GESTDOC®
Gestão de Arquivos

Políticas de segurança da informação

Janeiro de 2024

Índice

Siglas e abreviaturas

Siglas	Definição
GD	Acrônimo de Gestdoc
DV	Acrônimo de Doc-visão
SITGD	Acrônimo de sector de it da Gestdoc
ETRISI	Equipa de Tratamento e Resposta a incidentes em segurança da informação

1. Contextualização

1.1. Introdução

O presente documento, tem como objetivo normatizar diversos aspectos relacionados à segurança da informação, em conformidade com a Política de Segurança da Informação do sistema Doc-visão da Gestdoc.

Por meio da orientação e do estabelecimento das diretrizes necessárias para proteger suas informações, a SITGD visa determinar os padrões de comportamentos relacionados à segurança da informação adequados às necessidades de seus clientes.

Os riscos típicos que a aplicação deste Código pretende evitar são:

- Revelação de informações sensíveis;
- Revelação de informações pessoais;
- Modificações indevidas de dados;
- Perda de dados;
- Interdições ou interrupções de serviços essenciais;
- Roubo/furto de propriedades.
- Utilização indevida dados.
- Acessos não autorizados.

Esses riscos ocorrem pelos seguintes motivos:

- **Negligência** – atos não intencionais de usuários.
- **Subversão** – ataques disfarçados praticados por usuários.
- **Acidente** – ocorrências acidentais e por fatores alheios.
- **Ataque furtivo** – ataques praticados por pessoas estranhas.
- **Ataque forçado** – ataques às claras praticados por usuários ou estranhos.
- **Ilícitas** - ocorrências Ilícitas e por fatores alheios

1.2. Responsabilidades

É de responsabilidade de todos os clientes conhecer e cumprir todas as obrigações decorrentes desta Política e regulamentações vigentes, bem como observar os mais altos padrões de conduta profissional ao conduzir suas atividades.

Também é dever de todos os clientes informar e reportar inconsistências em procedimentos e práticas definidas no presente documento à Gestdoc

1.3. Definições

Ameaças: Evento que tem potencial em si próprio para comprometer a informação, seja trazendo danos directos ou prejuízos indirectos decorrentes de situações inesperadas

Activos de informação: São meios de produção, armazenamento, transmissão e processamento de informações, os sistemas de informação, os locais aonde se encontram esses meios, as pessoas que têm acesso à essas informações, assim como as próprias informações coletadas, produzidas, processadas, custodiadas e descartadas.

Autenticidade: Propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por meio de um determinado sistema, órgão ou entidade.

Classificação da informação: Identificar quais são os níveis de proteção que as informações demandam e estabelecimento de classes de formas a identificá-las, além de determinar os controles de proteção necessários a cada uma delas.

Confidencialidade: Propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, entidade ou órgão não autorizado e credenciado.

Conformidade: Processo que visa verificar o cumprimento das normas estabelecidas.

Controle de acesso: Conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear acesso.

Criptografia: Método de codificação da informação que visa evitar que ela seja compreendida ou alterada por pessoas não autorizadas.

Dados pessoais: Todo e qualquer dado relacionado a pessoa.

Disponibilidade: Propriedade de que a informação esteja acessível e utilizável sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade no momento requerido.

Equipa de tratamento e resposta a incidentes em segurança da informação (ETRISI): Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações relacionadas a incidentes com **activos de informação**.

Gestor de segurança da informação: Funcionário responsável por gerir a segurança da informação.

Informação: Conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independente do suporte em que resida ou da forma pela qual seja veiculada.

Integridade: Propriedade de que a **informação** não foi modificada, suprimida ou destruída de maneira não autorizada ou acidental.

Tratamento da informação: Conjunto de acções referentes à recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da **informação.**

Vulnerabilidade: Fragilidade de um activo ou grupo de activos que pode ser explorada por uma ou mais **ameaças**.

2. Regras básicas da segurança da informação

2.1. Princípios da segurança da informação

Nossos compromissos com o tratamento adequado das informações do cliente estão fundamentados nos seguintes princípios:

- **Confidencialidade**

  Asseguramos que a informação do cliente não será divulgada a indivíduos, entidades ou aplicativos sem autorização prévia do cliente.

- **Integridade**

  Asseguramos que o conteúdo da informação não será alterado em qualquer momento de sua vida útil sem a solicitação do cliente. De tal modo que a informação permaneça intacta, íntegra e autêntica.

- **Disponibilidade**

  Asseguramos que o a informação estará disponível sempre que necessário para o cliente, desde que esteja autenticado e permitido a acede-la e houver a declaração da disponibilidade da mesma por parte da **GD**.

- **Responsabilização**

  Asseguramos que as operações realizadas no sistema por um determinado usuário serão vinculadas a sua conta com registros de actividades e históricos.

2.2. Ciclo de vida da informação

Para o efeito desta política, considera-se como ciclo de vida da informação o seguinte:

- **Manuseio**

  É a etapa aonde a informação é criada e manipulada.

- **Armazenamento**

  É a guarda da informação, na nossa base de dados.

- **Transporte**

  Ocorre quando a informação é solicitada de um ponto para o outro.

- **Descarte**

  É a declaração do fim da vida útil da informação.

2.3. Classificação da informação

Conforme o capítulo das definições, a classificação da informação é avaliada de acordo ao seu conteúdo e relevância. O acesso, divulgação e tratamento de um documento digital, dado ou informação são restritos aos funcionários que tenham necessidade de acede-las em razão de suas actividades dentro do sistema **DV,** sendo este acesso pautado pelas regras previstas nesta política e demais normas da empresa.

Toda a informação de uso corporativo deve ser classificada de acordo ao seu grau de sigilo para o negócio da empresa, portanto, considerando-se três níveis:

- **Confidencial**

  É o mais alto grau de sigilo, aplicadas às informações de caráter estratégico e que devem ser manuseadas por um grupo restrito de usuários. O acesso não autorizado a essas informações pode ter consequências críticas para o negócio, causando danos estratégicos à imagem da empresa.

- **Interno**

  São informações específicas para uso interno, com circulação exclusiva dentro da empresa. Essas informações podem estar disponíveis a todos os funcionários da empresa e devem ser utilizadas somente para atividades do cliente **GD**. Esse conteúdo, mesmo sendo de circulação livre dentro da empresa, não devem ser divulgados para externos sem os devidos cuidados, incluindo, quando necessário, a assinatura de acordos de confidencialidade ou de autorização formal previamente avaliada pela área responsável.

- **Público**

  São informações de circulação livre e domínio público. Esse tipo de informação não exige controles ou restrições de segurança para seu acesso ou guarda.

3. Sistema de Gestão da Segurança da informação

O sistema de gestão da segurança da informação é um conjunto de processos e boas práticas para estabelecer, implementar, operar, monitorar, revisar, manter e aprimorar a segurança da informação com ações em 4 grandes frentes de actuação:

- **Governança das políticas e procedimentos de segurança da informação**
- **Recursos e componentes de segurança da informação.**
- **Monitoramento contínuo do ambiente de tecnologia da informação;**
- **Gestão de crises e continuidade de negócios**

4. Controle internos da segurança da informação

O controle interno da segurança da informação na **GD** é fundamentado sobre os seguintes pilares:

- **Identificação/Avaliação de Ameaças e Vulnerabilidades**

  A identificação e avaliação dos riscos a que os processos e ativos estejam sujeitos e possíveis cenários de ameaça.

- **Ações de Prevenção e Proteção.**

  Serão adotadas rotinas padronizadas de prevenção e proteção dos processos e ativo, conforme previstas na norma interna, realizando análises de vulnerabilidade, testes de intrusão e outras avaliações específicas que certifiquem o cumprimento dos requisitos de segurança e as responsabilidades previamente estabelecidas.

  Destacando a execução periódica de testes de ataque e invasão, visando monitorar a eficiência de seu sistema de proteção a vulnerabilidades cibernéticas, a **GD** realiza testes periodicamente.

- **Monitoramento e Testes;**

  Devem ser implementados controles internos efetivos para proteção dos dados dos clientes, garantindo a sua confidencialidade, integridade, disponibilidade sempre observando as melhores práticas de mercado e regulamentações vigentes.

  A área de Segurança da Informação pode monitorar ou inspecionar os as informações que estiverem em suas custodia ou que interajam com os ambientes da **GD** sempre que considerar necessário.

- **Desenvolvimento contínuo**

São efectuadas actualizações contínuas na aplicação com vista na adaptação da solução **DV** de acordo ao mercado e as diferentes soluções encontradas mediante aos desafios propostos para melhor servir o cliente com segurança, disponibilidade e confiabilidade.

5. Gestão da segurança cibernética

5.1. Autenticação e controle de acessos

A prática de Controle de Acesso tem o objetivo de prevenir o acesso de indivíduos não autorizados ao ambiente e aos sistemas, garantindo assim a confidencialidade das informações. Para garantir um nível aceitável de controle de acessos, são executados os seguintes processos:

a. Controle de acessos através da matriz de segregação de função. Na matriz estão listadas todas as equipes, Colaboradores e acessos liberados;
b. Execução de procedimentos formalizados para a Concessão, Alteração, Revogação e Gerenciamento de acessos, sendo que para todos os procedimentos citados acima, é respeitado o princípio de menor privilégio e perfil mínimo restrito de acesso, conforme a matriz de segregação de função;
c. Todos os usuários são orientados a possuírem acesso apenas à informação de acordo com as necessidades;
d. É de responsabilidade do gestor da equipe o informe do nível de acessos para novos colaboradores.
e. Os acessos são limitados aos ativos de informação sob domínio da equipe do gestor.
f. Todos procedimentos de concessão e alteração do acesso dentro de uma equipe são aprovados pelo gestor responsável e pela diretoria de TI;
g. Existem casos específicos de colaboradores que necessitam de acesso aos ativos de informação pertencentes à outras equipes. Para estes casos, todos os procedimentos de