PSI-001

Política de Segurança da Informação

Governança Corporativa & Segurança da Informação

hcosta

Dez/24

V 2.2

Histórico de atualização do documento

Versão	Data	Alteração
1.0	30/09/2020	Emissão do documento.
1.1	23/09/2021	Revisão do documento.
1.2	27/09/2022	Revisão do documento.
2.0	11/09/2023	Revisão geral das políticas e normas.
2.1	14/02/2024	Revisão do documento.
2.2	05/12/2024	Revisão geral das políticas e normas.

Sumário

1. Introdução

Esta política tem como premissa definir estratégias que definem as regras para uso e proteção da informação companhia, com o intuito de resguardar tanto os princípios básicos (Conformidade, Integridade, Disponibilidade) como seus derivados (Autenticidade, não-Repúdio, propriedade).

O compromisso com a proteção dos ativos de informação de sua propriedade e sua guarda no que tange a companhia, com base nas normas técnicas ABNT, NBR e ISO/IEC 27001/27002 e NIST Cybersecurity Framework (CSF 2.0).

A segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional, governança e funções de softwares e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados, criticados e melhorados quando necessário para assegurar que os objetos do negócio e a segurança da informação da companhia sejam atendidos. A função "Governar", reconhece que a abordagem organizacional à segurança cibernética deve corresponder à estratégia do negócio em torno de seis áreas-chave: identificação, proteção, detecção, resposta, recuperação e governança.

2. Objetivo

Definir as diretrizes de segurança da informação para que todos os usuários e sistemas da companhia sigam tais práticas.

3. Conceito e Definições

PSI: Política de Segurança da Informação.

SI: Segurança da Informação.

GSI: Gestão de Segurança da Informação.

Segurança Cibernética (Cybersecurity): Conjunto de tecnologias, processos e práticas elaboradas para proteger ambientes de redes, computadores, sistemas e dados de ataques, danos ou acesso não autorizado, visa proteger somente assuntos relacionados ao digital.

LGPD: Lei Geral de Proteção de Dados.

Ativo: Hardware, software, dados ou qualquer elemento que represente valor para a companhia.

Vulnerabilidade: Refere-se a uma situação de risco, fragilidade aos efeitos de uma ação de ataque.

ISO: International Organization For Standardization, que tem como objetivo aprovar e promover o desenvolvimento de normas e políticas internacionais, testes e certificação de empresa e produtos. Tem como princípio geral a adoção pela organização de um conjunto de requisitos, processos e controles com os objetivos de mitigarem e gerirem adequadamente com o risco da companhia.

SGSI: Sistema de Gestão de Segurança da Informação.

SOC: *Security Operation Center*, sigla para centro de operações de segurança em tecnologia da informação, plataforma digital onde é registrada os imprevistos ou problemas que ameaçam o sistema de segurança da informação.

NIST: National Institute of Standards and Technology, sigla para Instituto Nacional de Padrões e Tecnologia, o NIST é responsável por desenvolver e promover padrões e diretrizes para uma ampla gama de áreas, incluindo tecnologia, ciência, engenharia e segurança da informação.

4. Abrangência

Esta política de Segurança da Informação tem abrangência sobre todas as unidades da companhia. Todas as regras aqui estabelecidas devem ser aplicadas aos colaboradores, estagiários, aprendizes, líderes, executivos, diretores, sócios e conselho administrativo de que agora em diante todos são denominados usuários, no que se refere a proteção da informação e uso de recursos tecnológicos da companhia e para os prestadores de serviços, parceiros e fornecedores, caso estes realizem qualquer forma de acesso ou manipulação das informações ou utilizem recursos tecnológicos da companhia.

5. Diretrizes

Para endereçar todo o esforço e manutenção necessária para a segurança da informação, a companhia estabelece as seguintes diretrizes:

I. Uma estrutura de gestão da segurança da informação será estabelecida e mantida com apoio da alta administração, através de um Sistema de Gestão de Segurança da Informação (SGSI).

II. A informação deverá ser utilizada com responsabilidade, de modo ético e seguro por todos, em benefício exclusivo dos negócios coorporativos.

III. A companhia reserva-se o direito de monitorar e registrar todo o uso das informações geradas, armazenadas ou veiculadas na companhia.
Todos os ativos de informação devem ser devidamente identificados, classificados e monitorados.

IV. A identificação de cada colaborador da companhia é única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas.

V. A utilização de senhas e dados são exclusivamente individuais, é estritamente proibido o compartilhamento destas e o não cumprimento desta norma será passível de punição.

VI. Os riscos identificados deverão ser analisados, classificados e apresentados ao Comitê de Gestão da Segurança da Informação (CGSI), que deliberará sobre o tratamento adequado para tais.

VII. A companhia, segue, registra e mantêm atualizadas as leis que regulamentam suas atividades, bem como dos aspectos de propriedade intelectual.

VIII. Quando razões tecnológicas ou determinações superiores tornarem impossível a aplicação dos requisitos previstos nesta política o solicitante deverá documenta-las com todos as informações do fato por um documento escrito e comunica-las imediatamente à área de segurança da informação através do endereço de e-mail soc@hcosta.com.br e registrar um chamado no sistema de ITSM para que possibilite a adoção de medidas alternativas que minimizem os riscos, bem como um plano de ação para corrigi-los, monitorá-los ou eliminá-los.

6. Controle

Para manter um nível satisfatório de segurança constitui-se o Comitê de Gestão de Segurança da Informação (CGSI) que adotará as diretrizes apresentadas.

I. O controle de acesso dos colaboradores ou terceiros aos ativos de informação deve ser devidamente controlado e aprovado pelo responsável pela informação (gerência ou diretoria), a qual o acesso permitirá a manipulação, quer seja para simples consulta ou para alteração.

II. O uso do e-mail sob domínios de propriedade da companhia será permitido para colaboradores e para terceiros somente quando for necessário, e por tempo determinado pela gerência da área solicitante mediante a assinatura do termo de responsabilidade. Este tempo poderá ser prorrogado mediante nova solicitação da gerência da área.

III. Copias de segurança (backup) devem ser realizadas através de mídias especificas para as informações que são consideradas vitais para os sistemas e para a retomada das atividades das áreas em casos de indisponibilidade.

IV. Regras para o desenvolvimento seguro de sistemas e softwares devem ser estabelecidas e aplicadas para desenvolvimentos realizados dentro da organização.

V. Terceiros, consultores e fornecedores deverão ter acessos a sistemas legados da empresa somente quando acompanhado por recurso interno ou via sistema de gerenciador de acesso administrado pela companhia.

VI. A concessão de acesso remoto para os colaboradores deve ser autorizada formalmente e solicitada ao departamento de tecnologia da informação e pela gerência da área solicitante, ocasião em que deverá ser indicado o tipo de acesso, permissão e as informações a serem acessadas, sendo de responsabilidade do solicitante dos atos oriundos em todo período de acesso.

VII. Dispositivo móvel entende-se qualquer equipamento eletrônico com atribuições de mobilidade no manuseio da informação e destina-se ao uso para realização das atividades de trabalho e para comunicação com a empresa, fornecedores ou clientes, devendo ser utilizado somente para esta finalidade, podendo haver especificações e/ou restrições de acordo com normativas contratuais de nossos clientes contratantes.

VIII. As informações devem ser classificadas e manuseadas de acordo com a "[PSI-001-NO0003] HCosta - Norma de Classificação da Informação" selecionando sempre um rótulo como pública, interna, restrita e confidencial que deverão ser tratadas, armazenadas e descartadas de maneira correta para garantir os aspectos de segurança da informação no negócio da companhia e nas informações dos seus clientes.

IX. As responsabilidades de todos quanto a segurança da informação deve ser definida, seguindo requisitos mínimos de boa conduta e ética.

X. Os ativos tangíveis e intangíveis de informação devem ser identificados de forma individual, inventariados, protegidos e monitorados de acessos indevidos. As mídias devem ser gerenciadas de forma adequada, conforme os requisitos de segurança da informação.

XI. Um conjunto de regras para garantir a padronização das técnicas criptográficas deve ser estabelecido, incluindo a aplicação adequada das mesmas e as responsabilidades para manter a segurança no transporte ou armazenamento das informações independente do meio utilizado. Quanto à transmissão de informações, este recurso é utilizado para garantir a privacidade na comunicação dos dados da companhia e de seus clientes.

XII. Um processo de gestão de mudanças deve estar em vigor para garantir que controles e modificações nos sistemas ou recursos de processamento da informação sejam realizados com planejamento, a fim de não ocasionar falhas operacionais ou de segurança no ambiente produtivo da companhia.

XIII. Medidas de segurança devem ser adotadas para garantir a proteção das informações de maneira eficaz, reduzindo os riscos de acesso não autorizado, perda ou dano à informação.

XIV. Os riscos devem ser identificados por meio de um processo estabelecido para análise de vulnerabilidades, ameaças e impactos sobre os processos nos aspectos de segurança da informação (Confidencialidade, Integridade e Disponibilidade).

XV. Todos os incidentes que afetem a segurança da informação devem ser reportados à área de segurança da informação através formalização para o e-mail soc@hcosta.com.br e abertura de chamado no sistema de ITSM utilizado na companhia. Estes analisarão o incidente e tomarão as ações devidas, repassando a tratativa às áreas responsáveis.

XVI. Todos os incidentes de segurança devem ser reportados para a área de segurança da informação, para que sejam analisados, avaliados e tratados pela área responsável.

XVII. As responsabilidades do departamento de tecnologia da informação e suas subdivisões devem ser estabelecidas, bem como as restrições do uso de ativos tecnológicos da companhia.

XVIII. Devem ser definidas regras para garantir que não ocorram violações jurídicas, regulamentares ou contratuais nos requisitos de segurança da informação na companhia.

XIX. Devem ser estipuladas diretrizes para garantir que, o acesso físico as instalações onde os ativos de tecnologia da informação e as informações críticas a continuidade do negócio esteja armazenada, seja controlado de forma a garantir a sua disponibilidade, integridade e confidencialidade.

7. Conformidade e Auditoria

A companhia monitora e registra todo o uso das informações geradas, armazenadas ou veiculadas na companhia. Para tanto a organização mantem controles apropriados e trilhas de auditoria ou registros de atividades em todos os pontos e sistemas que a empresa julgou necessário para reduzir os riscos, conforme os itens listados abaixo.

I. Implantar outros sistemas de monitoramento de acesso às estações de trabalho, servidores internos e externos, correio eletrônicos, navegação, internet, dispositivos moveis ou wireless e outros componentes da rede. A informação gerada por estes sistemas de monitoramento poderá ser usada para identificar usuários e respectivos acessos efetuados.

II. Inspecionar qualquer arquivo que esteja na rede, no disco local de estação ou qualquer ambiente, visando assegurar o rígido cumprimento desta política de segurança da informação.

III. Instalar outros sistemas de proteção e detecção de invasão para prevenir a segurança das informações e dos perímetros de acesso, levando em consideração normas especificas e contratual de nossos clientes e contratantes.

IV. Instalar câmeras nas instalações físicas, levando em consideração normas especificas e contratual de nossos clientes contratantes.

8. Penalidades

I. Para toda e qualquer infração à Política de Segurança da Informação (PSI), às normas de segurança da informação e ao código de ética e conduta, deverá ser aberto um incidente de segurança da informação, tratado de acordo com o plano de tratamento de incidentes de segurança da informação e informado ao Comitê de Gestão de Segurança da Informação (CGSI) e, por conseguinte, apurada através de procedimentos internos conduzidos pelas áreas de compliance e segurança da informação da companhia.

II. Caso o Comitê de Gestão de Segurança da Informação (CGSI) Julgue cabível, o colaborador envolvido poderá enquanto durar o processo de apuração interna, ser afastado da função ou suspenso.

III. Ao colaborador suspeito de cometer violações à política e norma de segurança da informação, deverá ser assegurado tratamento justo e correto, sendo que toda e qualquer medida resultante de sua infração deverá ser aplicada com proporcionalidade à ocorrência com base no código de ética e conduta, termo de confidencialidade e aceite da Política de Segurança da Informação (PSI) e as legislações vigentes na companhia.

IV. A companhia exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, reservando-se o direito de punir os infratores, analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios e adotar as medidas legais cabíveis.

V. O não cumprimento dessa política de segurança da informação implica em falta grave e poderá resultar em ações como advertência formal, suspensão, rescisão do contrato de trabalho, outra ação disciplinar e/ou processo civil ou criminal.

9. Princípios

Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para organização ou seus clientes. Ela pode estar guardada para uso restrito ou exposta ao cliente para consulta ou manuseio. Pode estar impressa, escrita, pode ser falada, transmitidas por e-mails ou outros meios eletrônicos.

Independente da forma apresentada ou o meio do qual a informação é compartilhada ou armazenada, a informação é o maior ativo da companhia e de seus clientes e, por isso, essencial ao negócio. Uma vez que se é trabalhado com informações de terceiros (clientes), além de prover segurança para a própria operação, é exigido também o cumprimento contratual de segurança destas informações, sendo a companhia responsável por qualquer incidente ou divulgação intencional ou arbitrária delas. Por esses motivos, a informação deverá ser devidamente protegida e atualizada de modo ético e seguro, garantindo confiabilidade através da proteção conforme imagem abaixo:

10. Divulgação

A política de segurança da informação deve ser de conhecimento de todos e estar disponível em locais de acesso dos colaboradores e protegida contra alterações, devendo ser divulgada da seguinte forma.

I. Por meios de canal digital, através da intranet corporativa.
II. Em campanhas de segurança da informação.
III. Reuniões e eventos da companhia.
IV. Por canais do RH e mural de recados.

11. Responsabilidades

A alta administração da companhia é responsável pela viabilização das condições necessárias para a devida aplicabilidade desta política de segurança da informação, o Comitê de Gestão de Segurança da Informação (CGSI), formado por representantes das principais áreas da empresa, os quais compõem o comitê de integridade, é responsável pela atualização desta política.

Todos os colaboradores, temporários, aprendizes, estagiários, lideres, executivos, diretores, sócios, além de prestadores de serviços, parceiros e fornecedores que realizem qualquer forma de acesso ou manipulação das informações ou utilizem recursos tecnológicos da companhia devem aderir formalmente ao "Termo de confidencialidade e ciência da política de segurança da informação" comprometendo-se agir de acordo com a política e normas de segurança da informação, além do código de ética e conduta da companhia.

12. Vínculos

I. Política de Gestão de Riscos
II. Política de Continuidade de Negócio
III. Política de Saúde e Segurança no Trabalho
IV. Política do Programa 5S
V. Código de Conduta e Ética da HCosta
VI. Aviso de Privacidade para Colaboradores
VII. Procedimento de Gestão de Acessos
VIII. Procedimento de Resposta a Incidentes de SI
IX. Procedimento de Monitoramento de Segurança Física
X. Procedimento de Perímetros de Segurança Física
XI. Procedimento de Gerenciamento de Crise
XII. Procedimento de Gerenciamento de Ativos
XIII. Procedimento de Auditoria Interna
XIV. Procedimento de Acessos e Privilégios
XV. Procedimento de Gerenciamento de Mudanças
XVI. Norma de Classificação de Informações
XVII. Norma ABNT NBR ISO IEC 27001 / 27002
XVIII. NIST Cybersecurity Framework (CSF 2.0)

13. Validação e Aprovação

O Comitê de Gestão de Segurança da Informação (CGSI) da companhia é responsável pela validação e aprovação das diretrizes deste documento.

14. Informações do documento

Repositório de documentos	Responsável pelo Documento	Classificação da Informação
\\fileserver\Tecnologia\GOVERNANCA\POLITICA	Governança Corporativa & Segurança da Informação	Confidencial

15. Revisão

A revisão deste documento deve ocorrer em intervalos planejados, ou após qualquer alteração significativa dos processos relacionados. Esta norma entrará em vigor na data de sua divulgação, revogando e substituindo qualquer comunicação anterior sobre o assunto.

Situações em que o processo será revisado:

I. Em no máximo 1 (um) ano;
II. Nos momentos em que a companhia julgar necessário;
III. Após ocorrência de algum evento ou mudança significativa nos ativos de informação, nas atividades ou em algum de seus componentes.

16. Aprovação

Nome do Aprovador	Cargo do Aprovador	Data	Assinatura
Luciana Pardo Razeira	Diretora Executiva		
Alan Colombo Cosin	Superintendente de Tecnologia e Planejamento		