Política de segurança da informação

Departamento de Segurança da informação

Histórico de atualização do documento

Versão	Data	Alteração
1.0	10/12/2016	Emissão Rev.1.
1.1	20/12/2017	Emissão Rev.2.
1.2	15/01/2018	Emissão Rev.3.
1.3	10/12/2018	Emissão Rev.4.
1.4	07/08/2019	Emissão Rev.5.
1.5	30/03/2020	Emissão Rev.6.
1.6	05/05/2021	Emissão Rev.7.

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 um 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 Politicas 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 SI 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 TI 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 área 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 GSI 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 TI 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 TI 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 politica 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 Apps: 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 Ti, 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 setor de Recrutamento e Seleção informa ao setor de Suporte, toda e qualquer movimentação de funcionários, temporários, estagiários ou prestadores de Serviços a área de TI, 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 CI, 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 politica 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 os App's homologados 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 TI, como: notebooks, smartphones e pendrives. 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 TI 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, passam por aprovação da Gerencia de TI 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:

- 002 - Política de Responsabilidades do corpo Diretor da Empresa
- 003-Código de Conduta e Ética
- 005 - Política de Papéis e Responsabilidades
- 010 - Política de Antivírus
- 021 - Política de Acesso e Acesso Remoto
- 024 - Política de Senhas
- 035 - Política de Auditorias Internas
- 049 - Política de Backup e Restore
- 092 - Política de Gestão de Riscos
- 093 - Política de Resposta a Incidentes
- 094 - Política de Segurança Cibernética
- 095 - Política de Privacidade de Dados
- 096 - Política de Retenção de Dados
- 097 - Política de Transferência de Dados
- 098 - Política de Resposta a Solicitações ref. a LGPD
- 099 – Plano de Continuidade dos Negócios

SERPRO
Assinado digitalmente por:
FLAVIO NEVES COSTA
CPF:/CNPJ
17044613837
Assinado em:
17/08/2021
Sua autenticidade pode ser confirmada no endereço :
<http://www.serpro.gov.br/assinador-digital>