Anexo 1 – Plano de resposta a incidentes

Commented [AES1]: Para aprender como preencher este documento, e ver exemplos reais do que você precisa escrever, veja este vídeo tutorial "How to Write a Business Continuity Plan According to ISO 22301".

Para acessar o tutorial: Em sua caixa de entrada, encontre o e-mail que você recebeu no momento da compra. Lá, você verá um link e uma senha que lhe permitirá acessar o vídeo tutorial.

Histórico de alterações

Data	Versão	Criado por	Descrição da alteração
	0.1	Advisera	Esboço básico do documento

Sumário

1. FINALIDADE, ESCOPO E USUÁRIOS 2

2. AUTORIZAÇÕES E RESPONSABILIDADES EM RESPOSTAS A INCIDENTES 2

3. COMUNICAÇÃO 2

4. PROCEDIMENTOS PARA INCIDENTES DISRUPTIVOS 3

4.1. GESTÃO DE INCIDENTES DISRUPTIVO 3

4.1.1. Obrigação de todos os funcionários em reportar incidentes 3

4.1.2. Gestão de incidentes disruptivos 3

4.1.3. Gerente de crises 4

4.2. CONTENÇÃO E ERRADICAÇÃO DE INCIDENTE 4

4.2.1. Evacuação do prédio (independentemente do tipo de incidente) 4

4.2.2. Incêndio 5

4.2.3. Interrupção no fornecimento de energia 5

4.2.4. Terremoto 5

4.2.5. Carta de ameaça 6

4.2.6. Ligação de ameaça/ameaça de bomba 6

4.2.7. Falha nas telecomunicações 7

4.2.8. Falha no sistema de informações 7

4.2.9. Ataque de código malicioso 7

4.2.10. Violação de regras internas ou externas 8

5. GESTÃO DE REGISTROS MANTIDOS DE ACORDO COM ESTE DOCUMENTO 8

6. VALIDADE E GESTÃO DE DOCUMENTOS 8

1. Finalidade, escopo e usuários

A finalidade deste Plano é garantir a proteção da saúde e segurança do pessoal em caso de desastres ou outros incidentes, e para conter o incidente. O objetivo é reduzir os danos aos negócios ao mínimo possível.

Este Plano aplica-se a todos os grandes incidentes que ameaçam interromper quaisquer atividades críticas no escopo do SGSI e/ou SGCN por um tempo superior ao objetivo de ponto de recuperação para cada uma das atividades individuais (mais adiante no texto: incidentes disruptivos).

Os usuários deste documento são funcionários da [nome da organização].

Commented [AES2]: Inclua o nome da sua organização.

2. Autorizações e responsabilidades em respostas a incidentes

Commented [AES3]: Para saber mais sobre o assunto, leia este artigo:

Papel na recuperação/cargo	*Autorizações e responsabilidades*
Qualquer funcionário	Notificação sobre o incidente ao responsável pela unidade organizacional
O [cargo] ou equipe da [nome da unidade organizacional]	Todos os passos necessários para ativar as soluções para resolver incidentes relacionados à tecnologia de TI e comunicações
O [cargo] ou equipe da [nome da unidade organizacional]	Todos os passos necessários para ativar as soluções para resolver todos os demais incidentes
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]

Commented [AES4]: Ex.: chefe do departamento de TI

Commented [AES5]: Ex.: oficial de operações

Commented [AES6]: Deve ser a pessoa indicada no Plano de [illegible]

Commented [AES7]: Veja também:

Commented [AES8]: Deve ser a pessoa indicada no Plano de [illegible]

Commented [AES9]: Deve ser nomeado pelo [illegible]

3. Comunicação

A tabela a seguir lista as responsabilidades pela comunicação com os diversos tipos de grupos-alvo:

	[Telefone]	*[Reuniões]*	[illegible]	[illegible]	[illegible]		
[Funcionários]							
[Proprietários/partes interessadas]							
[Familiares de funcionários]							
[illegible]							
[illegible]							
[illegible]							
[illegible]							

Commented [AES10]: Esta seção deve ser expandida com [illegible]

Commented [AES11]: Para saber mais sobre o assunto, leia este artigo:

Commented [AES12]: Copie as responsabilidades da Estratégia e adicione quando esta comunicação deve ser iniciada (imediatamente após um incidente ter ocorrido / após ter sido contido /após ter sido resolvido etc.)

[autoridades estatais]							

O procedimento de comunicação é o seguinte:

1. Qualquer funcionário que recebe uma solicitação de comunicação ou deseja iniciar uma comunicação com partes interessadas deve enviar tal solicitação a uma pessoa responsável, como indicado na tabela acima
2. Uma pessoa responsável deve estar de acordo com o [cargo] no conteúdo da comunicação. Sempre que possível, os modelos de conteúdos de comunicação devem ser utilizados como forma de equilibrar a necessidade de informação das partes interessadas e a prevenção de rumores e desinformação
3. [redacted]
4. [redacted]

A pessoa responsável na tabela acima é responsável por documentar cada documentação com qualquer parte interessada.

4. Procedimentos para incidentes disruptivos

4.1. Gestão de incidentes disruptivo

4.1.1. Obrigação de todos os funcionários em reportar incidentes

Todos os funcionários são obrigados a informar qualquer incidente disruptivo da seguinte forma:

- todos os incidentes relacionados à tecnologia de TI e comunicações são informados por telefone a [cargo ou equipe da unidade organizacional]
- [redacted]

Qualquer outro evento ou outra vulnerabilidade do sistema que ainda não tenha se tornado um incidente dispruptivo deve ser informado da mesma forma.

[redacted]

Caso ocorra um incidente, os funcionários podem comunicar-se livremente somente com seus familiares e com os serviços de polícia, ambulância e bombeiros, enquanto as demais comunicações são de responsabilidade do Equipe de gestão de crises.

4.1.2. Gestão de incidentes disruptivos

Commented [AES13]: Deve ser a pessoa indicada no Plano de [redacted]

Commented [AES14]: Inclua aqui todos os incidentes [redacted]

Commented [AES15]: Se a natureza do incidente não requerer [redacted]

Commented [AES16]: Ex.: chefe do departamento de TI

Commented [AES17]: Ex.: oficial de operações

Commented [AES18]: Se este problema estiver regulamentado [redacted]

A pessoa que recebeu informações sobre o incidente deve verificar imediatamente se o incidente/incidente em potencial é real ou falso. Se for real, ela deve imediatamente ativar este plano tomando as seguintes medidas:

- iniciar a contenção e erradicação do incidente conforme descrito nas seguintes seções deste documento
- notificar todos os responsáveis sobre a ocorrência do incidente na sua área de responsabilidade
- [illegible]
- [illegible]

Commented [AES19]: Ex.: gerente de continuidade de [illegible]

Caso uma pessoa não consiga conter e/ou erradicar o incidente, o gerente de crises deve ser informado. As informações que são repassadas para o gerente de crises devem incluir a natureza e extensão de um incidente disruptivo e seu impacto em potencial.

[illegible]

4.1.3. Gerente de crises

O gerente de crises deve monitorar o progresso da gestão de incidentes e o período de disrupção de cada atividade individual, e avaliar o tempo necessário para solucionar o incidente.

[illegible]

4.2. Contenção e erradicação de incidente

Commented [AES20]: Este capítulo fornece somente os [illegible]

4.2.1. Evacuação do prédio (independentemente do tipo de incidente)

O prédio é evacuado para os pontos de montagem especificados na Lista de locais de continuidade de negócios, anexa ao Plano de continuidade de negócios.

Gerente de crises	• Caso a vida ou a saúde das pessoas seja ameaçada, emita uma ordem de evacuação • [illegible] • [illegible]
Equipe responsável pela	• Evacuação direta para o ponto de montagem • [illegible]

evacuação	[illegible]
Todos os funcionários	• Evacue de acordo com os planos de evacuação do seu prédio • Siga as instruções fornecidas pelos responsáveis pela evacuação direta [illegible]
Equipe de suporte à gestão de crises	• Quando as pessoas estiverem reunidas no ponto de montagem, mantenha os registros de todos os presentes e ausentes

4.2.2. Incêndio

O prédio é evacuado de acordo com o plano de evacuação do prédio.

Gerente de crises	• Caso a vida ou a saúde das pessoas seja ameaçada, o gerente de crises emite uma ordem de evacuação [illegible]

4.2.3. Interrupção no fornecimento de energia

Equipe de suporte à gestão de crises	• Defina a causa da interrupção (se foi causada por problemas de fiação ou pela distribuidora de energia)
[Cargo] ou equipe designada	• Resolva o problema com a distribuidora de energia
[illegible]	[illegible]
[illegible]	[illegible]

Commented [AES21]: Por exemplo. analista de instalações, [illegible]

4.2.4. Terremoto

O prédio é evacuado de acordo com o plano de evacuação do prédio.

Todos os funcionários	• Procure abrigo em local fechado, próximo a uma parede de sustentação ou embaixo de uma mesa • Não use elevadores [illegible]

	[illegible]
Gerente de crises	• Caso a vida ou saúde das pessoas seja ameaçada, solicite a evacuação do prédio quando o terremoto acabar
Equipe de suporte à gestão de crises	• Interrompa o fornecimento de todos os serviços, como gás, eletricidade, aquecimento, ventilação, fornecimento de energia • [illegible]

4.2.5. Carta de ameaça

Todos os funcionários	• Se você receber uma carta suspeita, não abra e segure-as pelas bordas • Coloque-a em um envelope vazio • [illegible]
[Cargo] ou equipe designada	• Notifique a polícia pelo telefone [número de telefone] • [illegible]

Commented [AES22]: Por exemplo, oficial de segurança

Commented [AES23]: Por exemplo, oficial de segurança

Commented [AES24]: Por exemplo, oficial de segurança

4.2.6. Ligação de ameaça/ameaça de bomba

Todos os funcionários	• Se você receber uma ligação de ameaça, registre o horário e o número de telefone da ligação • [illegible] • Permita que a pessoa fale o máximo possível, sem interrompê-las: - tente fazer com que a pessoa fale - repita suas perguntas e diga que não entendeu o que foi dito - [illegible] • Em caso de ameaça de bomba, faça as seguintes perguntas: - A bomba explodirá? Quando? - Ela pode ser desativada? Como? - Onde ela está? - [illegible] • Só abra as portas do escritório se tiver certeza de que elas não estão ligadas à bomba • Não procure pela bomba no prédio. Isso é função da polícia • [illegible]
Gerente de crises	• Notifique o responsável pela unidade organizacional alvo da ameaça • [illegible]

	• Se você achar que a bomba pode realmente explodir, solicite a evacuação; o ponto de montagem deve estar a pelo menos 300 metros de distância

4.2.7. Falha nas telecomunicações

Funcionários no [nome do departamento]	• Qualquer funcionário recebe informações sobre a falha
Funcionários – usuários dos serviços de comunicação	• Use meios de comunicação alternativos

Commented [AES25]: Essas são responsabilidades do

4.2.8. Falha no sistema de informações

Funcionários no [nome do departamento]	• Qualquer funcionário recebe informações sobre o incidente
Gerente de crises	• Consulta de todos os serviços relevantes e avaliação da gravidade do incidente
Todos os funcionários	• Se possível, proceda de forma alternativa para realizar as atividades

Commented [AES26]: Essas são responsabilidades do

4.2.9. Ataque de código malicioso

Funcionários no [nome do departamento]	• Qualquer funcionário recebe informações sobre o incidente • Se você estiver lidando com um tipo desconhecido de código malicioso, a [nome da organização responsável pela segurança da informação] deve ser notificada • Notifique o fabricante do anti-vírus

Commented [AES27]: Essas são responsabilidades do

Todos os funcionários	• Desconecte fisicamente qualquer computador da rede; desative redes sem fio, bluetooth, etc. • [redacted]
Funcionários no [nome do departamento]	• Se o computador ainda não estiver desconectado da rede, avalie se a sua desconexão evita a infecção de outros equipamentos • Desative todas as conexões sem fio no computador • [redacted]

Commented [AES28]: Essas são responsabilidades do [redacted]

Commented [AES29]: Essas são responsabilidades do [redacted]

4.2.10. Violação de regras internas ou externas

[cargo]	• O procedimento é realizado conforme solicitado pelas leis trabalhistas que regulamentam os procedimentos disciplinares e os procedimentos disciplinares da organização

5. Gestão de registros mantidos de acordo com este documento

Nome do registro	*Local de armazenamento*	[redacted]	[redacted]	[redacted]
Registro de incidentes	Pasta compartilhada na intranet	[redacted]	[redacted]	[redacted]

Commented [AES30]: Insira os dados nesta coluna para refletir [redacted]

Commented [AES32]: Ex.: gerente de incidentes, oficial de [redacted]

Commented [AES31]: Ex.: gerente de incidentes, analista de [redacted]

Somente o [cargo] pode conceder aos demais funcionários o acesso aos registros.

6. Validade e gestão de documentos

Este documento é válido a partir de [data].

Este documento e todos os materiais adicionais são armazenados da seguinte forma:

- o formato em papel do documento é armazenado nos seguintes locais: Central de comando e todos os locais alternativos para atividades
- [redacted]

Commented [AES33]: Armazene o documento para permitir o [redacted]

O proprietário do documento é o [cargo], que deve verificar e, se necessário, atualizar o documento pelo menos uma vez por ano.

Commented [AES34]: Isso é apenas uma recomendação;

Ao avaliar a eficácia e a adequação deste documento, os seguintes critérios devem ser considerados:

- quantidade de incidentes não cobertos por este documento
- [illegible]
- [illegible]

[cargo]
[nome]

_____
[assinatura]

Commented [AES35]: Necessário somente se o Procedimento de controle de documentos e registros indicar que os documentos em papel devem ser assinados.