Ketra
soluções inteligentes

POLITICA DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Objetivo:

A Política de Gestão de Incidentes de Segurança da Informação tem como finalidade estabelecer os princípios, diretrizes e responsabilidades relacionadas à identificação, registro, tratamento e prevenção de incidentes de segurança da informação e cibernética na Ketra Soluções Inteligentes.

Seu objetivo é garantir uma resposta adequada e tempestiva a quaisquer incidentes que possam comprometer a confidencialidade, integridade e disponibilidade das informações, minimizando riscos e reduzindo ao máximo os impactos sobre as operações e os negócios da empresa.

Ketra
soluções inteligentes

Abrangência:

A Política de Gestão de Incidentes de Segurança da Informação possui abrangência corporativa na Ketra, ou seja, afeta todas as suas áreas de negócio, filiais, escritórios e demais operações no que se refere a ocorrência de incidentes de segurança da informação.

Ketra
soluções inteligentes

Conceitos e definições:

Informação:

- Qualquer conjunto de dados que possua significado compreensível e valor para a Ketra, seus clientes, parceiros ou colaboradores. A informação pode ser de propriedade da empresa ou estar sob sua custódia

Colaborador:

- Todos os profissionais que mantenham vínculo empregatício com a Ketra, em qualquer modalidade de trabalho — presencial, teletrabalho, home office, híbrido ou remoto —, bem como aqueles que possuam participação social em quaisquer das unidades da organização

Gestor:

- Colaborador que exerce cargo de liderança na Ketra, como Diretor, Gerente ou Gestor de equipe

Recurso:

- Qualquer ativo, tangível ou intangível, pertencente à Ketra ou sob sua responsabilidade, que possua valor para a organização. São considerados recursos: pessoas, ambientes físicos, tecnologias, serviços contratados, recursos em nuvem, sistemas e processos.

Ketra
soluções inteligentes

Conceitos e definições:

Recursos Tecnológicos:

- Equipamentos, sistemas, ferramentas, plataformas ou metodologias que sustentam o armazenamento, processamento ou transmissão de informações e que dão suporte aos processos de negócio da empresa.

SLA (Service Level Agreement – Acordo de Nível de Serviço):

- Documento que define os níveis de qualidade, disponibilidade e desempenho esperados na entrega de um serviço, com base em critérios objetivos previamente acordados entre as partes envolvidas

Ketra
soluções inteligentes

Diretrizes:

Esta Política não será extinta ou cancelada. Será revisada em períodos não superior a um ano, quando será publicada uma nova versão, caso haja necessidade de ajustes.

Será, portanto, substituída por outra com mesmo objetivo e valor que a administração entender cabível ou necessário.

Ketra
soluções inteligentes

Papeis e responsabilidades:

As responsabilidades do Comitê de Segurança da Informação da Ketra são:

- Condução do processo de Gestão de Incidentes de Segurança da Informação;
- Investigação de incidentes, levantamento, cadeia de custódia e segurança das evidências;
- Acompanhamentos dos planos de tratamento junto aos responsáveis pelos incidentes e criação de indicadores e relatórios;
- Comunicação aos Gestores responsáveis;
- Realização de análises pós-incidentes (post mortem) para identificação e tratamento de causas raiz e aprimoramento de processos da empresa e do próprio processo de gestão de incidentes de segurança da informação

Ketra
soluções inteligentes

Papeis e responsabilidades:

As responsabilidades dos Colaboradores são:

- Devem informar imediatamente ao Comitê de Segurança da Informação todas as violações às Políticas de Segurança da Informação, incidentes, violações de acessos ou anomalias que possam indicar a possibilidade de incidentes, sobre os quais venham a tomar conhecimento.

As responsabilidades da Gerência de Operações de TI são::

- Provimento dos acessos necessários para que o Comitê Gestor de Segurança da Informação possa realizar a identificação e investigação de incidentes de segurança;
- Responsável pelo provimento de trilhas de auditoria e evidencias para a investigação de incidentes;
- Suporte às investigações através do fornecimento de informações e esclarecimentos sobre o ambiente tecnológico e os processos da área

As responsabilidades dos Gestores são:

- Ao serem notificados sobre incidentes que envolvam recursos ou informações sob sua responsabilidade, devem colaborar com eventuais investigações e tratar os incidentes com a devida urgência e SLA's pré-definidos pelo ao Comitê Gestor de Segurança da Informação.

Ketra
soluções inteligentes

As responsabilidades da área Jurídica são:

- Suporte às questões legais relacionados a Incidentes de Segurança da Informação.

Papeis e responsabilidades:

Governança e Supervisão da Gestão de Incidentes:

- A gestão de incidentes de segurança da informação será conduzida operacionalmente pelo Comitê de Segurança da Informação, com coordenação do Departamento de Governança e Compliance, responsável por assegurar a rastreabilidade, a conformidade regulatória e o monitoramento das ações corretivas.

- O Departamento de Governança e Compliance, na função de Chief Compliance Officer (CCO), atuará como elo entre as áreas técnicas, o Departamento Jurídico, Recursos Humanos e a Alta Direção, avaliando impactos legais, contratuais, reputacionais e regulatórios decorrentes dos incidentes.

- Os incidentes classificados como críticos, recorrentes ou com potencial impacto relevante para os negócios, clientes, contratos, proteção de dados pessoais ou imagem institucional serão submetidos ao Comitê de Ética, Riscos e Governança (CORG), que atuará como instância estratégica de supervisão e deliberação, podendo inclusive exercer função de Comitê de Crise.

- Compete ao CORG analisar relatórios técnicos, deliberar sobre medidas corretivas e disciplinares, aprovar planos de mitigação e acompanhar a implementação das ações até o encerramento formal do incidente.

Ketra
soluções inteligentes

Dos Critérios Gerais sobre os Incidentes de Segurança da Informação:

São considerados Incidentes de Segurança da Informação quaisquer fragilidades ou eventos adversos de segurança, confirmados ou sob suspeita, que levem ou possam levar ao comprometimento de um ou mais dos princípios básicos de segurança da informação: confidencialidade, integridade, disponibilidade e conformidade, colocando o negócio e seus objetivos em risco.

Todos os colaboradores devem notificar qualquer evento de segurança ou fragilidade observada que possam causar: prejuízos, interrupções, maus funcionamentos, imprecisão ou vazamento de informação nos sistemas da empresa.

Vulnerabilidades ou fragilidades suspeitas não deverão ser objeto de teste ou prova pelos colaboradores, sob o risco de violar a política de segurança cibernética e da informação, bem como provocar danos aos serviços ou recursos tecnológicos.

Ketra
soluções inteligentes

Dos Critérios Gerais sobre os Incidentes de Segurança da Informação:

A lista a seguir exemplifica, mas não esgota os possíveis incidentes de segurança da informação tratados nesta política:

- Qualquer evento adverso confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores, bem como estruturas físicas e lógicas associadas, que comprometa a confidencialidade, a integridade e a disponibilidade do ambiente da organização;
- Indisponibilidade do ambiente tecnológico em virtude de ataque maliciosos interno e externo;
- Vazamento de informações confidenciais (informações de clientes, informações estratégicas, outros);
- Tentativas interna ou externa de ganhar acesso não autorizado a sistemas, a dados ou até mesmo comprometer o ambiente de TI;
- Ato de violar uma política de segurança, explícita ou implícita;
- Uso ou acesso não autorizado a um sistema;
- Modificações em um sistema, sem o conhecimento, instruções ou consentimento prévio do proprietário do sistema;
- Compartilhamento de senhas

O conteúdo da notificação precisa ser claro, em formato simples e deve incluir as informações necessárias para a rápida e correta identificação do problema e da ação requerida.

Ketra
soluções inteligentes

Dos Critérios Gerais sobre os Incidentes de Segurança da Informação:

Os eventos abaixo não são considerados eventos de segurança da informação:

- Eventos acidentais (falhas de hardware ou sistêmicas) não intencionais;
- Eventos não maliciosos (erro humano ou descuido que não infrinja as regras de segurança da informação).

Todos os eventos de incidente de segurança da informação devem ser registrados nos controles e/ou ferramentas para a devida triagem e tratamento.

A Gestão de Incidentes de Segurança da Informação deve contemplar processos que atendam aos seguintes objetivos:

- Detecção: identificação de incidentes por meio de monitoração, relatórios, denúncias, informações obtidas de áreas parceiras ou qualquer outra análise de eventos adversos;
- Registro e análise: registro dos incidentes, análise, classificação quanto ao tipo, severidade e priorização;
- Comunicação: comunicação do incidente às partes envolvidas e caso necessário entidades externas;
- Resposta: contenção do incidente, análises forenses, custódia de evidências, tratamento do incidente e da causa raiz;
- Finalização: encerramento formal e análise pós mortem para identificação de possíveis melhorias em processos, controles e na própria Gestão de Incidentes.

Ketra
soluções inteligentes

Dos Critérios Gerais sobre os Incidentes de Segurança da Informação:

Violações ou tentativas de violação da Política de Segurança da Informação, de normas ou de controles de segurança da informação, intencionais ou não, são considerados incidentes de segurança.

Incidentes de segurança podem ser identificados por processos de monitoração da área de infraestrutura por Colaboradores que observem fragilidades, anomalias e violações que coloquem a segurança da empresa em risco.

Todos os incidentes de segurança da informação devem ser documentados, classificados, priorizados de acordo com a criticidade da Ketra e comunicados aos gestores responsáveis no momento apropriado.

Em casos mais simples e de baixa criticidade apenas o gestor responsável pelo recurso ou informação deve ser comunicado.

Em casos mais graves a Diretoria e a Gerência de Operações de TI devem ser comunicadas.

A investigação de incidentes de Segurança da Informação deve ser realizada exclusivamente pela Comitê Gestor de Segurança da Informação, de forma a garantir a privacidade e o sigilo das informações obtidas.

As informações obtidas e arquivadas pelo processo de Gestão de Incidentes de Segurança da informação devem ser protegidas de forma a garantir a privacidade de colaboradores e o sigilo das informações da empresa, não podendo ser fornecidas a outros departamentos ou auditorias.

A identificação de incidentes de segurança pode ocasionar o corte imediato dos acessos de colaboradores envolvidos ou a desconexão de sistemas, até que sejam concluídas as investigações necessárias.

O acesso às evidências e relatório de incidentes de segurança da informação é permitido apenas pelo Comitê Gestor de Segurança da Informação, a Gerência de Operações de TI e aos Gestores diretamente envolvidos nos incidentes.

A documentação de incidentes, resultados de investigações, evidências e suas soluções devem ser atualizadas logo após a conclusão do tratamento do incidente.

O contato para a notificação de incidentes de segurança da informação deve ser feito diretamente ao Comitê Gestor de Segurança da Informação através de canais previamente definidos.

Ketra
soluções inteligentes

Dos critérios gerais:

- Penalidades:

Descumprimentos configuram falta grave e podem resultar em sanções disciplinares, inclusive demissão por justa causa.

- Revisão e Atualização:

Deve ser feita pelo menos uma vez por ano, conforme boas práticas e legislações aplicáveis.

- Dúvidas:

Devem ser encaminhadas ao Comitê de Compliance Corg.

Ketra
soluções inteligentes

OBRIGADA

Ketra
soluções inteligentes