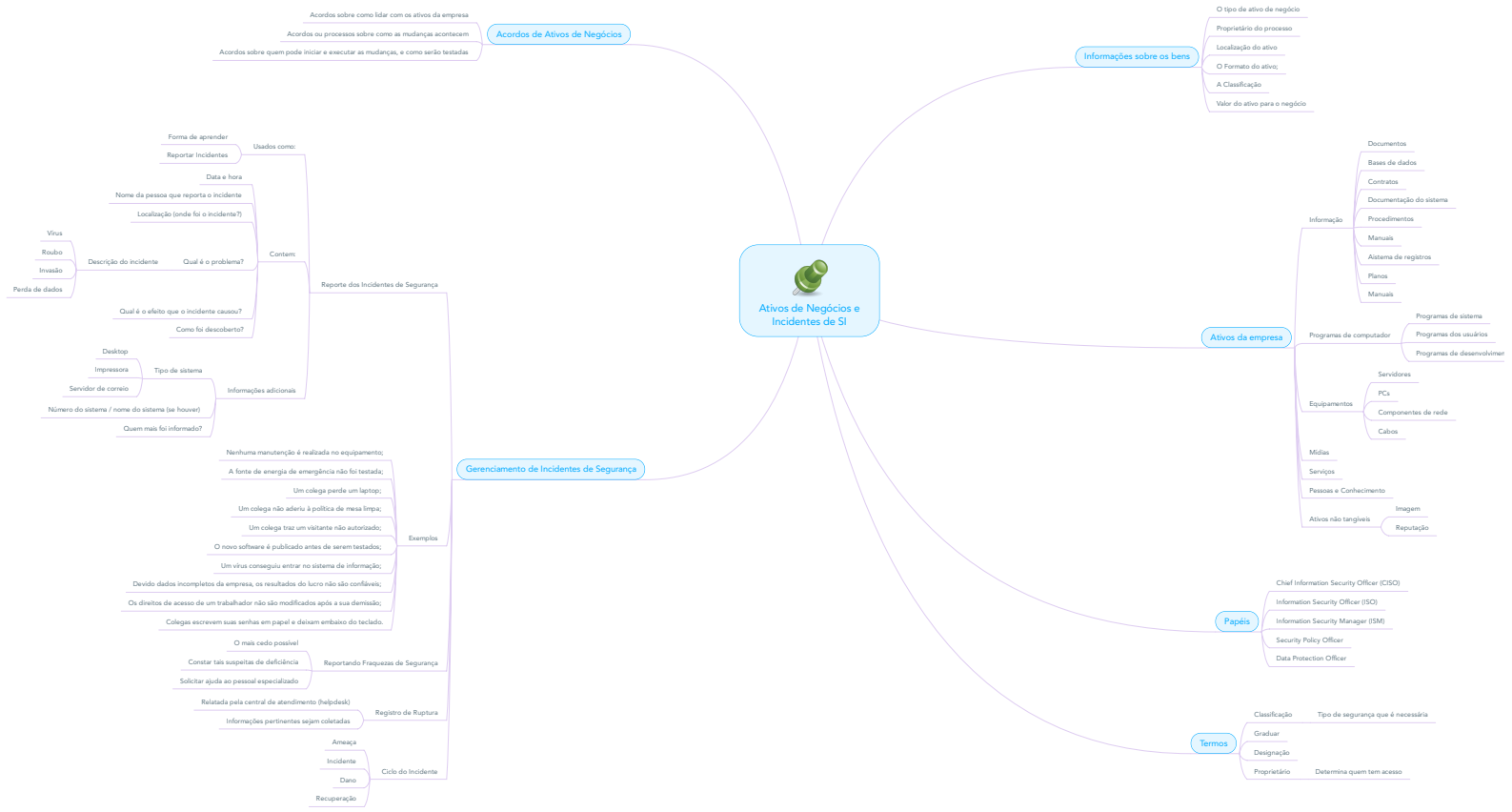
Ativos de Negócios e Incidentes de SI
Acordos de Ativos de Negócios
Acordos sobre como lidar com os ativos da empresa
Acordos ou processos sobre como as mudanças acontecem
Acordos sobre quem pode iniciar e executar as mudanças, e como serão testadas
Informações sobre os bens
O tipo de ativo de negócio
Proprietário do processo
Localização do ativo
O Formato do ativo;
A Classificação
Valor do ativo para o negócio
Ativos da empresa
Informação
Documentos
Bases de dados
Contratos
Documentação do sistema
Procedimentos
Manuais
Aistema de registros
Planos
Manuais
Programas de computador
Programas de sistema
Programas dos usuários
Programas de desenvolvimer
Equipamentos
Servidores
PCs
Componentes de rede
Cabos
Mídias
Serviços
Pessoas e Conhecimento
Ativos não tangíveis
Imagem
Reputação
Papéis
Chief Information Security Officer (CISO)
Information Security Officer (ISO)
Information Security Manager (ISM)
Security Policy Officer
Data Protection Officer
Termos
Classificação
Tipo de segurança que é necessária
Graduar
Designação
Proprietário
Determina quem tem acesso
Gerenciamento de Incidentes de Segurança
Reporte dos Incidentes de Segurança
Usados como:
Forma de aprender
Reportar Incidentes
Contem:
Data e hora
Nome da pessoa que reporta o incidente
Localização (onde foi o incidente?)
Descrição do incidente
Qual é o problema?
Virus
Roubo
Invasão
Perda de dados
Qual é o efeito que o incidente causou?
Como foi descoberto?
Informações adicionais
Tipo de sistema
Desktop
Impressora
Servidor de correio
Número do sistema / nome do sistema (se houver)
Quem mais foi informado?
Exemplos
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 serem testados;
Um vírus conseguiu entrar no sistema de informação;
Devido 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.
Reportando Fraquezas de Segurança
O mais cedo possível
Constar tais suspeitas de deficiência
Solicitar ajuda ao pessoal especializado
Registro de Ruptura
Relatada pela central de atendimento (helpdesk)
Informações pertinentes sejam coletadas
Ciclo do Incidente
Ameaça
Incidente
Dano
Recuperação