NORMA DE CONTINUIDADE DE NEGÓCIO

INTRODUÇÃO

Esta Norma de Segurança da Informação e Infraestrutura complementa a Política de Segurança da Informação, definindo as diretrizes para a devida Gestão de Risco da ELUBEL.

A gestão de risco deve levar em considerações modelos consolidados para a sua elaboração tais como ISO 31000 e ISO 27005.

1. OBJETIVO

Esta norma fornece diretrizes para o processo de gestão de riscos de segurança da informação da empresa.

2. ABRANGÊNCIA

Todos os equipamentos, processos, pessoas, departamentos, espaço físico e lógico.

3. ESCOPO

Esta norma segue o escopo definido previamente na Política de Segurança da Informação**.**

4. CONTEXTO

Esta gestão de risco tem como contexto a preparação para a criação de um plano de resposta a incidente.

5. DIRETRIZES

5.1. Da alta direção da ELUBEL

5.1.1. Apoiar a gestão de risco pois acredita no auxílio dela nas tomadas de decisões corretas da empresa e usá-la como parâmetro.

5.1.2. Determinar quais colaboradores irão compor a "Comissão de Segurança".

5.1.3. Orientar suas relações externas e internas nas regras, processos e práticas visando um consenso na operação da empresa.

5.1.4. Disponibilizar recursos necessários para a aplicação da gestão de risco em todas as frentes da empresa.

5.1.5. Realizar melhorias contínuas em todos os processos e produtos.

5.1.6. Incentivar todos os colaboradores da empresa a serem críticos em suas análises.

5.1.7. Aprovar o "Encarregado de Dados" que conduzirá a "Comissão de Segurança", dando-lhe todo respaldo necessário para o desempenho da função.

5.2. A gestão de risco está enquadrada nas atividades e necessidades da empresa.

5.3. A gestão de risco deve ser aplicada preferencialmente em toda tomada de decisão que envolva estratégia comercial, operacional, desenvolvimento e projetos.

5.4. O propósito da identificação de risco é encontrar, reconhecer e descrever riscos que podem ajudar ou impedir a empresa de alcançar seus objetivos.

5.5. A ELUBEL reconhece todas as suas obrigações e compromissos voluntários no qual trabalha ativamente para minimizar os riscos envolvidos.

5.6. A gestão de risco será responsável pela identificação, análise, estimativa, categorização e tratamento, de forma sistêmica através de um processo formal.

5.7. Todos na ELUBEL têm responsabilidade por gerenciar riscos.

5.8. Os colaboradores devem absorver o conhecimento apresentado e divulgado pelo conselho administrativo.

5.9. A gestão de risco deve examinar e entender seu contexto externo tais como:

5.9.1. Fatores sociais, culturais, políticos, jurídicos, regulatórios, financeiros, tecnológicos, econômicos e ambientais, em âmbito local, regional, nacional ou internacional.

5.9.2. Direcionadores-chave e tendências que afetem os objetivos da organização.

5.9.3. Relacionamentos percepções, valores, necessidades e expectativas das partes interessadas externas.

5.9.4. Relações e compromissos contratuais.

5.9.5. Complexidade das redes de relacionamento e dependências

5.10. A gestão de risco deve examinar e entender seu contexto interno tais como:

5.10.1. Visão, missão e valores.

5.10.2. Governança, estrutura, organizacional, papéis e responsabilizações.

5.10.3. Estratégia, objetivos e políticas.

5.10.4. Cultura da organização.

5.10.5. Normas, diretrizes e modelos adotados pela organização

5.10.6. Capacidades entendidas em termos de recursos e conhecimento (capital, tempo, pessoas, processos, sistemas e tecnologias)

5.10.7. Dados, sistemas de informação e fluxos de informação.

5.10.8. Relacionamentos como partes interessadas internas, levando em consideração suas percepções e valores.

5.10.9. Relações contratuais e compromissos.

5.10.10. Interdependências e interconexões

5.11. Os Membros da Comissão de Segurança são responsáveis pela análise e aprovação dos planos de ação dos riscos apontados.

5.12. Criar uma estrutura para disseminar o conhecimento dos riscos associados às atividades da empresa.

5.13. Todas as ações e decisões devem estar alinhados aos valores centrais da empresa, de modo a manter sua essência.

5.14. As ações devem ser claras, objetivas e inflexível pois poderão tratar os seguintes tipos de riscos: responsabilidade, propriedade ou às pessoas.

5.14.1. Riscos por responsabilidade, referem-se às perdas causadas pelo pagamento de indenizações a terceiros, responsabilidade ambiental, assim como pela qualidade e segurança do produto ou serviço prestado.

5.14.2. Riscos à propriedade consideram as perdas oriundas de incêndios, explosões, vandalismo, roubo, sabotagem, acidentes naturais e danos a equipamentos e bens em geral.

5.14.3. Riscos relativos às pessoas, referem-se a doenças ocupacionais ou acidentes de trabalho que levam à incapacidade temporária, invalidez ou morte de colaboradores.

5.15. Atuar na busca de possíveis falhas e na sua mitigação.

5.16. Toda análise de risco deve seguir os seguintes princípios:

5.16.1. Apontar o ativo relacionado

5.16.2. Impacto do ativo no negócio

5.16.3. Descrever a Ameaça

5.16.4. Apontar a probabilidade

5.16.5. Descrever a vulnerabilidade

5.16.6. Definir a Origem

5.16.7. Definir nível de maturidade de controle

5.16.8. Definir nível de exposição do ativo

5.16.9. Classificar o nível de risco

5.16.10. Determinar o impacto na segurança

5.16.11. Definir controles de mitigação

5.16.12. Criar plano de ação

5.16.13. Classificar o risco residual

6. RESPONSABILIDADES

6.1. Comissão de Segurança

6.1.1. Implementar e supervisionar os sistemas de gestão de riscos e de controle interno estabelecidos para a prevenção e mitigação dos principais riscos a que está exposta a Empresa.

6.1.2. Assegurar que os recurso necessários sejam alocados para gerenciar riscos.

6.1.3. Atribuir autoridades, responsabilidades e responsabilização nos níveis apropriados dentro da empresa.

6.1.4. Alinhar a gestão de riscos com seus objetivos, estratégias e cultura.

6.1.5. Estabelecer a quantidade e o tipo de risco que pode ou não ser assumido para orientar o desenvolvimento de critérios, assegurando que sejam comunicados à organização e às suas partes interessadas.

6.1.6. Promover o monitoramento sistemático de riscos.

6.1.7. Assegurar que a estrutura de gestão de riscos permaneça apropriada ao contexto da ELUBEL.

6.1.8. Assegurar que estes riscos sejam apropriados nos contextos dos objetivos da ELUBEL.

6.1.9. Compreender os ricos aos quais a empresa está exposta na busca de seus objetivos.

6.1.10. Analisar e aprovar atualizações da norma de gestão de risco apresentada pelo analista de risco.

6.1.11. Analisar e encaminhar os riscos apresentados no relatório do analista de risco.

6.1.12. Determinar as prioridades de tratamento dos riscos apresentados.

6.1.13. Determinar o planejamento e alocação de recursos financeiros, humanos e tecnológicos, necessários para mitigar os riscos analisados, tais como:

6.1.13.1. Pessoas, habilidades, experiência e competência.

6.1.13.2. Processos, métodos, ferramentas de gestão de risco.

6.1.13.3. Processos e procedimentos documentados.

6.1.13.4. Sistemas de gestão da informação e do conhecimento.

6.1.13.5. Necessidades de treinamento e desenvolvimento profissional

6.1.14. Planejar um calendário periódico de avaliação de risco.

6.1.15. Manter uma documentação completa e atualizada dos possíveis riscos de negócio da empresa.

6.1.16. Evidenciar todos os riscos apontados com suas análises de mitigação e correção, quando aceitos.

6.1.17. Avaliar o relatório de risco apresentado pelo analista e, aceitar ou propor alteração no tratamento sugerido, baseando-se nas opções do item 11 desta norma.

6.1.18. Apresentar informativos para conscientização dos riscos a empresas.

6.2. Gestores

6.2.1. Internalizar em sua equipe o responsável pela execução da medida de mitigação proposta.

6.2.2. Garantir a execução da medida.

6.2.3. Evidência a conclusão da execução.

6.2.4. Conscientizar sua equipe sobre as medidas preventivas propostas pelo Conselho Administrativo.

7. COMUNICAÇÃO

7.1. O propósito da comunicação é auxiliar as partes interessadas na compreensão do risco sobre decisões tomadas e ações requeridas.

7.2. A comunicação deve promover conscientização e o entendimento do risco.

7.3. Toda comunicação deve levar em consideração a confidencialidade e integridade da informação, bem como os direitos de privacidade dos indivíduos.

7.4. A comunicação e consulta visam a:

7.4.1. Reunir diferentes áreas de especialização para cada etapa do processo de gestão de riscos.

7.4.2. Assegurar que pontos de vista diferentes estejam considerados apropriadamente ao se definirem critérios de risco e ao se avaliarem riscos.

7.4.3. Fornecer informações suficientes para facilitar a supervisão dos riscos e a tomada de decisão.

7.4.4. Construir um senso de inclusão e propriedade entre os afetados pelo risco.

7.5. A Comissão de Segurança determinará as necessidades de comunicações preventivas, corretivas ou informativas, internas ou externas e definira:

7.5.1. 8.5.1. O que será comunicado;

7.5.2. 8.5.2. Como será comunicado;

7.5.3. 8.5.3. Quando será comunicado;

7.5.4. 8.5.4. Para quem será comunicado.

8. DOCUMENTAÇÃO

8.1. Que estejam disponíveis, utilizáveis e atualizados, quando e onde forem necessários;

8.2. Que tenha o devido controle de mudança e versionamento;

8.3. Que preserve a legibilidade do conteúdo;

8.4. Que se tenha a devida segurança nos documentos para que não ocorra modificação não autorizada ou deleção.

8.5. Risco assumido (conhecido e aceito)

8.5.1. O responsável da área, conivente com o risco não mitigado apresentado e documentado no tópico anterior, assinará este documento assumindo a responsabilidade.

8.5.2. A não assinatura deste documento implica no escalonamento à Diretoria da empresa.

8.5.3. A permanência de um risco não mitigado sem um responsável declarado, atribui esta responsabilidade ao responsável legal da empresa compulsoriamente.

8.5.4. O Encarregado de Dados estará isento de qualquer responsabilidade quando evidenciar:

8.5.4.1. Apresentação do risco e consequências

8.5.4.2. Indicação de medidas mitigatórias

8.5.4.3. Escalonamento até a última instância

8.6. Avaliação e Melhoria

8.6.1. Mensure periodicamente o desempenho da gestão de riscos em relação ao seu propósito, planos, indicadores e comportamento esperado.

8.6.2. Determine se permanece adequada para apoiar o alcance dos objetivos da organização

8.6.3. Analisar, monitorar e adaptar continuamente a gestão de riscos para abordar novos contextos externos e internos da empresa, a modo de melhorar seu valor

8.6.4. Lacunas e oportunidades de melhoria inevitavelmente irão aparecer com o tempo, convém que a ELUBEL desenvolva planos e tarefas, através da Comissão de Segurança e o analista de risco para se ter uma melhoria contínua no processo.

9. PROCESSO

9.1. A gestão de risco deve ter uma aplicação sistemática que visa os procedimentos e práticas para as atividades de comunicação, consulta, contexto, avaliação, tratamento, monitoramento, análise crítica, registro e relato de risco.

9.2. O processo de gestão de risco deve:

9.2.1. Adequar-se a cada nova necessidade, mantendo-se alinhada aos objetivos operacionais e concomitante a segurança da informação.

9.2.2. Ser aderente a realidade externa e interna no qual o projeto se desenvolve.

9.2.3. Levar em consideração o comportamento humano e cultural no qual a análise é feita.

9.2.4. Ter escopo claro e definido no qual deve se estipular seus níveis de elaboração (estratégico, operacional, desenvolvimento, projeto ou outros).

9.2.5. Ter um tempo definido para execução.

9.2.6. Ter um resultado esperado.

9.2.7. Ter no mínimo uma ferramenta e uma técnica apropriada para o processo de avaliação de riscos.

9.2.8. Ter recursos requeridos, responsabilidades e registros a serem mantidos

9.2.9. Manter uma sinergia entre as regras de negócio e as análises de risco.

9.2.10. Considerar a natureza e o tipo de incertezas que podem afetar os resultados e objetivos tangíveis e intangíveis

9.2.11. Considerar como as consequências (positivas e negativas) e probabilidades serão definidas e medidas.

9.2.12. Considerar a capacidade da empresa para desenvolver e manter um processo.

9.2.13. Conduzir a avaliação de risco de forma iterativa, colaborativa, com base no conhecimento e nos pontos de vista das partes interessadas.

9.3. A avaliação do contexto externo e interno é extremamente importante pois fatores organizacionais, estrutural, político, cultura, jurídico, regulatório, tecnológico, econômicos, social e outros podem ser uma fonte de risco.

9.4. A gestão de risco considerará esses fatores, mas não se limitando a eles:

9.4.1. Fontes tangíveis e intangíveis de risco;

9.4.2. Causas e eventos;

9.4.3. Ameaças e oportunidade;

9.4.4. Vulnerabilidades e capacidades;

9.4.5. Mudanças nos contextos externo e interno;

9.4.6. Indicadores de riscos emergentes;

9.4.7. Natureza e valor dos ativos e recursos;

9.4.8. Consequências e seus impactos nos objetivos;

9.4.9. Limitações de conhecimento e de confiabilidade da informação;

9.4.10. Fatores temporais;

9.4.11. Vieses, hipóteses e crenças dos envolvidos.

9.4.12. Probabilidade de eventos e consequências;

9.4.13. Natureza e magnitude das consequências;
9.4.14. Complexidade e conectividade;
9.4.15. Fatores temporais e volatilidade;
9.4.16. Eficácia dos controles existentes;
9.4.17. Sensibilidade e níveis de confiança.

10. AVALIAÇÃO E TRATAMENTO

10.1. O propósito da avaliação de risco é apoiar a decisão a ser tomada no qual pode ser:
10.1.1. Fazer nada referente ao risco apontado;
10.1.2. Considerar as opções de tratamento de riscos;
10.1.3. Realizar análise adicionais para melhor compreender o risco;
10.1.4. Manter os controles existentes;
10.1.5. Reconsiderar os objetivos.

10.2. O propósito do tratamento de risco é selecionar e implementar opções para abordar os riscos no qual envolve:
10.2.1. Formular e selecionar opções para o tratamento do risco
10.2.2. Planejar e implementar o tratamento do risco;
10.2.3. Avaliar a eficácia deste tratamento;
10.2.4. Decidir se o risco remanescente é aceitável
10.2.5. Se não for aceitável realizar tratamento adicional

10.3. As opções de tratamento de risco podem envolver uma ou mais das seguintes opções:
10.3.1. Evitar o risco ao decidir não iniciar ou continuar com a atividade que dá origem ao risco;
10.3.2. Assumir ou aumentar o risco de maneira a perseguir uma oportunidade;
10.3.3. Remover a fonte de risco;
10.3.4. Mudar a probabilidade;
10.3.5. Mudar as consequências;
10.3.6. Compartilhar o Risco (contratação, contratos ou seguros);
10.3.7. Reter o risco por decisão fundamentada

11. REFERÊNCIAS

• Norma ABNT NBR ISO 31000:2018 – Gestão de Risco - Diretrizes;

12. SANÇÕES E PUNIÇÕES

O descumprimento dessa norma pode acarretar sanções e punições aos envolvidos.

13. REVISÕES

Está norma deverá ser revisada anualmente ou extraordinariamente, a qualquer momento se for necessário, por um profissional qualificado para esta função.