Sumário

1. OBJETIVO

Esta norma tem como objetivo descrever o Processo de Análise de Risco do SGSI.

2. ÂMBITO DE APLICAÇÃO

2.1. Empresa

Esta norma é aplicável à CPFL Energia e a todas as suas controladas diretas e/ou indiretas (“Grupo CPFL”)[1]

2.2. Área

Não aplicável

3. DEFINIÇÕES

ACEITAÇÃO DO RISCO: É a decisão de aceitar um risco existente. Tipicamente, é tomada quando o custo dos controles é superior ao impacto.

AMEAÇA: É a causa potencial de um incidente de segurança da informação. Exemplos de ameaças são enchente, incêndio, furto, roubo, acidente etc.

[1] Exclui-se do âmbito de aplicação as sociedades Energética Barra Grande S.A. (Baesa), Campos Novos Energia S.A. (Enercan), Companhia Energética do Rio das Antas (Ceran), Foz do Chapecó S.A., Chapecoense Geração S.A., Centrais Elétricas da Paraíba S.A. (Epasa) e CPFL Renováveis S.A.

ANÁLISE DE RISCO: Uso sistematizado de informações para identificar fontes de risco e para estimá-lo.

AVALIAÇÃO DO RISCO: Definição do nível de risco com base em critérios de impacto e probabilidade.

CONTROLE: Medida empregada com vistas a reduzir o risco. Um controle pode ser uma norma, um procedimento, um dispositivo, um controle em sistema etc.

IMPACTO: Consequências que podem ocorrer caso o risco se manifeste.

IMPACTO DE IMAGEM: Está relacionado com os danos à imagem pública da empresa. Também é usado para danos à imagem interna de um setor da empresa.

IMPACTO FINANCEIRO: Está relacionado com perdas financeiras como multas, indenizações, perda de vendas.

IMPACTO LEGAL: Está relacionado com a violação de leis municipais, estaduais ou federais.

IMPACTO OPERACIONAL: Está relacionado com as atividades executadas pela empresa, p. ex., atraso em uma linha de produção, paralisação de uma área administrativa, paralisação no despacho de carga.

IMPACTO REGULAMENTAR: Está relacionado com a violação de portarias, decretos, estatutos de associação de classe etc., desde que não caracterize uma violação legal.

INCIDENTE DE SEGURANÇA DA INFORMAÇÃO: Evento ou série de eventos indesejados ou não esperados que podem comprometer as atividades da empresa e ameaçar a segurança das informações.

PROBABILIDADE: Probabilidade de ocorrência do risco.

REDUÇÃO DO RISCO: A redução do risco é feita pelos controles, que podem minimizar os impactos e/ou reduzir a probabilidade de ocorrência.

RISCO RESIDUAL: Nível de risco que permanece após a implantação dos controles.

TRATAMENTO DO RISCO: Processo de selecionar e implementar controles visando a reduzir o risco.

VULNERABILIDADE: Uma fraqueza ou uma deficiência de um ativo ou de um grupo de ativos que pode ser explorada por uma ameaça. Exemplos de vulnerabilidades são: documentos armazenados em local inseguro, sistemas de informação sem segregação de funções, senhas escritas em papel etc.

4. DOCUMENTOS DE REFERÊNCIA

Principais documentos e regulamentações relacionados com esta norma:

Internos

- Diretrizes de Segurança da Informação;
- Código de Ética e de Conduta Empresarial do grupo CPFL;

Externos

- NBR ISO/IEC 27001:2013
- Sarbanes-Oxley Act of 2002 – Section 404

5. RESPONSABILIDADES

Não aplicável.

6. REGRAS BÁSICAS

Descrever a sequência de etapas/tarefas necessárias para a execução de um processo ou atividade.

6.1. Introdução

A Área de Tecnologia da Informação é responsável pela condução das Análises de Risco (AR) de Segurança da Informação de acordo com este procedimento. Caso julgue necessário a área de Tecnologia da Informação poderá contratar empresa especializada para a condução das Análises de Risco de Segurança da Informação.

As seguintes ferramentas serão utilizadas como apoio para a execução deste procedimento:

Ferramenta	Descrição
Questionário de Análise de Impacto do SGSI	Lista de verificação com perguntas orientadas para identificação de riscos
Planilha de Gerenciamento de Riscos do SGSI	Planilha que consolida os riscos identificados, ameaças, vulnerabilidades, ativos e cálculo do risco
Planos de Ação do SGSI	Planilha contendo os, responsáveis e recursos que serão utilizados para tratamento dos riscos considerados inaceitáveis pela empresa. Pode conter além das entradas da Análise de Riscos outras medidas consideradas relevantes pela empresa, como oportunidades de melhoria, ações corretivas, análise crítica, entre outras.

O processo de Análise de Risco consiste das seguintes etapas:

- Identificação
- Avaliação
- Controles Existentes
- Tratamento

6.2. Revisão da Análise de Risco

Uma análise será feita abrangendo todo o escopo da Certificação ISO 27001. A análise deve ser revisada em intervalos de 12 meses ou em intervalos menores caso seja identificado essa necessidade. Mudanças significativas em processos, estrutura organizacional, pessoal, tecnologia, legislação e regulamentação devem gerar revisão da análise de risco.

6.3. Aprovação dos Riscos

Ao final da análise, a Planilha de Gerenciamento de Riscos do SGSI com seus riscos residuais deve ser aprovada pelas seguintes funções:

- Diretor de Tecnologia da Informação
- Gerente de Infraestrutura de TI
- Responsáveis pelos Riscos.

6.4. Execução

6.4.1. Identificação

A identificação de riscos será feita através de entrevistas utilizando como apoio o Questionário de Análise de Impacto do SGSI e revisada a Planilha de Gerenciamento de Riscos do SGSI mais recente, se houver.

Um risco deve ser identificado através de um número único de identificação, um título, responsável pelo risco, vulnerabilidades que podem permitir a manifestação do risco, ameaças que podem causar a manifestação do risco e, um ou mais ativos relacionados ao risco identificado. Estes ativos devem constar na Planilha Inventário de Ativos.

Ao final da identificação de riscos de um processo, deve ser feita uma dupla checagem para verificar se todas as ameaças e vulnerabilidades (Anexos I e II) foram consideradas.

6.4.2. Avaliação

Para avaliar um risco é necessário identificar a probabilidade de ocorrência que pode ser alta, média ou baixa; impacto causado que também devem ser classificados como alto, médio ou baixo; descrição do impacto e, o nível do risco.

6.4.3. Probabilidade

A probabilidade deve ser classificada de acordo com a seguinte metodologia:

Probabilidade	Descrição
Alta	Provável que ocorra no período de 1 ano
Média	Provável que ocorra no período de 2 anos
Baixa	Provável que ocorra em período superior a 2 anos ou improvável que ocorra

6.4.4. Impacto

O nível de impacto deve ser classificado de acordo com a seguinte metodologia:

Impacto	Descrição
Alto	• Impacto Financeiro de valor acima de R$ 1.000.000 • Parada de mais de um processo de negócio • Perda generalizada de credibilidade junto aos consumidores
Médio	• Impacto Financeiro entre R$ 500.000,00 e R$ 1.000.000,00 • Parada de um processo de negócio • Perda de credibilidade junto a um grupo de consumidores
Baixo	• Impacto Financeiro abaixo de R$ 500.000,00 • Atraso operacional em um ou mais processos de negócio • Perda de credibilidade temporária ou junto a uma pequena quantidade de consumidores

6.4.5. Cálculo do Risco Potencial

Deve ser descrito o que vai acontecer se o risco se manifestar, no campo Descrição do Impacto. Em nível de risco, deve conter o nível de acordo com a combinação da classificação da probabilidade e do impacto. O nível de risco é calculado da seguinte forma:

Probabilidade	Impacto	Nível de Risco
Alta	Alto	Alto
Alta	Médio	Alto
Alta	Baixo	Médio
Média	Alto	Alto
Média	Médio	Médio
Média	Baixo	Baixo
Baixa	Alto	Médio
Baixa	Médio	Baixo
Baixa	Baixo	Baixo

6.4.6. Controles

A fase de controles deve conter a descrição, itens da Norma ISO 27001 e, evidências e documentos relacionados.

A descrição dos controles deve conter os controles utilizados pela empresa para tratamento do risco identificado. Em itens da ISO 27001, deve constar o item ou capítulo da norma ISO 27001 relacionado ao risco identificado. Pode haver um ou mais controles.
Neste momento, deve ser analisado o último Relatório de Auditoria Interna para verificar como está o nível de eficácia desses controles. Controles ineficazes podem modificar o campo Residual na fase Tratamento.
No campo Evidências e documentos relacionados são enumerados os documentos utilizados pela empresa para controlar o risco identificado. Pode haver um ou mais documentos ou evidências. Descreve também quaisquer observações/comentários relevantes.

6.4.7. Tratamento

A fase de tratamento será evidenciada na Planilha de Planos de Ação do SGSI, no campo origem da planilha de planos de ação será registrado o número de identificação da planilha de risco para que o link seja estabelecido entre as duas planilhas.

A fase de tratamento deve conter a descrição do tratamento que será dado ao risco identificado.
Deve ser indicado um responsável pelo tratamento dos riscos identificados. Deve ser relacionada apenas uma pessoa.

Devem ser descritos os recursos necessários para o tratamento dos riscos (pessoas, financeiros, etc.) e, uma data prevista para o tratamento do risco identificado. Esta data define a priorização de tratamento dos riscos identificados.
Observação: Este campo permite descrever observações referentes àqueles riscos que forem aceitos.

O responsável pela Gestão da Segurança da Informação é o responsável pela seleção dos controles que serão usados no tratamento dos riscos. A seleção dos controles deve ser baseada nas orientações contidas na norma ISO 27001, sendo que controles adicionais podem ser necessários de acordo com o risco.
Ao selecionar controles adicionais, as seguintes opções devem ser consideradas:

- Evitar o risco: modificar a forma de executar a atividade para que seja eliminada a vulnerabilidade existente.
- Transferir o risco: transferir a atividade para outra empresa e definir o nível de serviço exigido.
- Segurar o risco: fazer um seguro para cobrir o impacto financeiro resultante da ocorrência do risco.

O acompanhamento da implementação das ações de tratamento deve ser feito pelo responsável pela Gestão da Segurança da Informação.

6.4.8. Risco Residual

Deve ser descrito um risco residual, após a implementação dos controles. O nível de risco poderá ser reduzido em 1 ou 2 níveis, segundo os critérios abaixo:

Redução de um nível:
- existem controles para reduzir a probabilidade ou o impacto do risco
- existem processos formalizados e evidências que comprovam a existência

Redução de dois níveis:
- existem controles para reduzir tanto a probabilidade quanto o impacto do risco
- existem processos formalizados e evidências que comprovam a existência

O nível de risco não poderá ser reduzido quando:
- não houver controles implantados
- os controles implantados forem avaliados como totalmente ineficazes pelas auditorias internas ou externas.

Quaisquer campos da planilha que não sejam preenchidos com informações, devem ser preenchidos com NA, para deixar claro que o campo não está em branco.

6.5. Elaboração da Declaração de Aplicabilidade

Um documento contendo os controles aplicáveis do Anexo A da ISO 27001, bem como as justificativas de exclusão deve ser elaborado/atualizado após a execução das análises de risco, este documento é a Declaração de Aplicabilidade.
A justificativa para seleção dos controles descritos na Declaração de Aplicabilidade é baseada nas análises de risco realizadas conforme o Procedimento de Análise de Risco do SGSI, nas determinações da Política de Segurança da Informação, nas Diretrizes de Segurança da Informação, Leis, Regulamentações e Obrigações Contratuais.

7. CONTROLE DE REGISTROS

Identificação	Armazenamento e Preservação	Proteção (acesso)	Recuperação e uso	Retenção	Disposição
Questionário de Análise de Impacto do SGSI	\\pfl-cps-file\AI\AIT\AITT\Seguranca_Informacao\Documentos\SGSI	Backup	Cronológico	Backup	Deletar
Planilha de Gerenciamento de Riscos do SGSI	\\pfl-cps-file\AI\AIT\AITT\Seguranca_Informacao\Documentos\SGSI	Backup	Cronológico	Backup	Deletar
Inventário de Ativos	CRM Dynamics	Backup	Cronológico	Backup	Deletar
Planilha de Planos de Ação do SGSI	\\pfl-cps-file\AI\AIT\AITT\Seguranca_Informacao\Documentos\SGSI	Backup	Cronológico	Backup	Deletar
Declaração de Aplicabilidade	\\pfl-cps-file\AI\AIT\AITT\Seguranca_Informacao\Documentos\SGSI	Backup	Cronológico	Backup	Deletar

8. ANEXOS

Anexo I - Lista de Verificação de Ameaças

Lista de Verificação de Ameaças
Paralisação (greve)
Acesso a rede por usuário não autorizado
Adulteração de identidade de usuário
Análise de Tráfego
Condições extremas de temperatura ou umidade
Congestionamento de tráfego

Dano intencional
Danos às linhas
Descarga eletrostática
Deterioração de meio de armazenamento
Enchente
Erro de manutenção
Erro de transmissão
Erro operacional de funcionários
Erros de usuários
Explosão de bomba
Falha de hardware
Falha de software
Falha dos serviços de comunicação
Falha no ar-condicionado
Falha técnica de componentes de rede
Falta de fornecimento de água
Falta de fornecimento de energia elétrica
Falta de funcionários
Flutuação de energia
Fogo
Furacão
Grampo (sniffing)
Importação ou exportação de software ilegal
Infiltração de comunicação
Não considerado incidente
Poeira
Radiação eletromagnética
Raio
Re-roteamento das mensagens
Repúdio
Roteamento indevido das mensagens
Roubo

Software malicioso
Terremoto
Uso da rede de modo não autorizado
Uso de armas
Uso de software de modo não autorizado
Uso de software por usuário não autorizado
Uso ilegal de software
Uso inadequado dos recursos
Uso não autorizado de meio de armazenamento

Anexo II - Lista de Verificação de Vulnerabilidades

Lista de Verificação de Vulnerabilidades
Armazenamento desprotegido
Ausência de logout ao deixar a estação
Ausência de pessoal
Conexões a redes públicas desprotegidas
Descarte ou reutilização de meios de armazenamento sem eliminação dos dados
Download e uso de software sem controle
Falhas de software bem conhecidas
Falta de clareza ou formalismo nas especificações para desenvolvedores
Falta de conscientização sobre segurança
Falta de controle de cópias
Falta de controle de mudanças eficaz
Falta de cópias de backup
Falta de cuidado com o lixo
Falta de documentação
Falta de efetividade no controle de mudanças de configuração
Falta de identificação e autenticação de remetente e destinatário
Falta de mecanismos de identificação e autenticação de usuário
Falta de mecanismos de monitoração
Falta de políticas de uso correto dos meios de comunicações e mensagens
Falta de procedimento de substituição periódica

Falta de proteção física do edifício, portas e janelas
Falta de prova de recebimento ou envio de mensagem
Falta de registros de auditoria
Fiação elétrica instável
Gerência de senhas inadequada ou ineficaz
Gerência inadequada de rede
Incorreta atribuição de direitos de acesso
Interface de usuário difícil de usar
Junção de cabeamento inadequada
Linhas de comunicação desprotegidas
Linhas de discagem para acesso remoto
Localização em área suscetível a enchente
Manutenção insuficiente/instalação deficiente de meios de armazenamento
Ponto único de falha
Procedimento de recrutamento inadequado
Resposta inadequada do serviço de manutenção
Sensibilidade a radiação eletromagnética
Sensibilidade a umidade, sujeira e poeira
Sensibilidade a variação de temperatura
Sensibilidade a variação de voltagem
Tabelas de senha desprotegidas
Teste de software insuficiente ou inexistente
Trabalho externo de limpeza não supervisionado
Tráfego de dados sensíveis desprotegido
Transferência de senhas em texto aberto
Treinamento em segurança insuficiente
Uso inadequado ou descuidado de controle de acesso físico ao edifício e salas
Uso incorreto de software e hardware

Anexo III – Questionário de Análise de Impacto do SGSI

Processo/Setor: _____ Data: ____/____/___

Entrevistado(s): _____

Introdução
As instruções para o preenchimento deste questionário e das demais atividades do processo de análise de riscos estão descritos no Procedimento de Análise de Risco do SGSI.

Os níveis a serem considerados nas respostas às questões sobre impactos são os seguintes:

ALTO	Impacto Financeiro no valor acima de 7 dias de faturamento médio Parada ou atraso em mais de um processo de negócio Problema de imagem com clientes e fornecedores
MÉDIO	Impacto Financeiro no valor entre 3 a 7 dias de faturamento médio Parada operacional de apenas um processo de negócio Perda de confiança interna em um departamento
BAIXO	Impacto Financeiro abaixo do valor de até 2 dias de faturamento médio Atraso operacional em um processo de negócio Queda da moral nos colaboradores de uma área

Seção 1: ESCALA DE OPERAÇÕES DO NEGÓCIO

Questão 1.1 (somente uma resposta)
Qual o faturamento total no ano das atividades executadas pelo processo ou setor?

( ) Menos de R$ 100.000
( ) Entre R$ 100.001 e R$ 500.000
( ) Entre R$ 500.001 e R$ 1 milhão
( ) Entre R$ 1 milhão e R$ 5 milhões
( ) Entre R$ 5 milhões e R$ 20 milhões
( ) Entre R$ 20 milhões e R$ 100 milhões
( ) Entre R$ 100 milhões e $500 milhões
( ) Acima de R$ 500 milhões

Questão 1.2 (selecionar uma ou mais respostas)
Identifique quais das seguintes atividades são executadas ou indiretamente suportadas por este processo ou setor:

( ) Suporte a decisão estratégica
( ) Pesquisa/análise de negócio
( ) Suporte a tomada de decisão
( ) Outro tipo de gerenciamento de informações do negócio
( ) Armazenamento/processamento de informações pessoais
( ) Armazenamento/processamento de informações de pessoas jurídicas

( ) EDI dentro da organização
( ) EDI para fora da organização (clientes, fornecedores etc)

Questão 1.3 (somente uma resposta)
Existe outro processo de negócio ou setor que dependa deste processo/setor para executar as suas atividades cotidianas?

( ) Sim
( ) Não (pular próxima pergunta)

Questão 1.4 (selecionar uma ou mais respostas)
Quantos processos de negócio ou setores dependem deste processo/setor e qual o nível de dependência?

Seção 2: ATIVIDADES DO PROCESSO

Questão 2.1 (somente uma resposta)
Os sistemas de informação que suportam este processo de negócio são usados, direta ou indiretamente, para cálculos, conciliações, relatórios etc., em que a exatidão e a disponibilidade sejam importantes para a organização?

( ) Sim
( ) Não

Questão 2.2 (somente uma resposta)
Os sistemas de informação que suportam este processo de negócio são usados, direta ou indiretamente, para armazenar ou processar os principais registros da contabilidade da organização, por exemplo, registros que reflitam as posições financeiras da organização?

( ) Sim
( ) Não

Questão 2.3 (somente uma resposta)
As informações processadas pelos sistemas do processo de negócio são usadas para basear decisões gerenciais ou estratégicas?

( ) Sim
( ) Não

Questão 2.4 (somente uma resposta)
O processo de negócio/setor executa transações financeiras como transferências eletrônicas de fundos, pagamento faturas/boletos, transações no mercado de ações, transações de importação/exportação, impressão de cheques etc.?

( ) Sim
( ) Não (Pular para pergunta 2.9)

Questão 2.5 (selecionar uma ou mais respostas)
Quais são os tipos de transações financeiras executadas?

( ) Transações de importação ou de exportação
( ) Transações no mercado de ações
( ) Transferência de fundos (DOC/TED etc.)
( ) Impressão/emissão de cheques
( ) Pagamentos de faturas/boletos
( ) Recebimentos de vendas
( ) Outras transações financeiras

Questão 2.6 (somente uma resposta)
Qual o número máximo diário, aproximado ou em média, de transações financeiras processadas?

( ) Menos do que 100
( ) De 101 a 500
( ) De 501 a 1.000
( ) De 1.001 a 5.000
( ) Mais de 5.000

Questão 2.7 (somente uma resposta)
Qual o valor médio aproximado de cada transação?

( ) Menos de R$ 1.000
( ) Entre R$ 1.001 e R$ 10.000
( ) Entre R$10.001 e R$ 50.000
( ) Entre R$ 50.001 e R$ 100.000
( ) Entre R$ 100.001 e R$ 250.000
( ) Entre R$ 250.001 e R$ 500.000
( ) Entre R$ 500.001 e R$ 1 milhão
( ) Entre R$ 1 milhão e R$ 10 milhões
( ) Acima de R$ 10 milhões

Questão 2.8 (somente uma resposta)
Qual o valor estimado máximo de uma única transação?

( ) Menos de R$ 1.000
( ) Entre R$ 1.001 e R$ 10.000
( ) Entre R$10.001 e R$ 50.000
( ) Entre R$ 50.001 e R$ 100.000
( ) Entre R$ 100.001 e R$ 250.000
( ) Entre R$ 250.001 e R$ 500.000
( ) Entre R$ 500.001 e R$ 1 milhão
( ) Entre R$ 1 milhão e R$ 10 milhões
( ) Acima de R$ 10 milhões

Questão 2.9 (selecionar uma ou mais respostas)
O processo de negócio executa algum destes tipos de transação:

Seção 3: IMPACTOS DE INDISPONIBILIDADE

Questão 3.1 (somente uma resposta)

Após qual período de tempo a indisponibilidade dos sistemas utilizados no processo/setor causará impacto de nível baixo? Todos os sistemas devem ser relacionados na Matriz de Sistemas.

( ) Somente poucos minutos
( ) 30 minutos
( ) 4 horas
( ) 1 dia
( ) 3 dias
( ) 1 semana
( ) Mais de 1 semana

Questão 3.2 (somente uma resposta)
Após qual período de tempo a indisponibilidade dos sistemas utilizados no processo/setor causará impacto de nível médio?

( ) Somente poucos minutos
( ) 30 minutos
( ) 4 horas
( ) 1 dia
( ) 3 dias
( ) 1 semana
( ) Mais de 1 semana

Questão 3.3 (somente uma resposta)
Após qual período de tempo a indisponibilidade dos sistemas utilizados no processo/setor causará impacto de nível alto?

( ) Somente poucos minutos
( ) 30 minutos
( ) 4 horas
( ) 1 dia
( ) 3 dias
( ) 1 semana
( ) Mais de 1 semana

Questão 3.4 (selecionar uma ou mais respostas)
Selecionar todos os tipos de impacto financeiro que poderiam ocorrer como resultado de indisponibilidade?

( ) Perda de faturamento corrente
( ) Perda de faturamento futuro
( ) Perdas indiretas (multa contratual, etc)
( ) Outras exposições financeiras

Questão 3.5 (somente uma resposta)
Qual é a exposição financeira total que poderia resultar um período de indisponibilidade a ser considerado crítico?

( ) Nenhum impacto financeiro
( ) Menos de $1.000
( ) $1.000 a $5.000
( ) $5.000 a $20.000
( ) $100.000 a $500.000
( ) $500.000 a $2.5 milhões
( ) $2.5 milhões a $10 milhões
( ) $10 milhões a $50 milhões
( ) Mais de $50 milhões

Questão 3.6 (uma ou mais respostas)
Qual é o nível de prejuízo de imagem que um período prolongado de indisponibilidade poderia causar para com o público externo (clientes, fornecedores, mercado em geral)? (0=nenhum, 1=baixo, 2=médio, 3=alto)

Unidade de Negócio =>
Empresa =>
Grupo =>

Questão 3.7 (somente uma resposta)
Qual é o nível de impacto que um período prolongado de indisponibilidade poderia ter na redução da confiança/moral da equipe?

( ) Alto
( ) Médio
( ) Baixo
( ) Nenhum

Questão 3.8 (somente uma resposta)
Qual seria a pior implicação regulatória resultante da indisponibilidade (não incluir implicações legais)?

( ) Nenhuma implicação regulatória (Pular a próxima pergunta)
( ) Poderia advertir a unidade (Pular a próxima pergunta)
( ) Aviso formal à unidade (Pular a próxima pergunta)
( ) Penalidades financeiras (p. e., multa)
( ) Cancelamento da associação da unidade (Pular a próxima pergunta)

Questão 3.9 (somente uma resposta)
Estimar o montante total de perda financeiras que poderia ocorrer?

( ) Menos de $50.000
( ) $50.000 a $500.000
( ) Mais de $500.000

Questão 3.10 (somente uma resposta)
A indisponibilidade poderia resultar em alguma implicação legal?

( ) Nenhuma implicação legal
( ) Menores danos – menos de $50.000
( ) Maiores danos – mais de $50.000

Verificar outros documentos que poderiam causar impactos de indisponibilidade.

Seção 4: IMPACTOS DE PERDA DE INTEGRIDADE

Questão 4.1 (somente uma resposta)
O processo de negócio, ou informação relacionada, é usado para qualquer finalidade que poderia tornar a integridade crítica?

( ) Sim
( ) Não (Pular para a questão 5.1)

Questão 4.2 (uma ou mais respostas)
O sistema ou função do negócio, ou informação relacionada, é usado por algum dos seguintes propósitos que torne sua integridade crítica?

( ) Financeiro
( ) Cliente
( ) Mercado
( ) Regulamento
( ) Legal
( ) Funcionário
( ) Acionistas
( ) Outros propósitos críticos

Questão 4.3 (uma ou mais respostas)
Selecionar os tipos de impacto financeiro que poderiam ocorrer por alterações não controladas de informações armazenadas ou processadas pelo sistema ou unidade de negócio?

( ) Perda de faturamento atual
( ) Perda de faturamento futuro
( ) Perdas indiretas (multa contratual, etc)
( ) Outras exposições financeiras

Questão 4.4 (somente uma resposta)
Qual é a exposição total financeira que poderia resultar uma alteração não controlada?

( ) Nenhum impacto financeiro
( ) Menos de $1.000
( ) $1.000 a $5.000
( ) $5.000 a $20.000
( ) $20.000 a $100.000
( ) $100.000 a $500.000
( ) $500.000 a $2.5 milhões
( ) $2.5 milhões a $10 milhões
( ) $10 milhões a $50 milhões

( ) Mais de $50 milhões

Questão 4.5 (uma ou mais respostas)
Qual é o nível de constrangimento que uma alteração sem controle poderia causar para cada um dos seguintes itens abaixo, em termos de relacionamento com o público externo (clientes, fornecedores, mercado em geral)? (0=nenhum, 1=baixo, 2=médio, 3=alto)

Unidade de Negócio =>
Empresa =>
Grupo =>

Questão 4.6 (uma ou mais respostas)
Qual é o nível de impacto que uma alteração não controlada poderia causar na confiança/moral da equipe?

( ) Alto
( ) Médio
( ) Baixo
( ) Nenhum

Questão 4.7 (somente uma resposta)
Qual é a pior implicação que pode resultar uma alteração não controlada?

( ) Nenhuma implicação (Pular a próxima pergunta)
( ) Advertência Verbal (Pular a próxima pergunta)
( ) Advertência Formal (Pular a próxima pergunta)
( ) Prejuízo financeiro
( ) Cancelamento de concessão/associação (Pular a próxima pergunta)

Questão 4.8 (somente uma resposta)
Estimar o montante total de prejuízo financeiro?

( ) Menos de $50.000
( ) $50.000 a $500.000
( ) Mais de $500.000

Questão 4.9 (somente uma resposta)
Quais das seguintes implicações legais poderiam resultar de uma alteração de informação não controlada?

( ) Prejuízo mínimo – menos de $50.000
( ) Prejuízo maior – mais de $50.000
( ) Ação Criminal individual
( ) Ação Criminal contra a Companhia

Seção 5: IMPACTOS DE DIVULGAÇÃO DE INFORMAÇÕES

Questão 5.1 (uma ou mais respostas)

Selecionar quais das seguintes categorias melhor descreve a informação processadas pelo processo de negócio?

( ) Informações de colaboradores
( ) Informações de clientes
( ) Informações de portfólio de cliente
( ) Informações comercialmente confidenciais
( ) Informações confidenciais de preços
( ) Segurança de dados
( ) Segurança física
( ) Outros detalhes críticos

Questão 5.2 (selecionar uma ou mais respostas)
As informações que são armazenadas ou processadas pelo processo ou unidade de negócio podem ser consideradas “confidenciais”?

( ) Sim
( ) Não (Pular para o fim)

Questão 5.3 (somente uma das respostas)
Quais pessoas são excluídas do conhecimento desta informação confidencial?

( ) Outras na mesma unidade de negócio
( ) Outras unidades na Companhia
( ) Outras Companhias no grupo
( ) Pessoas externas à companhia/grupo

Questão 5.4 (selecionar uma ou mais respostas)
Selecionar os tipos de impacto financeiro que poderiam ocorrer como resultado da divulgação de informações confidenciais.

( ) Perda de faturamento corrente
( ) Perda de faturamento futuro
( ) Perdas indiretas (multa contratual, etc)
( ) Outras exposições financeiras

Questão 5.5 (uma ou mais respostas)
Qual é o nível de constrangimento que uma divulgação de informação confidencial poderia causar para cada um dos seguintes itens abaixo, em termos de relacionamento com o público externo (clientes, fornecedores, mercado em geral)?? (0=nenhum, 1=baixo, 2=médio, 3=alto)

Unidade de Negócio =>
Companhia =>
Grupo =>

Questão 5.6 (somente uma resposta)
Qual é o nível de impacto que uma divulgação de informação confidencial poderia causar para a redução da confiança/moral dos colaboradores?

( ) Alto
( ) Médio
( ) Baixo
( ) Nenhum

Questão 5.7 (somente uma resposta)
Qual é a pior implicação que pode resultar uma divulgação de informação confidencial?

( ) Nenhuma implicação regulatória (Pular a próxima pergunta)
( ) Advertência (Pular a próxima pergunta)
( ) Advertência Formal (Pular a próxima pergunta)
( ) Prejuízos financeiros
( ) Cancelamento de concessão/associação (Pular a próxima pergunta)

Questão 5.8 (somente uma resposta)
Estimar o valor total que poderiam ser causados por prejuízos financeiros?

( ) Menos de $50.000
( ) $50.000 a $500.000
( ) Mais de $500.000

Questão 5.9 (somente uma resposta)
Quais das seguintes implicações poderiam ser causadas pela divulgação de informação confidencial?

( ) Prejuízos mínimos – menos de $50.000
( ) Prejuízos maiores – mais de $50.000
( ) Ação criminal Individual
( ) Ação criminal contra Companhia

9. REGISTRO DE ALTERAÇÕES

9.1. Colaboradores

Empresa	Área	Nome
Piratininga	EIQS	Heliane Pontes Ferreira
Paulista	EIQS	Rafael Fedozzi

9.2. Alterações

Versão Anterior	Data da Versão Anterior	Alterações em relação à Versão Anterior
6	03/10/2013	Atualização do Documento (Inclusão da tabela de Histórico das revisões).
7	15/07/2015	Atualização do Documento (Inclusão dos responsáveis pelo risco e sigla do departamento).
8	28/06/2017	Revisão geral do documento.
1.8	28/06/2017	Revisão geral do documento e adequação ao modelo para elaboração de documentos no GED.
1.9	03/04/2019	Revisão do item 6.3 Aprovação dos Riscos e item 7 – Controle de Registros