Política
de Segurança da Informação

Dep. de Seg. da Informação

hcosta

Histórico de atualização do documento

Versão	Data	Alteração
1.0	10/12/2016	Emissão
1.1	20/12/2017	Revisão 1
1.2	15/01/2018	Revisão 2
1.3	10/12/2018	Revisão 3
1.4	07/08/2019	Revisão 4
1.5	30/03/2020	Revisão 5
1.6	05/05/2021	Revisão 6
1.7	04/06/2022	Revisão 7
1.8	04/07/2023	Revisão 8

Sumário

1 Objetivo

Garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade da informação necessária para a realização do negócio da Advocacia Neves Costa – HCosta, definindo também diretrizes de Segurança da Informação praticadas pela Empresa e seus colaboradores.

2 Introdução

A presente política de segurança da informação – PSI está baseada nas recomendações da norma ABNT NBR ISO/IEC 27002:2013, reconhecida mundialmente como um código de prática para a gestão da segurança da informação. A informação é o ativo mais valioso da HCosta, por isso necessita ser adequadamente protegida.

"Segurança da Informação é a proteção da informação de vários tipos de ameaças e vários níveis para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio" (ABNT NBR ISO/IEC 17799:2005).

2.1 Glossário

PSI: Política de Segurança da Informação, inclui todas as políticas envolvendo a comunicação da empresa.

SI: segurança da informação.

GSI: departamento de gestão de segurança da informação.

CGC: comitê gestor de crise.

Segurança Cibernética: Conjunto de tecnologias, processos e práticas projetados para proteger 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 pessoais.

Ativo: Hardware, software ou informação, qualquer elemento que represente valor para a organização.

Pentest: O teste de intrusão, também traduzido como "teste de penetração", é um método que avalia a segurança de um sistema de computador ou de uma rede, simulando um ataque de uma fonte maliciosa.

Vulnerabilidade: Refere-se à incapacidade de resistir aos efeitos de uma ação hostil.

3 Abrangência

Este documento consiste na Política de Segurança da Informação(PSI) da HCosta, que deve ser mantida como uma medida de boas práticas, estabelecendo diretrizes para a proteção de ativos e definição de responsabilidades. A PSI deve ser adotada, cumprida e aplicada em todas as áreas da companhia em conjunto com nosso código de conduta e ética, também parte integrante deste documento. Esta versão pode ser alterada a qualquer momento, suas alterações devem ser aprovadas pela diretoria e veiculada em nossos canais de comunicação. As informações desta Política são revisadas e atualizadas ao mínimo uma vez ao ano, ou conforme as demandas de negócio e ou legais se tornem necessárias.

4 Escopo da área de tecnologia e segurança da informação

Garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade da informação necessária para a realização do negócio da Empresa, ser o gestor do processo de segurança digital, protegendo assim as informações da organização, catalisando, coordenando, desenvolvendo e/ou implementando ações para esta finalidade.

5 Dever dos colaboradores da HCosta

Considerar a informação como sendo um bem da organização, um dos recursos críticos para a realização do negócio, que possui grande valor para a HCosta e deve sempre ser tratada profissionalmente, bem como se manter alinhado ao nosso código de conduta e ética este uma das políticas Internas da HCosta.

6 Classificação da Informação

É de responsabilidade do gestor de cada área estabelecer a rotulagem da informação que o seu setor manipula, com critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias) gerada por sua área de acordo com a lista abaixo:

- Pública
- Interna
- Confidencial
- Restrita

Conceitos:

6.1 **Pública:** É toda informação que pode ser acessada por usuários da organização, clientes, fornecedores, prestadores de serviços e público em geral, cuja divulgação externa não compromete a empresa. Exemplos de Informação pública: agenda de negócios, participação em eventos política de Segurança da Informação.

6.2 **Interna:** São as informações disponíveis aos colaboradores da HCosta, para a execução de suas tarefas rotineiras, não se destinando ao público externo, pois seu grau de confidencialidade assim o define. Exemplos de informação Interna: memorandos, políticas Internas, avisos e campanhas internas.

6.3 **Confidencial:** São informações que podem ser acessadas por um número mais restrito de colaboradores e parceiros da organização. Sua publicação não autorizada pode violar leis vigentes (Ex: LGPD), acordos de confidencialidade, podendo causar impacto (financeiro, de imagem ou operacional) ao negócio da organização ou ao negócio do parceiro. Exemplos de informação confidencial: dados de funcionários ou pessoas físicas identificáveis, processos judiciais.

6.4 **Restrita:** É toda informação que pode ser acessada somente por usuários da organização explicitamente indicados pelo nome ou área a que pertencem, em geral, associadas ao interesse estratégico da empresa. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização. Todo gerente deve orientar seus subordinados que tenham acesso a esse tipo de informação, por necessidade da função exercida, a não circularem informações e/ou mídias consideradas confidenciais e/ou restritas, como também não deixar relatórios nas impressoras, e mídias em locais de fácil acesso, tendo sempre em mente o conceito "mesa limpa", ou seja, ao terminar o trabalho não deixar nenhum relatório e/ou mídia confidencial e/ou restrito sobre suas mesas.

Exemplos de informação restrita: Atas de reuniões da governança, indicadores e estatísticas dos processos de negócio, resultados de auditorias Internas.

Processo

O processo de classificação segue a seguinte linha:

Inventário do Ativo (Informação).	→	Classificação da Informação.	→	Rotulagem.	→	Utilização dos Ativos.

- Todo documento não classificado é considerado pela HCosta informação pública.

7 Gestão da segurança da informação

Sendo a informação o ativo mais valioso da corporação, cabe a esta promover orientações aos seus colaboradores e treinamentos em Segurança da Informação, pois ela precisa transitar no cotidiano das atividades da empresa, tal qual a responsabilidade do ponto eletrônico, pois só os controles digitais não são suficientes para manter um ambiente seguro, todos os colaboradores precisam estar envolvidos e participativos no tema em suas atividades rotineiras.

cabe ao setor de gestão de segurança da informação:

- Montar subcomitê de segurança da informação envolvendo outras lideranças da empresa conforme estratégia adotada junto a diretoria;
- Propor melhorias e ajustes na PSI;
- Estar sempre alinhado junto ao CGC;
- Análise de investimentos em S.I. com o intuito de minimizar os riscos operacionais;
- Apuração, análise e toda governança dos incidentes em segurança da informação;
- Apoio na gestão dos processos em tecnologia da Informação
- Classificar e reclassificar junto com o subcomitê de segurança da Informação os níveis de acesso sempre que necessário.

8 Dados pessoais e LGPD

A HCosta tem o compromisso em não acumular ou manter dados pessoais sensíveis a LGPD além daqueles relevantes na condução do seu negócio e que por razões legais a empresa possui o direito ou obrigação de mantê- los, bem como operá-los e ou controlá-los. Todos os dados armazenados são considerados dados confidenciais e quer estejam em repouso ou não são protegidos por criptografia conforme nossas políticas internas. Todo fluxo e manipulação desses dados, quer seja de colaboradores internos ou não, são operados e ou controlados mediante a termos de confidencialidade e não declaração, geralmente disposto em contratos baseados na lei vigente do país.

A empresa possui controles e ferramentas para o monitoramento dos dados pessoais em concordância com a lei geral de proteção de dados pessoais.

9 Segurança cibernética

A Gerência de T.I. da HCosta, é responsável por estabelecer as políticas, procedimentos e controles em segurança Digital para manter a integridade, disponibilidade e a confidencialidade das informações contidas nos ambientes corporativos, com o intuito de reduzir impactos e possíveis vulnerabilidades no Ambiente, para evitar a ocorrência de incidentes de Segurança da Informação. Possui como diretrizes básicas:

- Gestão dos acessos através do monitoramento do processo contido na política de acesso e acesso remoto;
- Assegurar a confidencialidade, integridade e disponibilidade das informações da organização;
- Garantir que os ativos(dados e informações) sejam utilizados apenas para as finalidades aprovadas pela organização, com monitoração, rastreabilidade e auditoria;
- Gestão e detecção de vulnerabilidades;
- Pentests semestrais;

- Prevenção a ameaças e ataques cibernéticos, bem como resposta a ataques cibernéticos;
- Melhoria contínua dos processos e recursos necessários para segurança da informação e cibernética;

10 Responsabilidade das lideranças

Os gestores das áreas e departamentos da HCosta são responsáveis pelas definições dos direitos de acesso de seus subordinados aos sistemas de informações da companhia, cabendo a eles verificar se os mesmos estão acessando exatamente as rotinas compatíveis com as suas respectivas funções. a empresa possui auditoria das ações dos usuários em seus sistemas.
A diretoria da HCosta é a responsável em viabilizar as condições necessárias para a aplicabilidade das diretrizes desta política de segurança da informação.
A área de gestão de segurança da informação é responsável pela atualização das políticas que compõe este documento.
O comitê de gestão de crise é o responsável em fomentar a área de Gestão de segurança da informação com as demandas e compliances de negócio.

11 Sanções

O não cumprimento desta política de segurança da informação implica em falta grave e poderá resultar nas seguintes ações: advertência formal, suspensão, rescisão do contrato de trabalho, outra ação disciplinar e/ou processo civil ou criminal. havendo qualquer omissão de qualquer conduta que possa comprometer em qualquer nível a empresa ou a lealdade das relações para com a HCosta implicará nas mesmas sanções do descumprimento da nossa política de segurança da informação.

12 Gestão dos processos em tecnologia da informação

Uso de antivírus: Todas as estações de trabalho, dispositivos móveis e servidores devem ter a solução corporativa do antivírus instalado. A atualização do antivírus é automática, conforme as rotinas estabelecidas do servidor que provê esse serviço. O usuário não tem permissão para desabilitar o programa antivírus instalado nas estações de trabalho ou notebooks, no entanto caso isso ocorra, o colaborador está sujeito a penalidades descritas no nosso código de conduta e ética.

Uso do correio eletrônico (e-mail) corporativo: O correio eletrônico fornecido pela HCosta é um instrumento de comunicação interna e externa para a realização do negócio da empresa. As mensagens devem ser escritas em linguagem profissional, não devem comprometer a imagem da empresa, não podem ser contrárias à legislação vigente e nem aos princípios éticos da HCosta conforme explicitado em nosso código de conduta e ética.

Novos sistemas, apps e equipamentos: O setor de T.I. é responsável pela aplicação da política da HCosta em relação à definição de compra e substituição de “software” e “hardware”. Qualquer necessidade de novos apps dentro da corporação ou de novos equipamentos, será validada e homologada pela área de T.I. com aprovação da Gerência. Não é permitido a compra ou o desenvolvimento de "softwares" ou "hardwares" diretamente pelos usuários.
Internet: O acesso à Internet é autorizado para aos usuários conforme seu perfil, são acessos aos conteúdos que necessitarem para o desenvolvimento de suas atividades na Empresa. Demais conteúdos são bloqueados por padrão. Há política específica a este controle.

Sistemas de telecomunicações: O controle de uso, a concessão de permissões e a aplicação de restrições em relação aos ramais telefônicos da HCosta, assim como, o uso de eventuais ramais virtuais instalados nos computadores de responsabilidade do setor de Suporte. Todas as ligações são gravadas. A área de qualidade efetua auditorias constantes com feedback as gerências da HCosta.

Programas e aplicativos: A HCosta respeita direitos autorais dos programas que utiliza, reconhece que deve pagar o justo valor por eles, é terminantemente proibido o uso de programas ilegais (Sem licenciamento) na Corporação.

Backup: Todos os dados da HCosta são protegidos através de rotinas sistemáticas de backup. Cópias de segurança do sistema integrado e servidores de rede que são de responsabilidade do setor Interno, são executadas diariamente e possuem política específica a este fim.

Segurança e integridade dos bancos de dados: O gerenciamento do(s) banco(s) de dados é responsabilidade exclusiva do Setor de T.I., que visa proteger usando as tecnologias digitais disponíveis, mantendo integro e disponível ao negócio com as devidas configurações necessárias ao Funcionamento Seguro.

Admissão e desligamento de colaboradores: O departamento pessoal informa ao setor de suporte, toda e qualquer movimentação de funcionários, temporários, estagiários ou prestadores de serviços a área de T.I., para que os mesmos possam ser ativados ou desativados no sistema da companhia e terem os privilégios de perfil atribuído ao respectivo login de acordo com a função que este exercerá dentro da HCosta. O novo colaborador, deverá nortear suas ações em consoante com esta PSI e nosso código de conduta e ética.

Propriedade intelectual: São de propriedade da HCosta, todos os "designs", criações ou procedimentos desenvolvidos por qualquer funcionário durante o curso de seu vínculo empregatício com a empresa. **Política de senhas:** A senha do colaborador é pessoal e intransferível que protege a identidade do colaborador. O uso de dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no código penal brasileiro(art. 307 – falsa Identidade). A HCosta possui política de senha e esta é aplicada a todos os colaboradores.

Uso de dispositivos, notebooks e estações de trabalho: Tais equipamentos devem permanecer o maior tempo possível disponível aos Colaboradores, para que estes possam exercer suas funções em sua plenitude. Os equipamentos devem conter, antivírus e somente as aplicações homologadas pela Empresa. Em nosso código de conduta e ética são descritos os compromissos e responsabilidades dos Colaboradores no tocante a todos os Ativos da Empresa. Caracteriza-se por dispositivo móvel qualquer equipamento eletrônico com atribuições de mobilidade, seja de propriedade da HCosta ou particular com prévia aprovação e permissão pela gerência de T.I., como: notebooks, smartphones e pen drives. Todos deverão estar de acordo com nossa política de Acesso e Acesso Remoto.

Utilização da rede: O acesso a rede interna da empresa é controlado, estações ou dispositivos não autorizados, não conseguirão fazer uso dos recursos de T.I. da Empresa. Para visitantes temos uma rede completamente apartada, com Internet disponível e monitorada. O acesso a rede Interna por dispositivos que não pertencem a HCosta, passa por aprovação da gerência de T.I. e homologação pela equipe de suporte, dispositivos sem antivírus não terão permissão para trafegar na rede Interna e todas suas ações serão monitoradas na rede. A rede de computadores da empresa é totalmente segmentada, não há exceções.

13 Disposições Gerais

As dúvidas decorrentes de fatos não descritos nesta política de segurança da Informação deverão ser encaminhadas à governança para avaliação e decisão. Esta PSI entra em vigor a partir da data de publicação e pode ser alterada a qualquer tempo, por decisão da governança, mediante o surgimento de fatos relevantes que apareçam ou não tenham sido contemplados neste documento.
Compõem essa política de segurança da Informação, como documentos complementares os seguintes itens:

- Política de Responsabilidades do corpo Diretor da Empresa
- Código de Conduta e Ética
- Política de Papéis e Responsabilidades

- Política de Antivírus
- Política de Acesso e Acesso Remoto
- Política de Senhas
- Política de Auditorias Internas
- Política de Backup e Restore
- Política de Gestão de Riscos
- Política de Resposta a Incidentes
- Política de Segurança Cibernética
- Política de Privacidade de Dados
- Política de Retenção de Dados
- Política de Transferência de Dados
- Política de Resposta a Solicitações ref. a LGPD
- Plano de Continuidade dos Negócios