QUESTOR POLÍTICA DE GESTÃO DE ATIVOS DA TECNOLOGIA DA INFORMAÇÃO		
ÁREAS RESPONSÁVEIS Tecnologia da Informação	**APROVADO POR** Comitê de Segurança da Informação	**DATA DA ÚLTIMA ATUALIZAÇÃO** 21/07/2023
VERSÃO 02	**CLASSIFICAÇÃO** Uso Interno	**CÓDIGO** Questor_PolíticadeGestãodeAtivosdaTecnologiadaInformação

Resumo

A gestão de ativos é fundamental para que se alcance os objetivos traçados no planejamento estratégico. Diante disso, se faz necessário a gestão de software e hardware, a fim de criar procedimentos capazes de garantir a disponibilidade e integridade dos ativos em uso, preservando assim a informação gerada ou mantida.

Índice

1- Objetivo

O objetivo desta política é garantir que os ativos de informação da Questor Sistemas S.A. sejam identificados adequadamente e que os controles de proteção recomendados para estes ativos da informação estejam em vigor.

Para manter a segurança e continuidade do negócio da Questor Sistemas, é fundamental mapear e monitorar os ativos tecnológicos, para maior controle da empresa, auxiliando na aplicação de atualizações, controles de segurança, gestão de riscos e também na recuperação de incidentes.

2- Abrangência

Esta política se aplica a todos os ativos de informação na Questor Sistemas S.A., incluindo ativos fora da empresa armazenados em um serviço de nuvem. Ativos de informação neste contexto, incluem documentos, base de dados, contratos, documentação de sistemas, procedimentos, log de sistemas, softwares, servidores, arquivos pessoais e compartilhados.

3- Declarações da Política

Dos princípios gerais

1. A política de Gestão de Ativos da Tecnologia da informação deve estar alinhada à Política de Segurança da Informação da Questor Sistemas S.A.
2. A política de Gestão de Ativos da Tecnologia da informação deve estar alinhada com uma gestão de continuidade de negócios em nível organizacional.
3. O processo de mapeamento de ativos de informação deve estruturar e manter um registro de ativos de informação, destinados a subsidiar os processos de gestão de risco, de gestão de continuidade e de gestão de mudanças nos aspectos relativos à segurança da informação.
4. As rotinas de inventário e mapeamento de ativos de informação devem ser orientadas para a identificação dos ativos de informação da organização, a fim de manter o escopo da organização mapeado e documentado.

5. O processo de mapeamento de ativos de informação deve considerar, preliminarmente, os objetivos estratégicos da organização, seus processos internos, os requisitos legais e sua estrutura organizacional.
6. O registro de ativos de informação resultante do processo de mapeamento de ativos de informação deverá conter: os responsáveis (proprietários e custodiantes) de cada ativo de informação; as informações básicas sobre os requisitos de segurança da informação de cada ativo de informação; os contêineres de cada ativo de informação; as interfaces de cada ativo de informação e as interdependências entre eles.

Os seguintes ativos de informação devem ser considerados no processo de mapeamento de ativos de informação:

1. Ativos físicos – Eletricidade, ar condicionado, escritórios;
2. Banco de dados;
3. Hardwares – Computadores, notebooks, servidores, impressoras, modens, headset, mouses, teclados, telefones, dispositivos móveis ou cartões memória;
4. Serviços – Terceirizados, mas também online como Gmail, Google Drive;
5. Softwares – Desenvolvidos, comprados e gratuitos;
6. Níveis de permissões;

4- Diretrizes

4.1- Informações ou ativos de informação de instalações de processamento de informações devem ser inventariados e documentados e esse registro deve ser mantido atualizado.

- A categorização do inventário deve ser aprovada pelas partes apropriadas ou autoridade de autorização.
- A organização emprega o uso de mecanismos automatizados para identificar sistemas autorizados e não autorizados, incluindo hardware ou software.

- O inventário também deverá incluir atualizações ou remoções do sistema de informação.

4.2- Das responsabilidades do proprietário do processo

- Identificar potenciais ameaças aos ativos de informação;
- Identificar vulnerabilidades dos ativos de informação;
- Consolidar informações resultantes da análise do nível de segurança da informação de cada ativo de informação ou de grupos de ativos de informação em um relatório;
- Avaliar os riscos dos ativos de informação ou do grupo de ativos de informação.
- Indivíduos que requerem acesso aos sistemas de informação devem seguir o procedimento adequado para receber tal acesso, como descritos na política de controle de acesso e catalogadas no sistema de gestão de ativos.
- Os processos em torno do gerenciamento de mudança e de configuração também serão estabelecidos e monitorados.
- Todos os ativos de informação devem ser devolvidos após a rescisão do contrato de trabalho ou contrato.

4.3- Criticidade do ativo de informação

- A criticidade dos ativos de informação críticos da organização é determinada pelo:
  1. Requisitos legais;
  2. Pelo valor financeiro;
  3. Pelo seu potencial de agregar valor ao negócio;
  4. Por sua vida útil

4.4- Classificação das informações

- Todos os ativos de informação devem ser classificados de acordo com sua criticidade.

- As informações armazenadas, transmitidas, processadas ou que se encontram sob a guarda dos ativos de informação da Questor Sistemas S.A. devem ser classificados de acordo com as definições já estabelecidas na Política de Classificação da Informação.

4.5- Manipulação de mídia

- A mídia removível também deve ser gerenciada pelo mesmo procedimento de classificação de ativos de informação usado pela organização.
- A mídia removível deve ser protegida contra acesso não autorizado e uso indevido durante o uso e em trânsito, e deve ser descartada com segurança, usando os procedimentos apropriados.
- A mídia contendo informações confidenciais e internas do [Órgão ou entidade] devem ser protegidas contra acesso não autorizado, uso indevido, corrupção durante o transporte e, preferencialmente, com o uso de criptografia.

5- Ciclo de Vida

a) Um processo de gestão de ativos deve ser estabelecido e documentado, para garantir que os ativos de tecnologia da informação sejam gerenciados e monitorados;
b) O processo de gestão de ativos deve levar em consideração as fases do ciclo de vida do ativo:
   I. Planejamento – Fase de alinhamento das ações com a estratégia corporativa. Esta fase envolve a revisão dos ativos que são atualmente usados em toda a organização e análise dos custos de compra e instalação de novos ativos de TI.
   II. Aquisição – Fase de definição do padrão técnico, empresas fornecedoras, contratações e estabelecimento de acordo contratuais;
   III. Implantação - Fase de configuração/instalação técnica e disponibilização conforme padrões estabelecidos;
   IV. Gerenciamento - Fase de controle, apoio técnico, manutenção, atualização e monitoração;

V. Descarte – Processo realizado quando um bem perde sua utilidade e torna-se antieconômico. Esta fase corresponde a transferência de um bem para uma outra categoria, que são: material obsoleto, inservível ou excedente.

c) O planejamento das ações relacionados à gestão de ativos devem estar em conformidade com o plano estratégico da área de tecnologia da informação da Questor Sistemas S.A.;

d) Na aquisição de ativos físicos ou de software da Questor Sistemas S.A. deve-se estabelecer formalmente uma área única responsável pela aquisição;

e) Os ativos físicos ou de software da Questor Sistemas S.A. devem ser padronizados, para serem adquiridos e disponibilizados conforme perfil funcional e homologados baseado nestes padrões;

f) As licenças de ativos de software e períodos de garantia dos ativos físicos devem ser controladas pela área técnica da Questor Sistemas S.A.;

g) Para cada ativo físico da Questor Sistemas S.A. identificado, deve ser definido e nomeado o seu respectivo responsável funcional;

h) Um fluxo com critérios específicos deve ser estabelecido para o descarte dos ativos físicos e de software, levando em consideração a máxima utilização, o que, por que, como e onde descartar;

i) A área de gestão de ativos da Questor Sistemas S.A. deve ser responsável, mas não somente, por:

I. Estabelecer os padrões funcionais para aquisição;

6- Inventário

a) Os ativos de tecnologia da informação da Questor Sistemas S.A. devem ser inventariados, claramente identificados e registrados;

b) As áreas de patrimônio com o apoio da área de gestão de ativos da Questor Sistemas S.A. têm a responsabilidade de realizar periodicamente os inventários e armazenar os resultados por um período de 2(dois) anos para fins de auditoria interna;

c) Periodicamente deve haver uma revisão pela área técnica de segurança da informação para assegurar que os ativos de tecnologia da informação da Questor Sistemas S.A. estejam em conformidade com o inventário;

7- Uso Aceitável

a) Os ativos de tecnologia da informação da Questor Sistemas S.A. são destinados para uso das atividades relacionadas ao trabalho da Questor Sistemas S.A., assim, devem ser utilizados para este fim por seus respectivos usuários e responsáveis;

b) Os usuários devem estar atentos aos princípios de segurança da informação (Confidencialidade, Integridade e Disponibilidade) e perfeito funcionamento na utilização dos ativos de tecnologia da informação da Questor Sistemas S.A.;

c) Os usuários devem manter a integridade (configurações) dos ativos físicos e de software da Questor Sistemas S.A.. Caso seja necessário, deverá entrar em contato com a Central de Serviços, que acionará as áreas responsáveis com prerrogativa para realizar estas atividades;

d) Os ativos de tecnologia da informação da Questor Sistemas S.A. disponibilizados pela empresa, devem ser cadastrados e configurados com identificação única, padrões mínimos de segurança e usuário responsável pelo uso, no intuito de serem homologados e incorporados na rede corporativa.

8- Boas Práticas

a) Sempre que possível, os ativos físicos portáteis (notebooks, celulares, etc.) devem permanecer nas instalações da Questor Sistemas S.A. para evitar exposição e risco de furto ou roubo;

b) É recomendável que ao trafegar com ativos físicos portáteis (notebooks, celulares, etc.) da Questor Sistemas S.A, estes sejam devidamente protegidos, guardados em locais seguros ou não exposto, como por exemplo na mala do carro;

c) Em aeroportos ou taxis, recomenda-se que ativos físicos portáteis (notebooks, celulares, etc.), sempre estejam sob sua visão e guarda.

9- Adequação da Política

a) Os novos projetos de desenvolvimento ou para novas aquisições, devem seguir os padrões estabelecidos nesta política;

b) Para estarem adequados a esta política, as implementações necessárias deverão ocorrer no prazo de 1(um) ano a partir de sua publicação;

c) Caso não seja possível a adequação, recurso técnico ou processo, o Comitê de Segurança da Informação deve documentar estar ciente, para fins de auditoria.

10- Referências

- ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação – Técnicas de segurança – Sistemas de gestão da segurança da informação – Requisitos;
- ABNT NBR ISO/IEC 27002:2013 Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação;
- Framework Information Technology Infrastructure Library – ITIL, v. 4, conjunto de boas práticas a serem aplicadas na infraestrutura, operação e gerenciamento de serviços de TI;

11- Revisões e Aprovações

Data	Versão	Descrição	Autor
16.08.2021	1.0	Criação da Política	Comitê de Segurança da Informação
21.07.2023	2.0	Atualização da Política	Setor de TI e Setor de Proteção de Dados