

# Política Pública de Segurança da Informação

## 1 Objetivo

Para que a Segurança da Informação seja completamente eficaz, a **DASA** implementou uma série de controles compostos por políticas, práticas, procedimentos, estruturas organizacionais e tecnologia.

Este documento lista os principais controles utilizados pela **DASA** para atender às necessidades da segurança da informação e cibernética, mitigando as vulnerabilidades a incidentes.

## 2 Introdução

A **DASA**, através de seu departamento de Segurança da Informação e de forma alinhada com os objetivos e requisitos do negócio, estabelece regras e direcionamentos baseados nas normas NBR ISO 27001, 27002 e no NIST *National Institute of Standards and Technology* a serem seguidos e aplicados a pessoas, processos e tecnologia, de forma a proteger as informações da organização, de seus clientes, fornecedores e parceiros de negócios.

## 3 Diretrizes Gerais

Com propósito de auxiliar seus funcionários e partes interessadas a entenderem as suas responsabilidades, para garantir que estejam em conformidade com as diretrizes previamente definidas e com a legislação, foram desenvolvidos alguns documentos para disseminar o conhecimento dos processos e procedimentos de segurança da informação.

Estes documentos estão em ambiente protegido contra alteração, estão disponíveis em local acessível aos colaboradores e são encaminhados às partes interessadas quando solicitado.

## 4 Segurança da Informação no Negócio

A seguir estão relacionados os principais controles utilizados pela **DASA** para proteger as informações, atender às necessidades da segurança cibernética e reduzir a vulnerabilidade a incidentes.

### 4.1 Acesso Lógico e Físico

- Acesso Físico à Salas Restritas

Determina o perímetro e controle de acesso físico necessário para os ambientes que hospedam dispositivos críticos, amostras biológicas e documentos sigilosos.

- Acesso Lógico da Rede de Dados e Sistemas de Informação

Estabelece as diretrizes e requisitos dos controles de acesso de aplicações e sistemas do ambiente de tecnologia.

- Acesso a Rede Wireless Corporativa

Estabelece as diretrizes gerais de instalação, configuração, liberação de acesso e segurança para rede wireless.

- Gerenciar Senhas em Sistemas de Informação

Estabelece as diretrizes de utilização de senhas para auxiliar na segurança dos acessos à rede e aos sistemas informatizados.

- Credenciais de acesso aos Sistemas Informáticos

Estabelece os padrões para os tipos de credenciais, privilégios e nomenclatura das contas dos usuários para acesso aos sistemas informatizados.

- Conceder acesso à internet

Estabelece as diretrizes de acesso à internet pelo tipo de perfil do usuário.

## **4.2 Proteção de dados**

- Classificação, Rotulação e Tratamento da Informação

Estabelece as diretrizes para a classificação, rotulação e tratamento das informações de acordo com sua sensibilidade e criticidade para a organização visando o estabelecimento de níveis adequados de proteção.

- Compartilhamento e armazenamento de informações

Estabelece diretrizes para manter a segurança na troca ou compartilhamento de informações e conhecimento na empresa, e com quaisquer entidades externas. Bem como a criptografia de dados em repouso e em trânsito.

- Enviar, acessar e receber e-mails criptografados

Estabelece as diretrizes para o envio e recebimento de e-mails criptografados.

- Tratar, Gerenciar e Descartar Mídias com Segurança

Estabelece diretriz para tratar, gerenciar e descartar com segurança mídias impressas ou digitais.

- Acesso para Pen-drive

Estabelece as diretrizes de acesso de pen-drive nos equipamentos da empresa pelo tipo de perfil do usuário.

- Prevenção contra vazamento de dados – DLP

Estabelece as diretrizes para que os dados da empresa sejam gerenciados de maneira uniforme em todo o conglomerado, garantindo que estejam classificados como confidenciais e de uso restrito, não sejam compartilhados de maneira equivocada, tendenciosa e/ou maliciosa para usuários não autorizados.

### **4.3 Segurança na rede**

- Uso e Acesso à Internet

Estabelece critérios e padrões para acesso e utilização da internet pelos usuários de rede mantendo a conformidade com a política de segurança da informação e com a legislação vigente.

- Serviço de Mensageria Eletrônica

Estabelece diretrizes para acesso e utilização do serviço de e-mails pelos usuários.

- Aplicar Segurança Perimetral

Estabelece diretrizes para aplicação de políticas de segurança em equipamentos, a fim de proteger e mitigar possíveis vulnerabilidades que podem ser criadas e que permitam um ataque externo (originado pela internet) ou lateral.

### **4.4 Segurança de aplicação**

- Aquisição, Manutenção e Desenvolvimento de Sistemas de Informação

Estabelece os requisitos mínimos para o aquisição, desenvolvimento e manutenção segura de aplicações e aplicativos visando à redução dos riscos associados de segurança dos dados utilizados pelas aplicações ou com a infraestrutura utilizada.

- Desenvolver Código Seguro em Softwares e Sistemas

Estabelece critérios e práticas para desenvolvimento seguro de aplicações, com objetivo de reduzir os riscos e impactos nas áreas de negócios, além de propiciar segurança e confiabilidade ao processo de desenvolvimento / implantação de mudanças e/ou novas versões de sistemas no ambiente de produção.

- Fundamentos e Orientações para Aquisição de Sistemas

Orienta e estabelece estratégia e métodos para aquisição de sistemas com segurança.

- Avaliar, testar e validar a segurança de aplicações desenvolvidas

Estabelece critério para avaliação, teste e validações de segurança de aplicações desenvolvidas em ambiente de homologação da Dasa.

- Criptografia para Sistemas de Informação

Estabelece um procedimento seguro definindo o escopo da aplicação de criptografia com o propósito de garantir um canal seguro para a comunicação das informações.

## 4.5 Segurança de Endpoint

- Prevenção contra Códigos Maliciosos

Estabelece as diretrizes de controle contra Códigos Maliciosos a serem aplicados nos dispositivos gerenciados pela Dasa.

- Uso Aceitável de Recursos de Tecnologia da Informação

Orienta os colaboradores nas práticas para a correta utilização dos ativos e recursos de Tecnologia da Informação.

- Backup

Estabelece as diretrizes para a realização de backup de informações. Arquivos corporativos, sistemas de produção, programas, aplicativos, sistemas operacionais, bancos de dados, scripts, parâmetros de configuração e testes periódicos de restauração de arquivos armazenados nos servidores.

## 4.6 Gestão da cadeia de suprimentos

- Avaliação de fornecedor

Determina os princípios e as regras para seleção, avaliação e reavaliação de provedores externos.

## 4.7 Prevenção

- Gestão de Mudanças

Estabelece as regras gerais do processo de Gerenciamento de Mudanças de TI, que visa assegurar a aplicação de métodos e controles que resultem no mínimo de impactos negativos, oriundos de mudanças mal planejadas e/ou executadas nos ativos.

- Gestão de Vulnerabilidades Técnicas

Estabelece os princípios e as regras para gestão de vulnerabilidades técnicas no ambiente identificando e mapeando risco de ataques e exposição de ativos.

- Gestão de Auditorias de Tecnologia da Informação

Estabelece as regras para a realização de auditorias de segurança da informação visando minimizar os riscos de comprometimento dos sistemas ou das informações. Estas auditorias têm como objetivo avaliar usuários, sistema, seus mecanismos e controles.

- Gestão de Continuidade de Negócios

Estabelece diretrizes a fim de minimizar os impactos negativos causados por quaisquer eventos que possam oferecer risco na continuidade dos negócios da Dasa. Responsável também por definir os papéis e responsabilidades necessários para a execução do processo de gestão.

- Teste de Intrusão

Estabelece diretrizes para execução do teste de Intrusão para buscar e identificar vulnerabilidades de segurança na rede, sistema ou ferramenta.

- Conscientização

Estabelece programa de conscientização e treinamento de segurança para colaboradores e prestadores de serviço.

## **4.8 Centro de Defesa e Operações Cibernéticas**

- Gestão de Incidentes de Segurança da Informação

Estabelece o processo para identificar, notificar e gerenciar os incidentes de segurança da informação e determina as regras para apurar, responsabilizar e aplicar as medidas corretivas e disciplinares em decorrência de violações da política de segurança da informação.

- Gestão de Crises em Tecnologia da Informação

Estabelece o plano de gerenciamento de crise, que engloba procedimentos e instruções a serem adotados quando ocorrer situação de crise ou de ameaça de crise.

- Gestão de Riscos

Este processo determina as diretrizes para identificar, analisar, medir e tratar os riscos de segurança da informação identificados no ambiente.

- Gestão de Consequências em Segurança da Informação

Este processo determina os critérios e procedimentos para a Gestão de Consequências em resultado de incidentes de segurança da informação ocorridos no ambiente, a fim de padronizar as ações administrativas e buscando garantir a confidencialidade, disponibilidade e integridade das informações, sistemas, aplicações e ativos relacionados.

- Gestão de logs e eventos

Este processo gerencia as atividades ou eventos através do gerenciamento e análise de logs detectando atividades não autorizadas ou inadequadas de processamento da informação e atende requisitos legais relevantes aplicáveis para suas atividades de registro e monitoramento.

## **5 Responsabilidades**

### **5.1 Colaboradores e Terceiros**

- Todos colaboradores e prestadores de serviço da **DASA** são responsáveis pelo cumprimento dos princípios de Segurança da Informação e Segurança descritos nas políticas, processos e procedimentos da organização.

## 5.2 Área de Segurança da Informação

- Definir, manter e conscientizar sobre as políticas corporativas de segurança da informação, seus procedimentos e padrões;
- Realizar o planejamento e condução de capacitações periódicas com o objetivo de disseminar a cultura de segurança dentro da empresa, bem como de comunicar as atualizações eventualmente efetuadas nas políticas corporativas de segurança da informação, seus procedimentos e padrões;
- Garantir a concessão de acesso, término ou mudança de direitos de acesso à rede e aplicações críticas de acordo com o perfil do usuário;
- Garantir a melhoria de segurança da informação e segurança cibernética da organização através de projetos e iniciativas;
- Conduzir a Gestão de Incidentes de Segurança da Informação, incluindo as investigações para determinar as causas e os responsáveis, e realizar a comunicação interna dos fatos ocorridos.

## 5.3 Alta direção

A alta direção é a última instância responsável por supervisionar o desenvolvimento e implementação das políticas, procedimentos, controles de segurança da informação e segurança cibernética onde são responsáveis por:

- Aprovar as políticas e procedimentos de segurança da informação e suas mudanças subsequentes;
- Prover um claro direcionamento e apoio para as iniciativas de segurança da informação;
- Promover a cultura em segurança da informação e cibernética na organização;
- Fornecer os recursos necessários para o sistema de gestão de segurança da informação.

## 6 Canal de Comunicação de Segurança da Informação

Caso queira comunicar algum incidente, encaminhe para:

➤ [security@dasa.com.br](mailto:security@dasa.com.br)

## 7 Termos e Definições



<b>Termo</b>	<b>Definição</b>
Alta Direção	Pessoa ou grupo de pessoas que dirige e controla uma organização em seu nível mais alto
Backup	É a cópia de segurança de dados de um dispositivo de armazenamento para outro para que possa ser restaurado em caso da perda dos dados originais
Código Malicioso	É um código de computador nocivo que tem como objetivo criar vulnerabilidades nos ativos da empresa
Conformidade	Cumprimento de um requisito
Criptografia	É a prática de codificar e decodificar dados
Crise	Qualquer evento que ameaça à integridade das pessoas, que gere alto impacto para o negócio e/ou reputação da empresa
Evento	Ocorrência ou mudança em um conjunto específico de circunstâncias que pode ter várias causas
Incidente	Situação que pode representar ou levar à interrupção de negócios, perdas, emergências ou crises
Infraestrutura	Sistema de instalações, equipamentos e serviços necessários para a operação de uma organização
Firewall	Dispositivo de uma rede de computadores que tem o objetivo de aplicar políticas de segurança
Log	Expressão utilizada para descrever o processo de registro de eventos relevantes em um sistema computacional
Melhoria Continua	Atividade recorrente para melhorar o desempenho
NBR ISO 27001	Organização brasileira que estabelece requisitos para o sistema de gestão de segurança da informação de uma organização.
NIST	Agência governamental não regulatória da administração de tecnologia do Departamento de Comércio dos Estados Unidos
Partes interessadas	Pessoa ou organização que pode afetar, ser afetado ou que entendem ser afetados por uma decisão de uma organização
Pen-drive	Dispositivo de armazenamento de dados
Risco	Probabilidade de um evento acontecer, seja ele uma ameaça, quando negativo, ou oportunidade, quando positivo
Rede Wireless	Conhecida também como rede sem fio, é uma infraestrutura das comunicações sem fio que permite a transmissão de dados e informações sem a necessidade de uso de cabos
Teste de Intrusão	É um método que avalia a segurança de um sistema de computador ou de uma rede, simulando um ataque de fonte maliciosa
Vulnerabilidade	É uma fraqueza de um ativo que poderia ser potencialmente explorada por uma ou mais ameaças