POLÍTICA DE SEGURANÇA CIBERNÉTICA

1. Termos e Definições

Ameaça: Fonte potencial de dano; elemento ou atividade que possui potencial de causar uma consequência.

Evento de segurança da informação: Ocorrência identificada em um sistema, serviço ou rede que indica uma possível violação da Política de segurança da informação ou falha de controles de segurança da informação, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.

Evidência: Dados que apoiam a existência ou a veracidade de alguma coisa.

Incidente: Qualquer ocorrência que não é parte padrão da operação de um serviço e que pode causar uma indisponibilidade, redução na qualidade do mesmo, perda de integridade ou confidencialidade das informações.

Risco Cibernético: Ameaça à confidencialidade, integridade e disponibilidade das informações no Espaço Cibernético.

Vulnerabilidade: Brecha sistêmica que permite ataque de exploração ou violação à segurança da informação de uma aplicação/rede.

2. Objetivo

Estabelecer as diretrizes para compor um programa de Segurança Cibernética.

3. Abrangência

Esta política abrange todos os sistemas, sites, programas, aplicativos e monitoramento de Segurança da Informação e Segurança Cibernética no ambiente da Wx3 Sistemas LTDA ME, independente da sua localização física..

4. Atribuições e responsabilidades

4.1. Área de Segurança da Informação

Realizar a Gestão de Incidentes de Segurança da Informação.

a) Verificar a conformidade desta Política.

b) Implantar controles de Segurança da Informação de acordo com as instruções deste regulamento.

c) Desenvolver e atualizar, sempre que necessário, as diretrizes gerais para a Gestão de Riscos de Segurança da Informação e Segurança Cibernética.

d) Elaborar diretrizes para coleta e preservação de evidências de incidentes de segurança da informação.

e) Elaborar diretrizes para comunicação sobre incidentes de segurança da informação.

f) Implementar melhorias no tratamento de incidentes de segurança da informação;

g) Proteger o valor e a reputação da Wx3 Sistemas.

h) Identificar violações de Segurança Cibernética, estabelecendo ações sistemáticas de detecção, tratamento e prevenção de incidentes, ameaças e vulnerabilidades nos ambientes físicos e lógicos, objetivando a mitigação dos riscos cibernéticos, dentre outros.

i) Garantir a continuidade de seus negócios, protegendo os processos críticos de interrupções inaceitáveis causadas por falhas ou desastres significativos.

j) Atender aos requisitos legais, regulamentares e às obrigações contratuais pertinentes a atividade da empresa.

k) Estabelecer e melhorar continuamente um processo de Gestão de Riscos de Segurança Cibernética.

4.2 Gestor de Segurança da Informação

Atuar como proprietário do Processo de Gestão de Tratamento e Resposta a Incidentes de Segurança da Informação.

4.3 Colaboradores

a) Conhecer e cumprir as diretrizes estabelecidas nesta Política.

b) Reportar qualquer incidente de Segurança da Informação, mesmo que suposto, o mais rapidamente possível, por meio do canal apropriado.

5. Diretrizes

Os incidentes de segurança da informação podem ser notificados por qualquer usuário da Wx3 Sistemas ou identificados por áreas da Tecnologia da Informação “TI”..

5.1 Plano de Segurança Cibernética

Proteger as informações contra acesso, modificações, destruição ou divulgação não autorizada.

a) Prover a adequada classificação da informação, sob os critérios de confidencialidade, disponibilidade e integridade.

b) Assegurar que os recursos utilizados para o desempenho de sua função sejam utilizados apenas para as finalidades aprovadas pela Wx3 Sistemas.

c) Garantir que os sistemas e as informações sob responsabilidade da Wx3 Sistemas estejam adequadamente protegidos.

d) Garantir a continuidade do processamento das informações críticas de negócios.

e) Selecionar os mecanismos de segurança da informação, balanceando fatores de riscos, tecnologia e custo.

f) Comunicar imediatamente à área de Segurança da Informação, quaisquer descumprimentos da Política Corporativa de Segurança Cibernética.

5.2 Proteção do Ambiente

Devem ser constituídos controles e responsabilidades pela gestão e operação dos recursos de processamento das informações que garantem a segurança na infraestrutura tecnológica de redes locais e internet, através de um gerenciamento efetivo no monitoramento, tratamento e respostas aos incidentes, para minimizar o risco de falhas e a administração segura de redes de comunicações, incluindo a gestão de serviços contratados de processamento e armazenamento de dados e informações em nuvem.

5.3 Segurança Física e Lógica

Os equipamentos e instalações de processamento de informação críticas ou sensíveis devem ser mantidos em áreas seguras, com níveis e controles de acesso apropriados, incluindo proteção contra ameaças físicas e ambientais. Os requisitos de segurança de sistemas de informação devem ser identificados e acordados antes do seu

desenvolvimento e/ou de sua implementação, para que assim possam ser protegidos visando a manutenção de sua confidencialidade, integridade e disponibilidade. Os colaboradores e terceiros da Wx3 Sistemas devem ser treinados periodicamente sobre os conceitos de Segurança da Informação, através de um programa de conscientização.

5.4 Gestão de Acesso

Os acessos às informações devem ser controlados, monitorados, restringidos à menor permissão e privilégios possíveis, revistos periodicamente com a aprovação do gestor do responsável e o da informação, e cancelados tempestivamente ao término do contrato de trabalho do colaborador ou do prestador de serviço.

5.5. Processamento, Armazenamento de Dados e Computação em Nuvem

Para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, a Wx3 Sistemas deve possuir procedimentos efetivos para a aderência às regras previstas na regulamentação em vigor.

5.6. Continuidade de Negócios

O processo de gestão de continuidade de negócios relativo a segurança da informação, deve ser implementado para minimizar os impactos e recuperar perdas de ativos da informação, após um incidente crítico, a um nível aceitável, através da combinação de requisitos como operações, funcionários chaves, mapeamento de processos críticos, análise de impacto nos negócios e testes periódicos de recuperação de desastres. Incluem-se nesse processo, a continuidade de negócios relativos aos serviços contratados de nuvem e os testes previstos para os cenários de ataques cibernéticos.

6. Considerações Finais

6.1. Treinamento

Um programa de conscientização em Segurança Cibernética à garantia dos objetivos e diretrizes definidos nesta Política é realizado adequando-se às necessidades e responsabilidades específicas de cada colaborador e, onde pertinente, terceiros da Companhia.

Criado por: Jurandir Júnior

Wx3 Sistema LTDA ME