Tabela de avaliação de riscos implementado de [data] a [data]

Num.	Nome do ativo	Proprietário do ativo	Ameaça	Vulnerabilidade	Proprietário do risco	Consequência	Probabilidade	Risco	Controles existentes
1	*administrador do sistema*	*gerente de RH*	*engenharia social*	[illegible]	[illegible]	3	3	2	
2	*software aplicativo*	*gerente de TI*	*erros de aplicações*	[illegible]	[illegible]	2	3	3	
3	*relatórios*	*CEO*	*espionagem industrial*	[illegible]	[illegible]	3	2	2	*controle de acesso*
4	*laptops*	*do utilizador*	*furto*	[illegible]	[illegible]	3	3	2	
5	*escritórios*	*gerente de instalações*	*vandalismo*	[illegible]	[illegible]	3	2	1	
6	*links de comunicação*	*gerente de TI*	*quebra de relações contratuais*	[illegible]	[illegible]	2	3	3	
7	*administrador do sistema*	*gerente de RH*	*pandemia, epidemia*	[illegible]	[illegible]	3	2	2	
8	*software aplicativo*	*gerente de TI*	*erros de aplicações*	[illegible]	[illegible]	2	3	3	
9	*software aplicativo*	*gerente de TI*	*vandalismo*	[illegible]	[illegible]	3	2	2	
10	*escritórios*	*gerente de instalações*	*interrupção no fornecimento*	[illegible]	[illegible]	3	2	2	

11	*escritórios*	*gerente de instalações*	*interrupção no fornecimento*	[illegible]	[illegible]	*3*	*1*	*3*	
12	*links de comunicação*	*gerente de TI*	*falha nos equipamentos*	[illegible]	[illegible]	*3*	*1*	*3*	

Categorias dos ativos

Seguem abaixo exemplos de ativos de informações que podem ser encontrados na organização.
Esta lista não é definitiva. Cada organização deve especificar seus próprios ativos importantes para a segurança da informação.

Pessoas

- alta direção (membros da diretoria administrativa, membros do conselho supervisor e gerentes da unidade de negócios)
- direção intermediária
- funcionários - especialistas (como administradores do sistema, projetistas, especialista em segurança, etc.)
- outros funcionários
- funcionários externos que trabalham meio período
- pessoas que visitam a organização

Aplicações e bancos de dados

- software de aplicação (licenciado)
- freeware; shareware
- software do sistema
- ferramentas diversas
- bancos de dados

Documentação (em papel ou formato eletrônico)

- contratos
- correspondência com clientes e parceiros
- registros
- logs
- manuais
- normas
- recibos
- documentação dos equipamentos
- documentação de treinamento
- documentos internos
- decisões
- relatórios

planos
registros contábeis
documentos da equipe

TI, comunicação e outros equipamentos

computadores desktop
laptops
CDs de instalação
Dispositivos UPS
geradores de energia
ar-condicionado
equipamentos de rede
cabos de alimentação
servidores
telefones
sistemas de troca de telefone
telefones móveis
dispositivos PDA
impressoras
escâneres
fotocopiadoras
fitas de cópia de segurança
mídia de armazenamento móvel
equipamentos de medição
máquinas de fax
alarmes
veículos
cartões e leitores de cartão
cofres
chaves

Infrastrutura

escritórios

arquivos
depósitos
cofres
gabinetes

Serviços terceirizados

alimentação de energia elétrica
links de comunicação
manutenção de equipamentos de informação e comunicação
manutenção de sistemas de informação
serviços de correspondência e encomenda
auditores
consultores
instituições de supervisão

Catálogo de ameaças

Segue abaixo de uma relação de ameaças. Esta lista não é definitiva. Cada organização pode adicionar ameaças de situações específicas.

acesso físico não autorizado
acesso não autorizado à rede
acesso não autorizado ao sistema de informações
alteração acidental de dados do sistema de informação
alteração não autorizada de registros
ameaça de bomba
apropriação indevida
ataques terroristas
bombardeio
códigos maliciosos
danos causados durante o teste de penetração
danos causados por atividades de terceiros
destruição de registros
deterioração de mídias
divulgação de senhas
enchente
engenharia social
erro do usuário
erros de aplicações
erros de manutenção
escuta
espionagem industrial
falha dos links de comunicação
falha nos equipamentos
falsificação de registros
fraude
furto
greve
incêndio

instalação não autorizada do software
interceptação de informações
interrupção no fornecimento de energia
ocultação de identidade do usuário
outros desastres (causados pelo homem)
outros desastres (naturais)
pandemia, epidemia
perda de serviços de suporte
poluição
quebra da legislação
quebra de relações contratuais
raios
uso de código não autorizado ou não testado
uso indevido de ferramentas de auditoria
uso indevido de sistemas da informação
uso não autorizado de materiais licenciados
uso não autorizado do software
vandalismo
vazamento/divulgação de informações

Catálogo de vulnerabilidades

Segue abaixo de uma relação de vulnerabilidades.
Esta lista não é definitiva. Cada organização pode adicionar vulnerabilidades de situações específicas.

amplos poderes
bancos de dados desatualizados para proteção contra códigos maliciosos
capacidade de gestão inadequada
chaves criptográficas acessíveis para pessoas não autorizadas
conexões de rede pública não protegidas
contas de usuários e senhas geradas pelo sistema inalteradas
controle de alterações inadequado
cópia única, somente uma cópia das informações
cópias não controladas
descarte de mídias de armazenamento sem apagar os dados
direitos inadequados de usuários
downloads da Internet não controlados
equipamentos móveis sujeitos a furto
falta de controle de dados de entrada e saída
falta de evidências de mensagens enviadas ou recebidas
falta de implementação ou implementação ineficiente da auditoria interna
falta de validação de dados processados
funcionários desmotivados ou descontentes
gestão de rede inadequada
informações disponíveis para pessoas não autorizadas
interface de usuário complicada
local sensível a desastres naturais
local sensível a vazamento de água
manutenção inadequada
más condições de higiene
não desativação de contas de usuários após o encerramento das atividades
nenhuma separação do ambiente de teste e operacional
nível de confidencialidade incerto

nível inadequado de conhecimento e/ou conscientização de funcionários
permissão de acesso não autorizado às instalações
posicionamento de cabos
redes acessíveis a pessoas não autorizadas
regras criptográficas incertas
regras incertas para controle de acesso
regras incertas para trabalhar fora das instalações da empresa
regras organizacionais incertas
requisitos incertos para o desenvolvimento de software
segregação inadequada de funções
seleção inadequada de dados de teste
senhas frágeis
sensibilidade do equipamento à temperatura
sensibilidade do equipamento à umidade e poluição
sensibilidade dos equipamentos à alteração de tensão
sessões ativas após horas de trabalho
sistemas não protegidos contra acesso não autorizado
software não documentado
superdependência de um dispositivo/sistema
supervisão inadequada de fornecedores externos
supervisão inadequada do trabalho dos funcionários
uso de equipamentos antigos
uso não controlado dos sistemas de informações