 

**Centro Universitário Estácio de Sergipe**

**Pós-graduação em Segurança de Redes de Computadores**

**Política de Gestão de Riscos,**

**Gestão de Incidentes e**

**Infraestrutura Tecnológica na XPTO**

**Disciplina: Sistema de Gestão de Segurança da Informação**

**Professor: Adriano Lima**

**Equipe 4: Ely Barbosa**

**Jonathas Almeida**

**Marco Antonio**

**Márcio Costa**

**Missão, Visão e Valores da XPTO**

**MISSÃO**

Disponibilizar prestação de serviços de treinamentos em Informática com qualidade, através de soluções eficazes e criativas, auxiliando nossos clientes na conquista de seus objetivos.

**VISÃO**

Ser referência em qualidade de serviços de treinamentos de Informática da Bahia nos próximos 05 anos, com o fundamental apoio dos nossos colaboradores e parceiros.

**PRINCÍPIOS E VALORES**

• Ética

• Transparência

• Confiabilidade

• Orientação a resultados

• Crescimento sustentável

• Valorização e respeito aos nossos parceiros e colaboradores.

**Política de Gestão de Riscos - PGR**

1. **Introdução**

Definição de Risco – efeito de incerteza nos objetivos (ABNT NBR ISO 31000:2009)

O risco é inerente à atividade de qualquer organização, por isso todas as organizações estão expostas aos riscos. Não podemos eliminá-los totalmente, mas podemos mitigá-los. Ainda assim existem os riscos positivos, que podem revelar oportunidades, e nesse caso devemos potencializá-los para melhor aproveitá-los.

Devemos investir cada vez mais em controles internos e ações de prevenção a eventos que possam impactar o alcance dos objetivos, através de um conjunto de métodos e atividades coordenadas para direcionar e gerir a Empresa no que se refere a riscos (Gestão de Riscos).

1. **Objetivos**

Estabelecer conceitos, diretrizes, atribuições e responsabilidades do processo de gestão de riscos da XPTO, bem como orientar a identificação, a análise, a avaliação, o tratamento, o monitoramento e a comunicação dos riscos institucionais.

1. **Abrangência**
2. **O que é a PGR na XPTO**

Para que os processos da XPTO funcionem em conformidade com os desenhos dos mesmos, uma abordagem voltada para riscos deve ser considerada, estabelecendo a proteção de todas as informações relacionadas aos processos de matrícula, pagamento e recebimento de contas, folha de pagamento, execução das aulas, seleção de professores, recepção de visitantes, atendimento de OS’s, e contratação e desligamento de colaboradores, visando garantir a continuidade dessas operações.

* 1. **Princípios norteadores**

Os princípios são partes integrantes dos processos organizacionais, devem agregar valor e ajudar nas tomadas de decisões, de forma sistemática e estruturada, e devem ser adequados e compatíveis com a organização. Pontos como conformidade, fatores humanos e melhoria contínua devem ser considerados, assim como a proteção dos dados e comprometimento na entrega de serviços para a manutenção do ambiente institucional.

Você destacou bem a importância dos princípios e como eles deve funcionar, mas não enquadrou isso na empresa.

1. **Gestores de Riscos**

Os gestores de riscos são os titulares responsáveis pelo gerenciamento dos riscos em seus respectivos escopos de atuação. São eles, o Diretor geral, a Assessoria Jurídica, o Coordenador administrativo-financeiro, o Coordenador pedagógico e a Coordenação da Segurança da Informação.

* 1. **Competências**

Compete aos gestores de riscos: decidir sobre a escolha dos processos que devam ter os riscos gerenciados; estabelecer as ações de tratamento ou monitoramento; fixar um prazo para implementação; priorizar os riscos (tratamento imediato, curto prazo, médio prazo ou longo prazo); avaliação dos resultados obtidos por meio de indicadores; manter ações de aperfeiçoamento contínuo.

Falta definir o papel de cada gestor no escopo de riscos.

1. **Comitê de Avaliação de Riscos – CAR**

Foi criado o Comitê de Avaliação de Riscos, sob coordenação da Diretoria Geral, que possui as seguintes competências: aprovação de políticas, diretrizes, metodologias e mecanismos para divulgação e implementação da gestão de riscos e seus controles internos; promover o desenvolvimento contínuo, e a integração dos colaboradores incentivando a adoção de boas práticas de gestão de riscos; garantir o Compliance; supervisionar o mapeamento, a avaliação e o monitoramento dos riscos; e oferecer suporte necessário para a efetiva implementação da PGR na instituição.

* 1. **Diretrizes**

O gerenciamento de riscos deve ser realizado semestralmente, abrangendo os processos de trabalho, sistemas informatizados, gestão orçamentária, gestão de pessoas e Compliance, visando reduzir os riscos negativos e potencializando os riscos positivos (oportunidades). O ciclo de gerenciamento de riscos de cada processo de trabalho será decidido por cada gestor, levando em conta o limite máximo estipulado anteriormente.

1. **Tratamento de Riscos**

Evitar – Não iniciar ou deixar de utilizar o item/atividade que representa o risco;

Eliminar – destruir a respectiva fonte causadora;

Mitigar – Implementar medidas para reduzir os impactos e a probabilidade de ocorrência;

Aceitar – Não fazer nada previamente, de forma consciente e justificada;

Transferir – Tornar outra parte responsável pelo risco;

Aumentar – riscos positivos devem ser explorados para melhor aproveitá-los.

* 1. **Ações de tratamento de riscos**

Os riscos considerados muito baixo poderão ser apenas monitorados, mas quando a sua avaliação indicar um risco estratégico, orçamentário ou de imagem da instituição, podemos definir ações para tratamento dos mesmos de acordo com os seguintes prazos:

Tratamento Imediato – classificado como risco alto ou extremo;

Curto prazo – classificado como risco médio;

Médio e Longo prazo – classificado como risco baixo;

1. **Níveis de riscos**
2. **Processo de gestão de riscos**
3. **Matriz de Riscos**
4. **Ferramentas de avaliação de riscos**
5. **Referências**

- DESCRICAO DA EMPRESA.pdf (Aula Pós)

- Apresentação PSI - EQUIPE 2.pdf (Equipe 2)

- Política de Segurança da Informação da XPTO.pdf (Equipe 2)

- [http://www.ans.gov.br/images/stories/A\_ANS/Transparencia\_Institucional/gestao\_de\_](http://www.ans.gov.br/images/stories/A_ANS/Transparencia_Institucional/gestao_de_riscos/cartilha-gestao-de-riscos.pdf)

[riscos/cartilha-gestao-de-riscos.pdf](http://www.ans.gov.br/images/stories/A_ANS/Transparencia_Institucional/gestao_de_riscos/cartilha-gestao-de-riscos.pdf)

- <https://www.ufcspa.edu.br/ufcspa/normasedocs/politica-de-gestao-de-riscos.pdf>

- [http://www.ans.gov.br/images/stories/A\_ANS/Transparencia\_Institucional/gestao\_de\_](http://www.ans.gov.br/images/stories/A_ANS/Transparencia_Institucional/gestao_de_riscos/manual-de-gestao-de-riscos-da-ans.pdf)

[riscos/manual-de-gestao-de-riscos-da-ans.pdf](http://www.ans.gov.br/images/stories/A_ANS/Transparencia_Institucional/gestao_de_riscos/manual-de-gestao-de-riscos-da-ans.pdf)

-

**Gestão de Incidentes**

1. **Introdução**
2. **Termos e definições principais**

1. **Objetivos do Gerenciamento de Incidentes**
2. **Escopo da Gestão de Incidentes**
3. **Benefícios**
4. **Funções e responsabilidades**
5. **Fluxo do processo**
6. **Principais atividades do processo**
7. **Referências**

- DESCRICAO DA EMPRESA.pdf (Aula Pós)

- Apresentação PSI - EQUIPE 2.pdf (Equipe 2)

- Política de Segurança da Informação da XPTO.pdf (Equipe 2)

-

-

-

-

**Infraestrutura Tecnológica**

1. **Introdução**
2. **Infraestrutura ATUAL** 
   1. **Hardware e software**

1. **Melhorias Sugeridas**
   1. **Hardware e software**
2. **Diretrizes gerais**
3. **Infraestrutura FINAL XPTO**
4. **Referências**

- DESCRICAO DA EMPRESA.pdf (Aula Pós)

- Apresentação PSI - EQUIPE 2.pdf (Equipe 2)

- Política de Segurança da Informação da XPTO.pdf (Equipe 2)

-

-

-