| | | |
|---|---|---|
| | **NORMA CORPORATIVA**<br>**Política de Segurança da Informação** | |
| **Área Funcional: Brasil (todos os escritórios)** | **Data de Emissão / Alteração: 13/11/2020** | **Documento: N12** |
| **Proprietário da Política: Grupo de Segurança da Informação** | **Data de Entrada em Vigor: 13/11/2020** | **Versão: 1.0** |

# Sumário

## 1. SOBRE A POLÍTICA

### 1.1. Finalidade:

A presente Política de Segurança da Informação ("Política") tem como finalidade estabelecer diretrizes, princípios e responsabilidades, que descrevam a conduta adequada para o tratamento, controle, proteção, armazenamento e descarte de ativos, dados e informações de propriedade ou sob guarda das empresas do grupo Certsys ("Certsys"), com objetivo de preservar a confidencialidade, integridade, disponibilidade e autenticidade da informação, garantindo assim a conformidade com as melhores práticas de segurança da informação e governança de dados.

### 1.2. Abrangência

Essa política aplica-se a todos os colaboradores, terceiros, fornecedores, parceiros, visitantes e outras partes que tenham relacionamento direto ou indireto com o tratamento de dados sob responsabilidade da Certsys.

### 1.3. Vigência e revisões

Essa política e todos os seus tópicos, passam a vigorar a partir da data de sua publicação e permanecerá vigente por prazo indeterminado, podendo ser revisada a qualquer momento, no caso de alteração na legislação ou se houver alguma alteração das práticas de negócios da Certsys.

### 1.4. Plano de comunicação e treinamento

A Certsys comunicará às partes descritas no item 1.2 desse documento, por meios diversos, todos os tópicos dessa política, bem como suas eventuais alterações. Também se responsabilizará por prover treinamento adequado sempre que necessário.

### 1.5. Princípios de Segurança da Informação

São as bases para as ações e linhas de conduta de Segurança da Informação que atuam como guia para a implementação desta Política os seguintes princípios:

- **Estabelecer a Segurança da Informação em toda Certsys**: A Segurança da Informação deve ser tratada em nível organizacional, de acordo com as diretrizes desta Política e a tomada de decisões que levem em consideração todos os processos críticos de negócio da Certsys.
- **Adotar uma abordagem baseada em riscos**: A Segurança da Informação deve observar a natureza da informação tratada (o tratamento de dados pessoais e dados pessoais sensíveis deve observar as diretrizes estabelecidas na Política de Privacidade) e ser fundamentada em decisões baseadas em riscos como perda da vantagem competitiva, conformidade, de responsabilidade civil, interrupções operacionais, danos à reputação e perdas financeiras.

- **Promover um ambiente positivo de segurança**: A Segurança da Informação é estruturada com base na análise do comportamento humano, observando as crescentes necessidades de todas as partes interessadas, através da conscientização e maturidade dos colaboradores fortalecendo um dos elementos fundamentais para manter o nível apropriado de Segurança.

### 1.6. Definições

- **Colaborador**: Empregados de quaisquer cargos ou posições hierárquicas, estagiários, parceiros, fornecedores e/ou prestadores de serviços;
- **Prestadores de serviços**: Pessoa jurídica ou física que mantenha contrato de prestação de serviços com a Certsys;
- **Informação**: Reunião ou conjunto de dados e conhecimentos resultante do processamento, manipulação e/ou organização de dados;
- **Processamento e/ou Tratamento**: Qualquer manipulação da Informação que de tal forma represente uma modificação (quantitativa ou qualitativa) dos dados e forma de arquivo do conhecimento do sistema (humano ou máquina) que a recebe;
- **Segurança da Informação**: Conjunto de ações e controles que tem como objetivo garantir a preservação dos aspectos de confidencialidade, integridade, disponibilidade, autenticidade e conformidade das informações, contribuindo para o cumprimento dos objetivos estratégicos da companhia;
- **Confidencialidade**: A Informação deve estar disponível e somente ser divulgada a indivíduos, entidades ou processos autorizados;
- **Integridade**: Salvaguarda da exatidão da Informação e dos métodos de Processamento;
- **Disponibilidade**: As pessoas autorizadas devem obter acesso à informação e aos ativos correspondentes sempre que necessário;
- **Conformidade**: Processo de garantia do cumprimento de um requisito, podendo ser obrigações empresariais com as partes interessadas (investidores, empregados, credores, etc.) e com aspectos legais e regulatórios relacionados à administração das empresas, dentro de princípios éticos e de conduta estabelecidos pela Alta Administração da Certsys;
- **Incidente de Segurança da Informação**: Evento decorrente da ação de uma ameaça, que explora uma ou mais vulnerabilidades e que afete algum dos aspectos da segurança da informação: confidencialidade, integridade ou disponibilidade;

- **Risco de Segurança da Informação**: Riscos associados à violação da Confidencialidade e Integridade, bem como da Disponibilidade das informações da companhia nos meios físicos e digitais;
- **Termos de ciência de Segurança**: Declaração onde o Colaborador atesta a ciência sobre todos os termos tratados nessa Política, bem como sobre as normas a ela vinculadas e a sua estrutura de funcionamento.

## 2. DIRETRIZES

### 2.1. Informação é Patrimônio

Toda Informação elaborada, adquirida, manuseada, armazenada, transportada e/ou descartada nas dependências e/ou em ativos das empresas do grupo Certsys é considerada patrimônio da empresa e deve ser utilizada exclusivamente para os interesses corporativos.

### 2.2. A Responsabilidade e o comprometimento deve ser de todos.

Todos os Colaboradores, em qualquer vínculo, função ou nível hierárquico, são responsáveis pela proteção e salvaguarda das Informações de que sejam usuários ou com os quais tenham contato, assim como dos ambientes físicos e computacionais a que tenham acesso, independentemente das medidas de segurança implantadas.

### 2.3. O acesso à Informação deve ser gerenciado

O acesso lógico, o controle de acesso físico e o uso da Informação da Certsys e/ou de terceiros devem ser aprovados, controlados, registrados, armazenados e monitorados, de forma a permitir a adequada execução das tarefas inerentes ao seu cargo ou função.

### 2.4. Incidentes de Segurança da Informação precisam ser tratados

Os incidentes de Segurança da informação devem ser identificados, monitorados, comunicados e devidamente tratados de forma a reduzir riscos no ambiente, evitando interrupção das atividades e não afetar o alcance dos objetivos estratégicos da Certsys.

### 2.5. Os ativos da Certsys e sua utilização podem ser monitorados

A Certsys pode monitorar o acesso e a utilização de seus ativos tecnológicos, como dos ambientes, equipamentos e sistemas da informação, de forma que ações indesejáveis ou não autorizadas sejam detectadas.

### 2.6. Procedimentos que garantam a segurança devem ser aplicados

Todas as atividades realizadas pelos Colaboradores ou outras partes que representem os interesses da Certsys, serão orientadas por procedimentos

específicos que contemplarão a proteção das Informações de acordo com seu grau de classificação.

### 2.7. Riscos devem ser mensurados e mitigados

A Certsys implementará, conforme necessário, métodos de análise de riscos das operações de forma a orientar todos os envolvidos com o Tratamento das Informações, em todos os níveis dos serviços, sobre as formas adequadas de mitigar ao máximo agentes ofensores a quaisquer tópicos referentes a Política.

### 2.8. Dados em nuvem ou fora do país devem ser controlados

A Certsys assegurará que a contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem no país ou no exterior, contemple as políticas, estratégias e estruturas definidas neste Política, necessárias para o adequado gerenciamento dos riscos quanto à terceirização de serviços.

### 2.9. Produtos e serviços devem ser desenvolvidos de forma segura

A Certsys irá avaliar e propor controles que visem oferecer segurança adequada para todos os desenvolvimentos de sistemas, configurações de ambientes ou outras atividades relacionadas a garantia da segurança da informação da Certsys e de seus clientes.

### 2.10. Todo tratamento de dados deve ser seguro

Quaisquer processos de Tratamento de dados sob responsabilidade das Certsys, deve ocorrer de forma a garantir confidencialidade, integridade e disponibilidade das Informações, protegendo os dados e os sistemas da Informação, contra acessos indevidos e alterações não autorizadas.

### 2.11. Comunicar violações da Política

Os Colaboradores devem Comunicar imediatamente à área de Segurança da Informação, bem como ao Compliance da Certsys, qualquer violação desta Política e/ou das demais normas e procedimentos de Segurança da Informação, a fim de sejam aplicadas as medidas de remediação e penalidades previstas.

### 2.12. Todos devem ser orientados adequadamente

A Certsys manterá programa contínuo de treinamento e conscientização sobre a Política e os procedimentos operacionais a ela relacionados. Esse programa será aplicado de acordo com critérios internos, a todos os possíveis envolvidos com o Tratamento de Informações. Também caberá a Certsys, zelar para que todos os envolvidos estejam cientes dos termos desta Política antes de iniciar as atividades na empresa.

### 2.13. A Certsys pode auditar a conformidade com as práticas de Segurança da Informação

A Certsys pode auditar periodicamente as práticas de Segurança da Informação de seus Colaboradores, de forma a avaliar a conformidade das ações de seus Colaboradores em relação ao estabelecido nesta Política e na legislação aplicável.

### 2.14. A melhoria deve ser contínua

A Certsys irá monitorar constantemente o ambiente tecnológico, avaliando e implementando medidas técnicas, ferramentas ou procedimentos de melhoria dos processos relacionadas a disciplina de Segurança da informação.

## 3. PAPÉIS E RESPONSABILIDADES

Aos departamentos e pessoas abaixo indicados serão atribuídas as atividades e obrigações a eles relacionadas, quais sejam:

### 3.1. Administração Certsys

Grupo composto pelos diretores e gerentes da companhia.

- Determinar as diretrizes da Política de Segurança da Informação;
- Reforçar junto as equipes o cumprimento das diretrizes de Segurança da Informação, bem como servir como replicador das boas práticas e controles.;
- Propor ajustes e ferramentas à área de Segurança da Informação que auxilie nos processos de negócio das áreas;
- Informar, à área de Segurança da Informação, sobre o encerramento de contratos em que os prestadores de serviços possuam qualquer tipo de acesso físico ou lógico às informações;
- Contribuir nos processos de revisão periódica de acessos ou em outras situações em que forem acionados pela área de Segurança da Informação;
- Definir os critérios de acesso a ambientes e dados da Certsys ou tratados por ela.

### 3.2. Segurança da Informação

- Definir e documentar a Política de Segurança da Informação;
- Implementar ferramentas e procedimentos relacionados a operacionalização da Segurança da Informação;
- Apoiar a avaliação e a adequação de controles específicos de Segurança da Informação para novos sistemas ou serviços

- Aprovar e revisar periodicamente a Política;
- Monitorar e analisar os alertas relacionados à Segurança das Informações;
- Testar a eficácia dos controles utilizados e relatar possíveis riscos;
- Acompanhar os indicadores cabíveis;
- Acompanhar incidentes de segurança da informação;
- Apresentar assuntos relevantes a diretoria quando cabível;
- Propor controles e melhorias relacionados ao tema segurança da informação;
- Disseminar a cultura de segurança junto as demais áreas da instituição;
- Participar dos projetos em que a área estiver envolvida acompanhando e sugerindo questões relacionadas à segurança da informação;
- Assegurar que acessos sejam concedidos apenas a pessoas devidamente autorizadas e com perfil adequado ao cumprimento dessa política.

### 3.3. Recursos Humanos

- Disponibilizar a Política e as normas de Segurança da Informação para todos os Colaboradores e assegurar que eles estejam cientes das diretrizes, normas e procedimentos internos;
- Informar à área de Segurança da Informação todos os desligamentos, transferências, férias e modificações no quadro de Colaboradores;
- Garantir que os Colaboradores tenham ciência e assinem o Termo de Ciência de Segurança da Informação no processo de integração;
- Promover treinamentos sobre a Política de Segurança da Informação, bem como campanhas de conscientização;
- Assegurar que os pré-requisitos relacionados à Segurança da Informação, são avaliados antes da contratação de um novo recurso.

### 3.4. Tecnologia da Informação

- Realizar as cópias de segurança do ambiente tecnológico;
- Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos nesta política e normas adicionais;
- Planejar, implantar, fornecer e monitorar a capacidade de armazenamento, processamento e transmissão necessárias para ambiente computacional;

- Monitorar o uso dor recursos computacionais utilizados dentro ou fora do ambiente da Certsys;
- Garantir que quaisquer mudanças na infraestrutura de TI, ocorram de maneira coordenada e controlada e que cumpram todos os requisitos dessa política;
- Garantir que quaisquer descartes de dispositivos de armazenamento de dados, aconteçam de forma controlada e jamais exponham informações relacionadas aos negócios da Certsys ou de seus clientes;
- Tratar de acordo com impacto e urgência, todos os incidentes relacionados a política de segurança da informação, relatando o ocorrido à gestão de segurança da informação.

### 3.5. Compliance

- Aplicar as penas previstas na matriz de Penalidades desta Política, após deliberação do Comitê de Compliance em casos em que necessitarem desta ação;
- Avaliar as ações de remediação previstas para os casos de não conformidade a Política de Segurança da Informação e suas normas;
- Receber e analisar os eventos de riscos de segurança da informação, sugerindo ações de remediação.

### 3.6. Colaboradores

- Conhecer e cumprir as normas e orientações estabelecidas nesta Política e demais regulamentos que compõem a Política de Segurança da Informação da Certsys;
- Proteger as Informações contra acessos indevidos, divulgação não autorizados e descarte de forma segura;
- Zelar para que os recursos tecnológicos sejam utilizados de forma eficaz, dentro das finalidades corporativas e de conhecimento pela Certsys;
- Não discutir assuntos confidenciais de trabalho em ambientes públicos ou em áreas expostas (elevadores, taxi e quaisquer outros meios de transporte, restaurantes, etc.) ou com terceiros não autorizados;
- Não compartilhar ou divulgar credenciais de acesso ou equipamentos sem a autorização explicita da área de Segurança da Informação. As senhas são de responsabilidade do usuário, sendo individual e intransferível, sendo substituídas de forma periódica;
- Informar as situações que comprometam a segurança das informações nas unidades organizacionais das empresas do grupo Certsys, através do Canal de Denúncias e Relatos, presente no Código de Ética da Certsys;

- Toda informação criada, modificada no exercício das funções e qualquer informação contida em mensagens do correio eletrônico corporativo deve ser tratada como referente ao negócio da Certsys, não devendo ser considerada como pessoal, particular ou confidencial, mesmo que arquivadas na sua pasta pessoal;
- Garantir que seja conhecida e cumprida a proibição de compartilhamento ou negociação de credencias (ID, senhas, crachás, tokens e similares);
- Garantir que os requisitos de Segurança da Informação constem nas aquisições e/ou implementações tecnológicas;
- Estar atualizado em relação a esta Política e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da área de Segurança da Informação sempre que estiver com dúvidas;
- Solicitar quaisquer acessos ou perfis necessários as atividades profissionais por meio de ferramenta de chamados, contendo as aprovações do gestor imediato;
- Não criar, adquirir ou realizar uso de softwares não homologados e não instalados pela área de Tecnologia da Informação;
- Comunicar a área de Segurança da Informação quaisquer riscos de Segurança da Informação existentes na área de atuação;
- Para trabalhos executados de forma remota, sejam com equipamentos da Certsys ou dos responsáveis pela execução dos serviços, todos os itens dessa Política se aplicam sem restrições ou concessões.

### 3.7. Jurídico

- Requerer a inserção de cláusulas que obriguem o cumprimento desta Política e demais leis, regulamentos e normas aplicáveis aos prestadores de serviços, cujos contratos tenham sua análise requerida ao departamento, assegurando que as informações sejam utilizadas apenas para sua finalidade e preservando sua confidencialidade.

### 3.8. Geral

- As Informações geradas e os ambientes tecnológicos utilizados por seus respectivos usuários são de exclusiva propriedade da Certsys, sendo vedada a sua utilização para fins pessoais ou quaisquer outros, que não os estabelecidos nas políticas normas e procedimentos existentes;
- Todas as disposições legais e demais normas da Certsys, como o Código de Ética, devem ser rigorosamente observadas.

## 4. PROCEDIMENTOS PARA SEGURANÇA CIBERNÉTICA DAS INFORMAÇÕES

A Certsys adota procedimentos e controles para garantir a segurança das Informações sob seu controle, visando um gerenciamento efetivo do monitoramento, Tratamento e resposta aos Incidentes de Segurança da Informação. Tais procedimentos e controles compreendem as seguintes ações, sem prejuízo de outras que se façam necessárias conforme o caso e a critério da Certsys:

### 4.1. Autenticação de Pessoas Autorizadas:

O acesso às Informações e aos ambientes tecnológicos da Certsys somente deve ser permitido às pessoas que tenham necessidade de conhecê-las e/ou acessá-las, observadas as funções desempenhadas dentro da Certsys, levando-se em consideração a segregação de funções conflitantes e a classificação da Informação.

O controle de acesso aos sistemas deve ser formalizado, observada a necessidade de utilização de login e senha ou credencial de acesso individualizado, monitorado e passíveis de bloqueios, restrições e/ou remoções (automatizados e manuais).

A Certsys, por meio do departamento de Recursos Humanos, deve garantir a revisão periódica das autorizações concedidas.

### 4.2. Gestão e Comunicação de Incidentes de Segurança da Informação

A Certsys adota controles para identificar possíveis ataques à Segurança da Informação, através de controles de detecção implementados no ambiente, como filtro de conteúdo, ferramenta de detecção de comportamentos maliciosos, Antivírus, Antispam, entre outros.

Qualquer Incidente de Segurança da Informação deverá ser comunicado à Gestão de Segurança da Informação, que adotará as medidas cabíveis para mitigação e contingenciamento de eventuais danos ocorridos, além de adotar as medidas necessárias à comunicação dos órgãos competentes e possíveis interessados, em especial quando o Incidente envolver dados pessoais e/ou dados pessoais sensíveis, conforme a legislação aplicável.

### 4.3. Controle Contra Software Malicioso

Todos os ativos (computadores, servidores, etc.) que estejam conectados à rede da Certsys ou façam uso de Informações da Certsys, devem, sempre que compatível, ser protegidos com uma solução anti-malware determinada pela área de Segurança da Informação.

### 4.4. Criptografia

Quando necessário e a critério da Certsys, toda solução de criptografia utilizada deverá seguir as regras de Segurança da Informação e os padrões de segurança dos órgãos reguladores.

### 4.5. Acesso à Rede

O acesso a Rede da Certsys somente será realizado por pessoas autenticadas e desde que assegurado que o acesso não comprometerá a segurança de qualquer Informação.

Além disso, todos os computadores/notebooks de propriedade da Certsys e/ou disponibilizados por esta estarão com antivírus devidamente instalados.

A inserção de qualquer nova informação, realizada por meio de dispositivos removíveis só será liberada mediante autorização do gerente ou gestor do setor responsável.

O acesso às estações de trabalho de forma remota só deverá ocorrer mediante autorização do usuário da estação de trabalho.

### 4.6. Cópias de Segurança (Backup)

O processo de execução de backups nas Informações da Certsys ou sob a sua guarda é realizado periodicamente, a critério da Certsys, de forma a evitar ou minimizar a perda de dados diante da ocorrência de incidentes.

### 4.7. Testes

A Certsys realiza testes periódicos para verificar os procedimentos adotados para gestão da Segurança da Informação da companhia.

## 5. COMPROMISSO E PENALIDADES

5.1. Todas as garantias necessárias ao cumprimento desta Política estão estabelecidas formalmente com os Colaboradores das empresas do grupo Certsys, sendo assim, o descumprimento da Política é considerado uma falta grave e poderá acarretar na aplicação de sanções previstas em lei, assim como advertências conforme regulamentos internos e nas disposições contratuais.

5.2. Na hipótese de violação desta Política de Segurança da Informação ou das normas de Segurança da Informação, a Diretoria, com o apoio das áreas de Segurança da Informação, Compliance e Recursos Humanos, determinarão as sanções administrativas que serão aplicadas ao infrator, sendo que:

- Para os prestadores de serviços, o não cumprimento da Política poderá acarretar a rescisão imediata do contrato referente ao serviço violado e outros contratos eventualmente estabelecidos com a Certsys.

## 6. TREINAMENTO, ATUALIZAÇÃO E DIVULGAÇÃO

6.1. Um programa de conscientização, educação e treinamento em Segurança da Informação é disponibilizado, conforme necessidade identificada, para garantia dos objetivos, princípios e diretrizes definidas nesta Política.

6.2. O programa deve ser seguido adequando-se às necessidades e responsabilidades específicas de cada Colaborador das empresas do grupo Certsys.

6.3. Da mesma forma, o conteúdo da Política é amplo e constantemente atualizado e divulgado. A releitura desta Política, mesmo que não seja diretamente solicitada, deve ser feita periodicamente para melhor entendimento.

## 7. REFERÊNCIAS


- ABNT NBR ISO/IEC 27001 Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos.
- ABNT NBR ISO/IEC 27002 Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação.
- ABNT NBR ISO/IEC 27005 – Tecnologia da informação - Técnicas de segurança - Gestão de risco da segurança da informação


HISTÓRICO DE REVISÕES:

| Nº da Versão | Entrada em Vigor | Alteração(ões) | Nº de Registro | Autor |
|---|---|---|---|---|
| 1.0 | 13/11/2020 | Versão Inicial | 1 | Augusto Kiramoto |
| | | | | |
| | | | | |

ESTE DOCUMENTO REVOGA VERSÕES ANTERIORES