantir uma resposta rápida, eficaz, consistente e ordenada a incidentes de segurança da informação, incluindo comunicação sobre eventos de segurança da informação.

O que precisamos fazer para garantir uma rápida resposta?

1. Definir papéis e responsabilidades;
2. Procedimentos do gerenciamento de incidentes;
3. Procedimentos de emissão de relatórios.

Considerações

- Os incidentes de segurança da informação podem transcender as fronteiras organizacionais e nacionais.
- Orientações detalhadas sobre gerenciamento de incidentes de segurança da informação são fornecidas na série ISO/IEC 27035.

Procedimentos e Responsabilidades no **Gerenciamento de Incidentes**

Deve-se considerar o seguinte:

- Um método comum para que todos possam relatar eventos de segurança da informação;
- Incluir um ponto de contato, como uma Central de Serviços;
- Estabelecer um processo de gerenciamento de incidentes para:
  - Administração;
  - Documentação;
  - Detecção;
  - Triagem;
  - Priorização;
  - Análise;
  - Comunicação;
  - Coordenação das partes interessadas;
- Processo de resposta a incidentes;
- Permitir apenas que pessoal competente lide com as questões relacionadas a incidentes de segurança da informação;
- Processo para identificar a formação, certificação e desenvolvimento para o pessoal que lida com resposta a incidentes.

Procedimentos de **Gerenciamento de Incidentes**

Deve ser criado um conjunto de procedimentos para eventos e incidentes de segurança da informação, como:

- Avaliação, monitoramento, detecção, classificação, análise e reporte;
- Coordenação com partes interessadas internas e externas, como autoridades, interesses externos, grupos, fóruns, fornecedores e clientes;
- Registro de atividades de gerenciamento de incidentes;
- Coleta de evidências;
- Análise de causa raiz;
- Identificação das lições aprendidas e quaisquer melhorias nos procedimentos.

Procedimentos de **Gerenciamento de Incidentes**

Detalhes:

Por meios humanos ou automáticos;

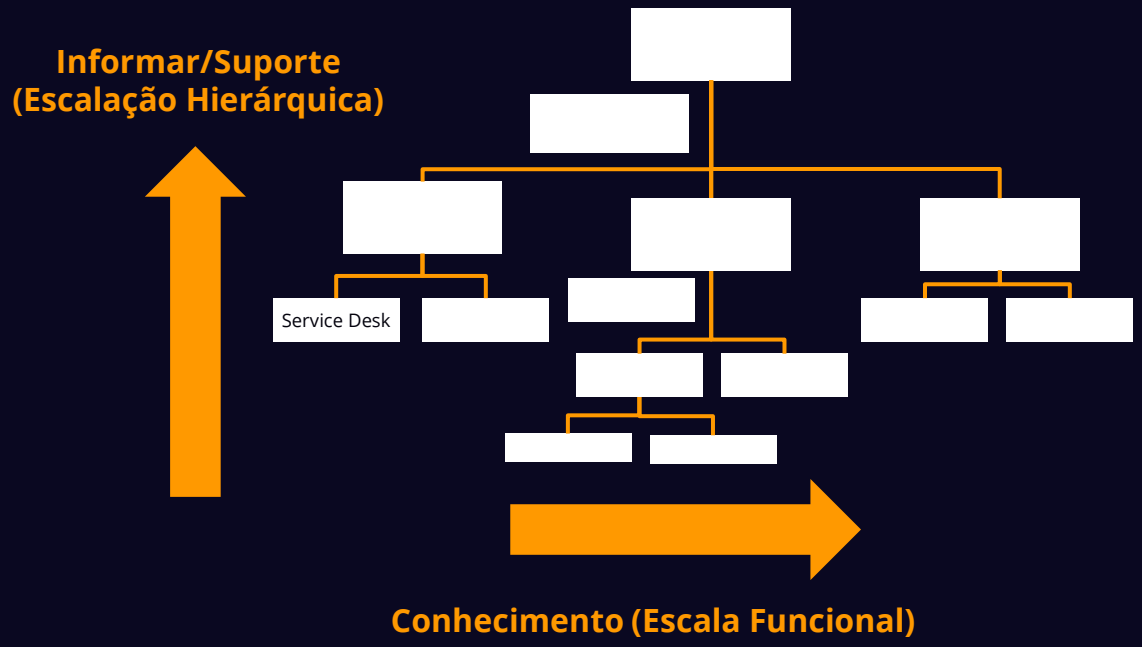
Gerenciar incidentes de segurança da informação até a conclusão;

Incluir procedimento de escalonamento por tipo:

- ✓ De categoria do incidente;
- ✓ Para ativação do gerenciamento de crises;
- ✓ Para ativação de planos de continuidade;
- ✓ Recuperação de um incidente;
- ✓ Comunicação às partes interessadas externas.

Reportando **Incidentes de Segurança**

- Todos os funcionários da empresa têm um papel importante na detecção e reporte, afinal, são os primeiros a verem um incidente de segurança.



Reporte dos **Incidentes de Segurança**

Os relatórios devem ser usados como:

- Uma forma de aprender (evitar novos incidentes)
- Reportar incidentes

Os relatórios devem registrar:


Data e hora


Nome da pessoa que reporta o incidente


Localização (onde foi o incidente?)


Qual é o problema?


Qual é o efeito que o incidente causou?


Como foi descoberto?

Exemplos de **Incidentes de Segurança**

- Nenhuma manutenção é realizada no equipamento;
- A fonte de energia de emergência não foi testada;
- Um colega perde um laptop;
- Um colega não aderiu à política de mesa limpa;
- Um colega traz um visitante não autorizado;
- O novo software é publicado antes de ser testado;
- Um vírus conseguiu entrar em um sistema;
- Devido a dados incompletos da empresa, os resultados do lucro não são confiáveis;
- Os direitos de acesso de um trabalhador não são modificados após a sua demissão;
- Colegas escrevem suas senhas em papel e deixam embaixo do teclado;
- Foram encontradas imagens de pornografia infantil no computador de um colega (o relato deve ser feito com cuidado para assegurar que nenhuma evidência seja removida).

Instruções

Um procedimento contém instruções do que fazer diante de um incidente

Procedimento sobre o que fazer deve incluir:

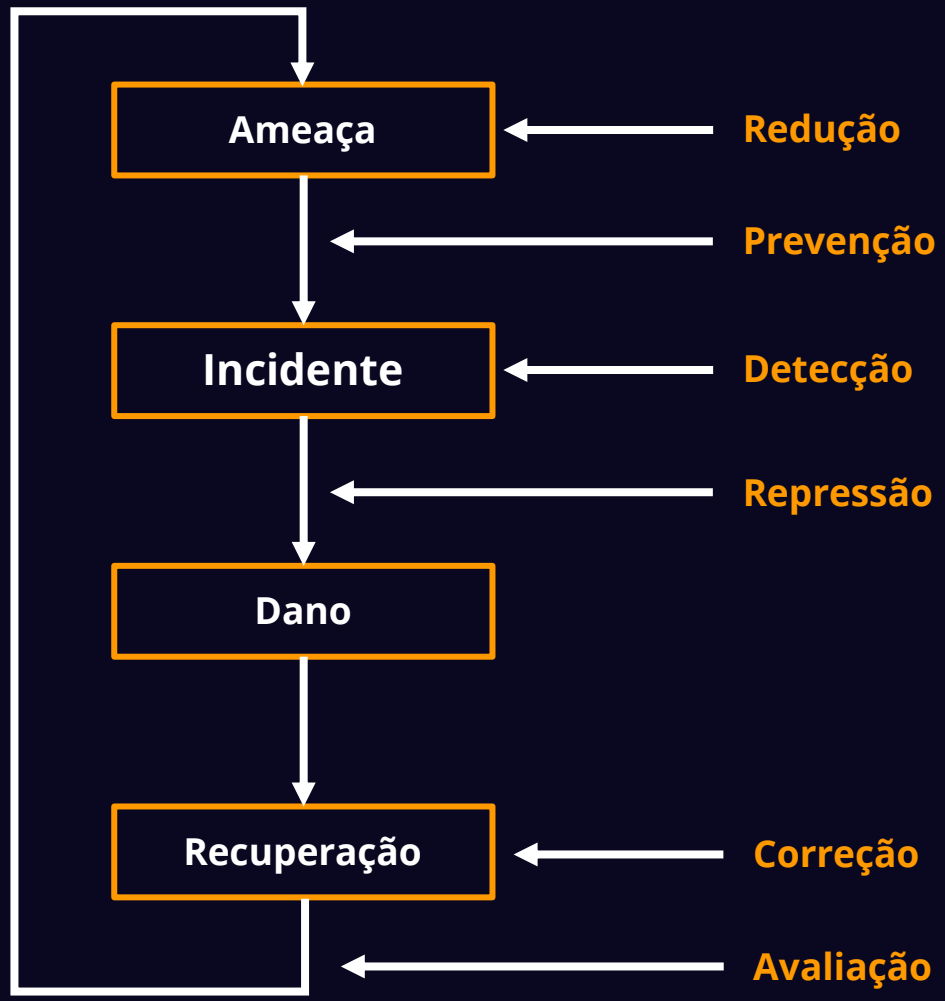
- Análise do incidente e sua causa;
- Medidas para minimizar as consequências do incidente;
- Medidas para determinar se as medidas corretivas são necessárias para evitar que o incidente ocorra novamente;
- Quais partes devem ser informadas em caso de incidente. (aqueles afetados ou que ajudam a resolver o incidente);
- O que é relatado sobre o incidente e para quem.

Reportando **Fraquezas de Segurança**

- Reportar fraquezas e deficiências, o mais cedo possível;
- Cuidado para que as provas não sejam destruídas, quer intencionalmente ou não;
- O relatório do incidente deve constar as suspeitas de deficiência;
- Em seguida, solicitar ajuda ao pessoal especializado para tomarem as medidas cabíveis;
- É possível que um advogado ou a polícia precise ser envolvido em um estágio inicial para que as provas sejam recolhidas.

Medidas no **Ciclo de Vida do Incidente**

Não é o mesmo processo do NIST: Preparação / Identificação e Análise / Contenção, Erradicação e Recuperação / Atividade Pós-Evento



Controle: Avaliação e Decisão sobre Eventos de Segurança da Informação

Objetivo:

Garantir a categorização e priorização efetivas dos eventos de segurança da informação.

O que é categorizar incidentes?

- É separar por tipo;
- Serve para delegar ou escalonar certos tipos de incidentes;
- É baseado no catálogo de serviços.

Controle: Avaliação e Decisão sobre Eventos de Segurança da Informação

O que é priorizar incidentes?

- É organizar por impacto e urgência;
- Baseado em uma matriz da análise de risco.

Considerações

- Este processo deve ser pensado antes e não durante o incidente;
- Normalmente executado pelo Service Desk, através de procedimentos;
- As decisões devem ser registradas em tickets, chamados etc.
- ISO/IEC 27035 fornece orientações adicionais sobre gerenciamento de incidentes.

Controle: Resposta a Incidentes de Segurança da Informação

Objetivo:

Garantir uma resposta eficiente e eficaz a incidentes de segurança da informação.

O que significa “responder a um incidente”?

- É lidar com o incidente, tratá-lo, aplicar as medidas;
- É conter o incidente, ou seja, suas consequências, evitar que se espalhem;
- Coletar provas;
- Escalonar, conforme necessário, para:
  - ✓ Segundo e terceiro níveis;
  - ✓ Plano de Continuidade de Negócios;
  - ✓ Plano de Gerenciamento de Crises.
- Registrar todas as ações para análise posterior;
- Comunicar detalhes importantes para as partes interessadas;
- Coordenar ações com autoridades, partes externas, fornecedores, clientes etc.;
- Quando resolvido, encerrar e documentar;
- Realizar a análise forense de segurança da informação, conforme necessário;
- Realizar análise pós-incidente para identificar a causa raiz;
- Identificar e gerenciar vulnerabilidades e fraquezas de segurança da informação;
- Identificar os controles que causaram, contribuíram ou falharam na prevenção do incidente.

Controle: Aprendendo com Incidentes de Segurança da Informação

Objetivo:

Reduzir a probabilidade ou consequências de incidentes futuros.

O que devemos aprender neste momento?

- Todas as lições aprendidas com incidentes resolvidos;
- Mais informações para quantificar e monitorar os tipos, volumes e custos dos incidentes de SI;
- Novas informações obtidas com a avaliação de incidentes;
- Aprimorar o plano e procedimentos de gerenciamento de incidentes;
- Identificar incidentes recorrentes ou graves;
- Identificar causas-raiz para atualizar a avaliação de risco;
- Determinar e implementar controles adicionais para reduzir a probabilidade ou consequências de futuros incidentes semelhantes;
- Conscientização e o treinamento do usuário através de exemplos.

Controle: Coleta de Evidências

Objetivo:

Assegurar uma gestão consistente e eficaz das provas relacionadas com incidentes de segurança da informação para efeitos de ações disciplinares e legais.

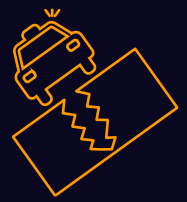
Essas evidências só terão valor legal se:

- Os registros estão completos e não foram adulterados de forma alguma;
- As cópias das provas eletrônicas são idênticas aos originais;
- A evidência foi coletada de um sistema que estava funcionando corretamente no momento em que as provas foram registradas.

Considerações

- Garantia de que a organização tem direito de coletar informações como evidências;
- É aconselhável o envolvimento jurídico ou aplicação da lei no início de qualquer ação legal;
- Desenvolva um procedimento para coleta de evidências antes de colocá-lo em prática.

Continuidade e Desastres



O que são Desastres?

- Uma inundação
- Falha em um sistema
- Falha de energia
- Placa de rede com defeito

Plano de evacuação

- Em caso de uma falha em um sistema, contate o Service Desk;
- Onde estão as saídas de emergência no edifício;
- Qual o telefone de emergência em caso de incêndio;
- Como acionar o sistema sprinkler ou um alerta de incêndio.

Por Que Gestão de Continuidade de Negócios?

- Proteção de processos de negócios;
- Continuidade de serviço;
- Sobrevivência da companhia;
- Lucro ou perda;
- Publicidade negativa.

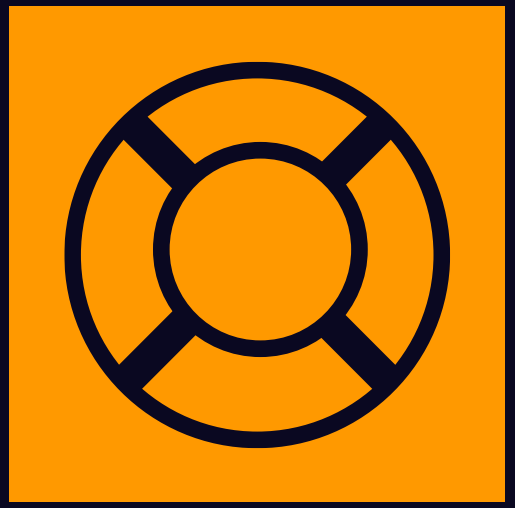
Gerenciamento de **Continuidade de Negócio**

O objetivo do Business Continuity Management (BCM) é evitar que as atividades empresariais sejam interrompidas, protegendo os processos críticos contra as consequências e interrupções em sistemas de informação e permitir a rápida recuperação.

DRP – Disaster Recovery Planning (PRD)

BPC – Business Continuity Planning (PCN)

DRP e BCP



DRP	BCP
Executa enquanto o desastre está em curso;	Executa com a finalidade de voltar ao normal;
Existe agora um desastre e tenho que voltar a trabalhar;	Nós tivemos um desastre e tenho que voltar à situação de como era antes do desastre.
Minimizar as consequências de um desastre;	Métodos e procedimentos também estão dispostos para falhas que podem durar um longo tempo.
Mais focado em ativos, processos e funcionários;	Mais abrangente, ou seja, no negócio como um todo;
Pensa no agora!	Pensa no futuro!
Toma medidas para a voltar a operação normal em um tempo aceitável.	Visa um local alternativo, mais focado na continuidade, mesmo que parcialmente.

Redundâncias e **Locais Alternativos**

Redundâncias:

Objetivo:

Garantir a disponibilidade de instalações de processamento de informações.

Local Alternativo

- Site Redundante: Para empresas que têm diversas localidades e um único Data Center;
- Hot Site sob demanda: Site Móvel.

Ações e Considerações

- Teste o BCP, já que as catástrofes não acontecem só com os outros;
- Mudanças nos processo de negócios devem refletir no BCP. Um plano ultrapassado não irá ajudar a organização a se tornar operacional novamente;
- Pessoas são ativos da empresa, consequentemente podem não estar mais disponíveis após um desastre;
- É essencial que sejam testados simulando uma situação da vida real para verificar se essas medidas são de fato corretas e eficazes.

Controle: Segurança da Informação Durante a Interrupção

Objetivo:

Para proteger as informações e outros ativos associados durante a interrupção por meio de um Disaster Recovery Planning – DRP e Business Continuity Planning - BCP.

Qual o objetivo de um DRP e BCP?

- Manter ou restaurar a segurança das informações de processos críticos de negócios após interrupção ou falha;
- Restaurar as informações no nível e nos prazos exigidos;

Controle: Segurança da Informação Durante a Interrupção

O que tem dentro do DRP e BCP?

- Controles de segurança da informação;
- Sistemas e ferramentas de suporte dentro da continuidade de negócios;
- Planos de continuidade de TIC;
- Processos e procedimentos que são (e não são) executados durante a interrupção.

Considerações

- Não esquecer da Análise de Impacto nos Negócios (BIA);
- Não esquecer da Avaliação de Riscos e as consequências da perda do CID;
- Informações sobre continuidade de negócios: ISO 22301 e ISO 22313;
- Mais orientações sobre análise de impacto nos negócios (BIA) ISO/TS 22317.

Controle: Prontidão de TIC para Continuidade de Negócios

Objetivo:

Durante uma interrupção, a TIC deve estar de prontidão, conforme os requisitos levantados da análise de impacto nos negócios (BIA).

O que é BIA?

BIA

- Processo que determina os critérios de impacto de negócios;
- Serve para avaliar os impactos ao longo do tempo resultantes da interrupção;
- Determina quais recursos são necessários para apoiar as atividades priorizadas;
- Define requisitos de desempenho e capacidade de sistemas de TIC;
- Usa duas grandes métricas:
  - ✓ Objetivo de tempo de recuperação (RTO);
  - ✓ Objetivos de ponto de recuperação (RPO).

Controle: Prontidão de TIC para Continuidade de Negócios

Qual o resultado da BIA e avaliação de risco?

- Identificação e seleção das estratégias de continuidade de TIC antes, durante e após a interrupção;
- Definição das estratégias de continuidade de negócios;
- Ponto de partida para elaboração dos planos.

Considerações

- Inclua procedimentos detalhados de resposta e recuperação;
- Avalie regularmente por meio de exercícios e testes;
- Aprove os planos com a administração.

OBRIGADO

ISF – GERENCIAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO