RZK digital media

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

PROPÓSITO

Esta política estabelece as diretrizes para a gestão de segurança da informação, que regem os sistemas de informação da RZK Media.

Os objetivos da Política de Segurança da Informação da RZK Media são os seguintes:

- Assegurar direção para o cumprimento dos requisitos legais e regulamentares;
- Orientar a todo o pessoal da RZK Media sobre como proteger os ativos de informação, de uma maneira que haja um equilíbrio de custo, eficácia, racionalidade, e um nível proporcional de proteção; e
- Fornecer uma base comum para o desenvolvimento de normas de segurança organizacional e práticas eficazes de gestão de segurança da RZK Media.

ESCOPO / APLICABILIDADE

Estas políticas se aplicam a todos colaboradores, colaboradores temporários, contratadores, consultores, vendedores, provedores de serviço, parceiros, afiliados, terceiros, ou qualquer outra pessoa ou entidade, autorizada a utilizar os recursos de informação (a seguir referida para “usuários”). Este inclui todas as informações de sistemas, hardware, dados, Media e arquivos em papéis na RZK Media e benefícios aprovados para terceiros.

Esta política também se aplica a todos os sistemas, redes e usuários conectados aos recursos na RZK Media através de quaisquer meios, incluídos, mas não limitados a: acesso local, linhas alugadas, pontos de acesso wireless, ou qualquer outro dispositivo de telecomunicações, quer através de redes privadas, ou de redes

públicas. Também se aplica a todos as conexões locais ou remotas de terceiros, bem como ativos não envolvidos no armazenamento, processamento e transmissão de informações ou dados.

Todas as informações, sistemas, redes e outros ativos de informação devem ter controles adequados para atingir níveis apropriados de confidencialidade, integridade, disponibilidade, responsabilidade e segurança. Estes ativos valiosos devem ser administrados e controlados, para proteger contra perda, utilização indevida, divulgação, fraude ou destruição.

DECLARAÇÃO DA POLÍTICA

i. Estrutura das Políticas de Segurança da Informação:

A informação é um recurso que, como outros ativos importantes, tem valor para uma organização e consequentemente necessita ser adequadamente protegida. Segurança da Informação é projetada para permitir o uso de informações somente de acordo com intenções da administração. Ela protege a informação de uma ampla gama de ameaças com o objetivo de apoiar os esforços de continuidade de negócios, segurança e minimizar os efeitos adversos relacionados aos impactos nos negócios.

A segurança da informação é conseguida através da implementação de um conjunto adequado de controles, em ambas as políticas e práticas. Esses controles incluem as políticas, normas, diretrizes e procedimentos que guia os processos de negócios, para alcançar e manter preservada as metas da Organização. Também incluem o uso e manutenção de várias tecnologias destinadas a reforçar as políticas, normas e orientações.

ii. Obrigações do Departamento de Tecnologia da Informação:

Esta política define a segurança da informação, administração da política e sua execução:

1. **Segurança da Informação** – A empresa deve fornecer para o seu pessoal uma evidente orientação, para

a proteção de ativos de informação ao cliente.

2. **Autorização, acordos e contratos** – Modalidades envolvendo acessos de terceiros às instalações de processamento de informação organizacional, devem ser com base em um contrato formal contendo, ou referindo-se, todos os requisitos de segurança, para assegurar a conformidade com políticas de segurança interna e normas da RZK Media.

3. **Classificação de Dados** – Sistemas de informação e dados da RZK Media devem ser classificados para indicar a necessidade, prioridade e grau de proteção que são necessários para proteger a informação proporcional ao risco, e para permitir controles adequados.

4. **Gestão de Ativos de TI** – Os recursos de TI (hardware, software e equipamentos), devem ser gerenciados para garantir a segurança e a proteção do valor do ativo.

5. **O Pessoal de TI** – O time de T.I. desempenha um papel vital na proteção dos ativos de informação. Para proteger estes ativos, as responsabilidades de segurança pessoal, devem ser identificadas e incorporadas em todo o ciclo de vida de trabalho. O time precisa entender os requisitos para proteger os ativos de informação e suas responsabilidades para a adesão e aplicação desses requisitos.

6. **Segurança Ambiental e Física** – Ambiente de processamento de informação, equipamentos, e registros devem ser fornecidos proteção de segurança de ambiente físico, que são compatíveis com o resultado de uma análise de risco.

7. **Gestão de Operações** – A gestão e operação dos ativos de informação da RZK Media, devem conter controles para proteger as informações e os processos que os utilizam.

8. **Backup e Restore** – Gestão de dados inclui uma estratégia de backup baseado em risco. Análises adequadas de restaurações ajudam a garantir a valorização de dados e software, após falhas do sistema ou desligamento acidental.

9. **Segurança de Comunicações** – Todas as informações da RZK Media classificados como não-públicas,

devem ser transmitidas através de um caminho confiável, ou médio, com controles eficazes que permitam autenticidade do conteúdo, prova da apresentação, prova da recepção, e não-repúdio de origem.

10. **Controle de Acesso** – O acesso aos ativos de informação da RZK Media, só será concedido quando expressamente autorizadas, e justificado baseado na função de trabalho. Para todas as informações e dados, deve ser dedicado algum nível de proteção, que estará em acordo com seu nível de classificação.

11. **Logs, Monitoramento e relatórios** – Logs de operações e Manutenção de natureza material devem ser mantidos para todos os sistemas de informação. Estes logs devem documentar data / hora / descrições de inatividade do sistema, Manutenção do sistema, e as anomalias de segurança operacionais.

12. **Resposta de Incidente** – Uma abordagem clara e concisa é definida e comunicada, em relação à resposta exigida quando incidentes de segurança foram identificados.

13. **Gestão de Mudança** – Alterações ao software, bases de dados e configurações de hardware, têm implicações de segurança e continuidade de negócios. Alterações devem ser gerenciadas através de uma política baseada no risco, com procedimentos adequados para garantir a fiscalização e autorização de mudanças.

14. **Ciclo de Vida de Desenvolvimento de Sistemas** – Mudanças significativas no sistema de informação devem ser gerenciadas para assegurar a confiabilidade, utilidade e aderência às políticas de segurança. Isso inclui todas as fases de estudo para revisão de pós-implementação.

iii. Requisitos de Segurança de Informação

A segurança da informação é um conjunto de políticas, normas, tecnologias e práticas que foi projetado para proporcionar:

Confidencialidade: os processos, políticas e controles utilizados para proteger informações dos clientes e da instituição, contra o uso ou acesso não autorizado.

Integridade: Integridade de dados ou sistemas refere-se aos processos, políticas e controles utilizados para garantir se a informação não foi alterada de forma não autorizada e que os sistemas estão livres de manipulação não autorizada, que poderá comprometer a exatidão, integridade e confiabilidade.

Disponibilidade: A disponibilidade de sistemas em curso aborda os processos, políticas e controles utilizados para garantir que os usuários autorizados tenham acesso rápido à informação. Este objetivo protege contra tentativas intencionais ou acidentais para negar o acesso de usuários legítimos à informação ou sistemas.

Responsabilização: uma responsabilização clara envolve os processos, políticas e controles necessários para traçar ações para sua fonte. Prestação de contas suporta diretamente o não-repúdio, dissuasão, prevenção de intrusões, monitoramento de segurança, recuperação e admissibilidade jurídica de registros.

Garantia: Garantia aborda os processos, políticas e controles usados para desenvolver a confiança que a segurança técnica e operacional trabalha como pretendido. Os níveis de garantia são parte do projeto do sistema e incluem disponibilidade, integridade, confidencialidade e responsabilização. A garantia destaca que os sistemas de segurança forneçam a funcionalidade pretendida enquanto previnem ações indesejadas.

Não-repúdio: Integridade e responsabilização se combinam para produzir o que é conhecido como não-repúdio. Não-repúdio pode reduzir as fraudes e promover o cumprimento legal de acordos e transações eletrônicas.

CUMPRIMENTO

Todos os usuários, devem respeitar as políticas detalhadas nestes documentos do Programa de governança da Tecnologia da Informação. Qualquer usuário que tenham utilizado abusivamente do privilégio facilitado de acesso a sistemas de negócios, ou não, em conformidade com qualquer destas políticas, podem ser sujeitos a medidas disciplinares, até a inclusive demissão. Órgãos Federal, estadual e / ou agências locais de aplicação

da lei, também podem ser notificados, se existirem provas de atividades supostamente criminosas.

Contate o Departamento Jurídico para esclarecimentos de dúvidas sobre ações disciplinares relativas a violações da política.

RZK

digital

media