1 INTRODUÇÃO

A adoção de procedimentos que garantam a Segurança da Informação é prioridade permanente da Hostweb e seus colaboradores, de forma que se possa evitar ou suprimir incidentes que venham a prejudicar os serviços prestados pela Hostweb ou ocasionar prejuízo para a própria empresa ou a terceiros.

A Política de Segurança da Informação forma a base para o estabelecimento do Sistema de Gestão de Segurança da Informação da Hostweb, abrangendo todos os seus ativos, sistemas e ambientes de Informação, bem como padrões e procedimentos de segurança da Hostweb.

De modo geral, esta política resume os princípios de Segurança da Informação que a Hostweb reconhece como sendo importantes, devendo estar presentes no cotidiano de suas atividades. Assim, visa assegurar a confidencialidade, disponibilidade, integridade, autenticidade e não-repúdio do processamento, transferência, manuseio e armazenamento das informações da Hostweb.

2 ESCOPO

A Hostweb e suas subsidiárias (doravante referidas como "Hostweb") em razão de seu compromisso com a proteção das informações de sua propriedade e responsabilidade, tem como objetivo estabelecer diretrizes para tratamento dos ativos de informação e manter níveis aceitáveis de confiabilidade, diretrizes as quais devem ser observadas por todos os seus colaboradores, prestadores de serviço, parceiros e clientes.

Esta política é destinada e deverá ser cumprida por todos os seus colaboradores, prestadores de serviços, estagiários e terceiros, que atuam sob contrato, e que, nas suas atribuições e/ou execução do contrato, fazem uso de informações de negócio ou administrativas.

3 OBJETIVOS

Os objetivos do Sistema de Gestão de Segurança da Informação da Hostweb são:

- Garantir níveis aceitáveis de confidencialidade, integridade, disponibilidade, autenticidade e não-repúdio das informações da Hostweb;
- Garantir a existência de práticas e cultura que tenha como objetivo manter os controles de segurança em patamares aceitáveis, efetuando uma gestão de riscos de segurança assertiva e proativa;
- Atender aos requisitos regulatórios, legislativos e contratuais;
- Apoiar a manutenção das normas do Sistema de Gestão de Segurança da Informação: ISO 27001 - Gestão da Segurança da Informação;
- Garantir a capacidade da Hostweb para prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente da Hostweb conforme o

Processo de Gerenciamento de Incidentes (SGI_PR_002) e a Política de Gerenciamento de Vulnerabilidades (SGS_PO_011);

- Realizar o treinamento e a conscientização em Segurança da Informação para todos os colaboradores, estagiários e prestadores de serviço da Hostweb;

- Promover a melhoria contínua do Sistema de Gestão de Segurança da Informação, com o aumento da eficiência e segurança de seus controles.

4 DEFINIÇÕES E CONCEITOS

Estes são os conceitos referidos neste documento, conforme definidos pela ISO27000/2018:

- **Segurança da Informação**: Preservação da confidencialidade, integridade e disponibilidade da informação. Adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, também podem ser incluídas. É a proteção da informação contra uma ampla gama de ameaças, a fim de garantir a continuidade dos negócios, minimizar os riscos de negócio e maximizar o retorno sobre os investimentos e as oportunidades de negócio.
- **Confidencialidade**: Propriedade em que a informação não é disponibilizada ou divulgada para pessoas, entidades ou processos não autorizados.
- **Integridade**: Propriedade de proteger a exatidão e a integridade dos ativos. O conceito de integridade assegura que sejam prevenidas modificações não autorizadas ao software e ao hardware, que não sejam feitas modificações não autorizadas aos dados, por pessoal autorizado ou não autorizado e/ou processo, e que o dado seja internamente e externamente consistente.
- **Disponibilidade**: Propriedade de ser acessível e utilizável sob demanda por uma entidade autorizada.
- **Confiabilidade**: Propriedade de consistência dos comportamentos e resultados desejados.
- **Não repúdio**: Habilidade de provar a ocorrência de um suposto evento ou ação e suas entidades de origem.
- **Autenticidade**: Propriedade de uma entidade ser o que afirma que é.
- **Vulnerabilidade:** Fraqueza de um ativo ou controle que pode ser explorada por uma ou mais ameaças.
- **Ameaça**: Causa potencial de um incidente indesejado, a qual pode resultar no dano a um sistema ou organização.
- **Incidente de segurança da informação**: Um incidente de segurança da informação é indicado por um único ou uma série de eventos de segurança da informação, indesejáveis ou inesperados, que tenham uma probabilidade significativa de comprometer a operação dos negócios e ameacem a segurança da informação.
- **Controle**: Meios de gerenciar o risco, incluindo políticas, procedimentos, diretrizes e práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, gerencial ou legal, que modifiquem o risco à segurança da informação. É possível que os controles nem sempre exerçam os pretendidos ou assumidos efeitos de mudança, e o controle também é usado como sinônimo para salvaguarda ou contramedida.

- **Informação documentada**: informação requerida a ser controlada e mantida por uma organização e a mídia em que está contida. Informação documentada pode ser em qualquer formato e mídia e originada de qualquer fonte. Pode se referir ao sistema de gerenciamento, processos relacionados, informação criada para a operação regular da organização, evidências e registros.
- **Ativo**: Qualquer coisa que tenha valor para a organização, seja ela tangível (bens, imóveis, ferramentas, instalações, recursos, pessoas) ou intangível (softwares, propriedade intelectual, marcas, imagens, direitos, experiência, reputação).
- **ISO 27001/27002**: Normas da série ISO 27000 que fornece um framework com os requisitos e as melhores práticas para o Sistema de Gestão de Segurança da Informação (SGSI), bem como definem os controles necessários para a efetivação do SGSI;
- **Sistema de Gestão de Sistema de Informação (SGSI)**: Sistema criado para viabilizar o alcance dos objetivos, constituindo uma declaração formal acerca de seu compromisso. Parte do sistema total de gerenciamento, baseado em uma abordagem de riscos de negócio, para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar a segurança da informação nas atividades internas e externas da Hostweb. O sistema de gerenciamento inclui estrutura organizacional, políticas, atividades de planejamento, responsabilidades, práticas, procedimentos, processos e recursos.
- **Política**: A intenção e orientação geral de uma organização formalmente expressa pela administração.
- **Comitê de Gestão de Segurança da Informação (CGSI)**: Grupo multidisciplinar que reúne representantes de diversas áreas da Hostweb. É um órgão deliberativo, independente e de caráter permanente composto por indicados e aprovados pelas suas respectivas lideranças e vinculado às Diretorias. Este Comitê deve deliberar sobre assuntos referentes a temas estratégicos, métricas, riscos e eventos de segurança, documentações, controles organizacionais, planejamento e melhoria contínua do SGSI.

5 PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

5.1 Princípios

Os princípios da Segurança da Informação abrangem, basicamente, os seguintes aspectos:

- **Confidencialidade**: Garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- **Integridade**: Garantia de que a informação seja mantida em seu estado original, visando protegê-la, no processo, transporte e armazenamento, contra alterações indevidas, intencionais ou acidentais.
- **Disponibilidade**: Garantia de que os colaboradores autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.
- **Autenticidade**: Valida a autorização do usuário (mediante credenciais e processo de autenticação) para acessar, transmitir e receber determinadas informações, confirmando a identidade dos colaboradores antes de liberar o acesso aos sistemas e recursos, garantindo que não se passem por pessoas não autorizadas.
- **Não-repúdio**: Também conhecido como irretratabilidade. Garante que uma pessoa ou entidade não possa negar a autoria da informação fornecida, como no caso do

uso de certificados digitais para transações online e assinatura de documentos eletrônicos.

5.2 Ações para assegurar estes princípios

Definem-se como ações necessárias para assegurar a Confidencialidade, Integridade, Disponibilidade, Autenticidade e Não-Repúdio dos ativos e informações da Hostweb:

- Os colaboradores devem assumir uma postura proativa no que diz respeito à proteção das informações da Hostweb e devem estar atentos a ameaças externas, bem como fraudes, roubo de informações e acesso indevido aos sistemas de informação sob responsabilidade da Hostweb;

- As informações não podem ser transportadas em qualquer meio físico, sem as devidas proteções e autorizações;

- Assuntos sigilosos classificados como confidenciais não devem ser expostos publicamente;

- Senhas, chaves e outros recursos de caráter pessoal são considerados intransferíveis e não podem ser compartilhados e divulgados;

- Somente softwares licenciados para a Hostweb devem ser utilizados em seu ambiente;

- Documentos impressos e arquivos contendo informações confidenciais devem ser armazenados e protegidos. O descarte deve ser feito de forma segura, seguindo legislação pertinente;

- Todo colaborador, para poder acessar dados nos sistemas utilizados pela Hostweb, deverá possuir um login ou usuário de acesso atrelado à uma senha que siga os padrões estabelecidos agregado a um processo de duplo fator de autenticação;

- O login deve ser pessoal e intransferível, ficando vedada a utilização de login ou usuário de acesso genérico ou comunitário, exceto previamente autorizado e formalizado junto a área de Segurança da Informação;

- Os dados que necessitam de compartilhamento devem ser alocados em locais apropriados, atentando às permissões de acesso aplicáveis aos referidos dados;

- Todos os dados considerados como imprescindíveis aos objetivos da Hostweb devem ser protegidos através de rotinas sistemáticas e documentadas de cópia de segurança (backup), devendo ser submetidos aos testes periódicos de recuperação;

- O acesso físico às dependências da Hostweb deve ser controlado de maneira que sejam aplicados os princípios da integridade, confidencialidade e disponibilidade, autenticidade e não-repúdio garantindo a rastreabilidade e a efetividade do acesso autorizado;

- O acesso lógico aos sistemas computacionais disponibilizados pela Hostweb deve ser controlado de maneira que sejam aplicados os princípios da integridade, confidencialidade, disponibilidade, autenticidade e não-repúdio da informação, garantindo a rastreabilidade e a efetividade do acesso autorizado;

- São de propriedade da Hostweb todas as criações, materiais, códigos, informações criadas, manipuladas ou procedimentos desenvolvidos por qualquer colaborador durante o curso de seu vínculo com a empresa, nos limites legais como a Lei n° 9.279/96 (Propriedade Industrial), Lei n°9.609/98 (Lei de Software), Lei n°9.610/98 (Lei de Direitos Autorais) e demais legislações aplicáveis.

- Documentos imprescindíveis para as atividades da Hostweb deverão ser salvos em rede ou nuvem corporativa. Tais arquivos, se gravados apenas localmente nos computadores, com sua integridade e confidencialidade de responsabilidade do próprio colaborador.

- Arquivos pessoais e/ou não pertinentes às atividades diretas da Hostweb não deverão ser copiados ou movidos para os drives de rede ou nuvem corporativa. Caso identificados, os arquivos poderão ser excluídos definitivamente sem necessidade de comunicação prévia ao colaborador.

- Os projetos gerenciados e realizados pela Hostweb deverão adotar critérios de Segurança da Informação para o cumprimento desta política.

5.3 Melhoria Contínua

A Hostweb se compromete em buscar a Melhoria Contínua como prática permanente em todas as suas atividades, sistemas e processos, nestes inclusas o Sistema de Gestão de Segurança da Informação. buscando sua eficácia e adaptação frente a mudanças tecnológicas, operacionais e regulamentares.

Este compromisso é objeto de nosso Procedimento de Gestão de Melhoria Contínua (SGI_PG_003) e é assegurado por:

- Análises críticas periódicas do próprio Sistema de Gestão de Segurança da Informação por completo, bem como análises focadas em processos e procedimentos de segurança específicos;

- Acompanhamento permanente de indicadores estratégicos e operacionais do Sistema de Gestão de Segurança da Informação;

- Procedimentos específicos para tratamento de Não-Conformidades (SGI_PG_004), abrangendo a busca, tratamento e Gerenciamento de Problemas (SGI_POP_004), bem como implementação de Oportunidades de Melhoria (SGI_PG_003);

- Promoção de uma cultura de segurança junto a todos os colaboradores, clientes e parceiros de negócio.

6 PROGRAMA DE CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO

Uma das atribuições do Comitê de Gestão de Segurança da Informação é enviar regularmente informativos para todos os colaboradores sobre a importância de proteger os ativos de informação da Hostweb, bem como realizar programas de conscientização sobre as principais ameaças existentes e como evitá-las.

Anualmente são realizados treinamentos para conscientização de todos os colaboradores na Hostweb. Todo colaborador deve passar pelo programa de conscientização, com objetivo de tomar conhecimento dos controles, postura ideal e boas práticas de segurança, bem como entender detalhes dos riscos existentes e como lidar com cada situação.

Por ocasião do onboarding, é realizado em conjunto com a área de Gestão de Talentos (GETH) capacitação específica dos novos colaboradores, onde são apresentados aos novos colaboradores a estrutura do SGSI, normas e regulamentos internos bem como boas práticas de Segurança da Informação.

Soma-se ao programa de conscientização interno a disponibilização de informações de segurança aos usuários finais, parceiros e clientes sobre a utilização de produtos e serviços oferecidos pela Hostweb.

7 CLASSIFICAÇÃO, TRATAMENTO E RASTREABILIDADE DA INFORMAÇÃO

Todos os documentos que estruturam e compõem o Sistema de Gestão de Segurança da Informação da Hostweb devem estar aderentes aos padrões de classificação determinados no Procedimento de Gestão de Controle de Informações Documentadas (SGSI_PG_001), contendo uma identificação que facilite o reconhecimento imediato do seu grau de sigilo.

Toda informação deve ter um proprietário, ao qual cabe classificar a informação de acordo com os aspectos de grau de sigilo necessários, bem como ser responsável pela tomada de decisão quanto à proteção durante o ciclo de vida útil da informação.

O acesso à informação será disponibilizado de acordo com os perfis e regras de acesso definidas na Norma de Gestão de Acessos (SGI_NO_004) e Política de Classificação da Informação (SGI_PO_001).

Todos os sistemas computacionais, redes de comunicação, arquivos, sistemas de telefonia e documentos impressos devem ser classificados dentro dos níveis de segurança definidos na Política de Classificação da Informação.

Toda informação deve ser classificada e controlada de maneira que sejam aplicados os princípios da integridade, confidencialidade, disponibilidade, autenticidade e não-repúdio garantindo a rastreabilidade de acordo com seu grau de sigilo.

8 CONTROLE DE ACESSO E AUTENTICAÇÃO

A responsabilidade de criação, suspensão ou modificação de acessos lógicos e as respectivas permissões de acessos aos sistemas utilizados, bem como os procedimentos para gestão e análise crítica destes acessos e orientações de conduta aos colaboradores na Hostweb encontram-se estabelecidos na Norma de Gestão de Acessos (SGI_NO_004).

9 SEGURANÇA FÍSICA E DO AMBIENTE

Os ambientes físicos da Hostweb são classificados em níveis de acesso, os quais determinarão os controles de segurança adequados para cada nível de restrição de acesso dos ambientes, de acordo com a criticidade dos ativos contidos no ambiente. As responsabilidades, procedimentos e respectivos controles de segurança física, ambiental e dos equipamentos da Hostweb estão descritas na Política de Acesso às Áreas Seguras (SGI_PO_012) e na Política de Proteção Física de Equipamentos (SGI_PO_015).

10 SEGURANÇA EM NUVEM

O uso de aplicações e serviços em nuvem não somente é uma das soluções ofertadas aos nossos clientes, como também é por si essencial para a Hostweb atingir um ganho de disponibilidade, confiabilidade e escala para a prestação de seus próprios serviços. Nesse sentido, para atender aos requisitos de Segurança da Informação devem ser seguidas as diretrizes contidas tanto em nossa na Norma de Gestão de Segurança em Redes (SGI_NO_006) quanto nos demais documentos do SGSI para nortear responsabilidades, configurações e decisões relacionadas ao uso destes recursos.

A Hostweb possui infraestrutura própria de armazenamento de dados bem como faz uso de soluções terceirizadas de SaaS (*Software as a Service*) em nuvem, cujo acesso é franqueado aos colaboradores de acordo com a necessidade do negócio.

Diante disto convencionamos ser absolutamente proibido o envio, transmissão ou armazenamento de dados, arquivos ou informações da Hostweb ou de terceiros em soluções não homologadas pela Hostweb, bem como é proibido armazenar conteúdo pessoal ou particular nas soluções em nuvem homologadas.

11 CONTROLES CRIPTOGRÁFICOS

Cabe à equipe de Segurança de Informação a análise, implementação e revisão dos controles criptográficos para a proteção da informação de acordo com sua criticidade, conforme Política de Controles Criptográficos (SGI_PO_007). Os padrões de criptografia em trânsito e em descanso, gestão e cerimonial de chaves e revisão serão gerenciados atendendo às melhores práticas dos frameworks de segurança, legislação vigente e demais normas internas.

12 BACKUP

Toda informação, sistema, software e/ou dados considerados vitais ou críticos para o suporte e/ou a continuidade de negócios da Hostweb deverão ser submetidos à cópia de segurança sob forma de backup, em períodos previamente estabelecidos de acordo com seu grau de criticidade.

O Processo de Backup e Restore Hostweb (SGI_PR_004) contém as diretrizes para a gestão de cópia de segurança dos dados custodiados e de propriedade da Hostweb, direcionando e orientando sobre as bases comuns para a realização de cópias de segurança, restauração, armazenamento e testes de restore.

13 REDE CORPORATIVA

Para garantir a comunicação segura e que apenas dispositivos que não tragam riscos à operação da Hostweb façam parte da rede interna, o acesso à rede corporativa deverá ser liberado de acordo com os padrões previamente estabelecidos na Norma de Gestão de Acessos (SGI_NO_004) e Norma de Gestão de Segurança em Redes (SGI_NO_006). Dispositivos que não atenderem aos requisitos não deverão obter acesso à rede e se necessário deverão ser analisados pelas áreas responsáveis.

O acesso remoto à rede corporativa, principalmente a sistemas críticos, deverá ser feito mediante a meios de comunicação autorizados e homologados, a exemplo de VPN corporativa da Hostweb. O acesso a sistemas SaaS, poderá ser acessado via uso de VPN desde que tenha sido previamente analisado e parametrizado pela área responsável.

As redes e sub-redes encontram-se segmentadas física e logicamente, a fim de proporcionar o controle de acesso restrito, proteção e isolamento dos ambientes críticos. Os acessos e logs são armazenados em acordo com o determinado pela legislação brasileira, bem como são periodicamente analisados.

A responsabilidade pela gestão e manutenção da infraestrutura de rede interna e do Data Center Hostweb é de responsabilidade das equipes de Infraestrutura – Facilities e de Tecnologia – Redes.

14 CORREIO ELETRÔNICO, MENSAGERIA E TRANSMISSÃO SEGURA

O serviço de correio eletrônico, mensageria, bem como demais meios de comunicação disponibilizados pela Hostweb, devem ser usados exclusivamente para atender propósitos, suporte, serviços e objetivos específicos de negócios da Hostweb, sendo a ela legítimo, quando julgar necessário e sem prévio aviso as seguintes ações:

- Suspender o serviço de um ou vários usuários/logins;
- Não fornecer o serviço àqueles que não sejam de interesse da Hostweb;
- Monitorar o uso do e-mail corporativo, inspecionando os destinatários, conteúdo das mensagens, anexos, mesmo estes tendo conteúdo confidencial;

As ferramentas de comunicação utilizadas oficialmente pela Hostweb tanto para sua comunicação interna quanto eventual comunicação com parceiros, clientes e entidades externas, bem como eventuais orientações de conduta para o uso destas ferramentas estão determinadas na Norma de Gestão de Segurança em Redes (SGI_NO_006), devendo sempre serem observadas a classificação das informações tratadas conforme o grau de confidencialidade exigido.

Por meio de soluções de prevenção de vazamento de dados, a transferência de dados pessoais e sensíveis podem ser monitorados, bem como podendo ser bloqueado o envio de dados como: CPF, CNPJ, número de conta bancária, número de cartão de crédito (PAN), chaves criptográficas, token etc.

Não deve ser utilizado o e-mail ou ferramenta de CRM (Customer Relationship Management) SDM (Service Desk Management) ou ITSM (IT Service Management) para enviar para clientes, parceiros ou qualquer outra entidade externa à Hostweb dados sensíveis, confidenciais e sigilosos, tais como dados cadastrais de pessoas, empresas, dados financeiros, dados de cartão e etc, sem a devida utilização de técnicas de criptografia, conforme a Política de Controles Criptográficos (SGI_PO_007). Situações que eventualmente tragam essa necessidade deverão ser discutidas com a área de Segurança da Informação. Os clientes sempre devem acessar ou obter seus dados das nossas plataformas através das API's (Application Programming Interface) ou aplicações que a Hostweb disponibiliza.

Dados sensíveis e pessoais não devem ser enviados via web, e-mail ou formas semelhantes, sem prévia autorização.

15 GESTÃO DE VULNERABILIDADES

Para verificação da segurança no ambiente da Hostweb, quais sejam, mas não se limitando, a redes, arquiteturas, sistemas, aplicações, APIs, deve-se:

- Executar periodicamente ou toda vez que houver mudanças significativas, varreduras nos ambientes da Hostweb a fim de identificar possíveis fragilidades e vulnerabilidades que possam comprometer os sistemas e/ou informações;
- Executar periodicamente, ou toda vez que houver mudanças significativas no ambiente, testes de invasão;
- Repetir todas as varreduras até que se obtenha um resultado satisfatório;
- Documentar formalmente todas as varreduras, a fim de efetuar o levantamento dos riscos nas vulnerabilidades encontradas;
- Tratar e resolver todas as vulnerabilidades encontradas conforme a sua classificação;

Todas as diretrizes acima devem respeitar e seguir a Política de Gerenciamento de Vulnerabilidades (SGI_PO_011), sem prejuízo das demais normas internas.

16 MONITORAMENTO DO AMBIENTE

Define-se como necessário a existência de mecanismos de monitoramento permanente dos recursos e sistemas da Hostweb para:

- Permitir o monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede, de modo que a informação gerada por esses sistemas possa ser usada para identificar logins e respectivos acessos efetuados, bem como situações anômalas;
- Tornar disponível as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial ou por determinação do setor Jurídico;

- Realizar, a qualquer tempo, inspeção física e/ou lógica, auditoria interna ou externa e demais coletas de informação nos equipamentos e informações de propriedade da Hostweb;
- Permitir mecanismos e práticas de proteção preventivos, detectáveis, ou corretivos para garantir a segurança das informações e dos perímetros do ambiente;
- Desinstalar ou solicitar a remoção, remotamente ou *in loco*, a qualquer tempo, de qualquer software ou sistema que represente risco ou esteja em não conformidade com as políticas, normas e procedimentos vigentes.

17 SISTEMAS ANTIMALWARE

A Hostweb possui sistemas de Antimalware instalados em todos seus servidores e estações de trabalho, bem como em seus serviços de e-mail.

Os serviços de Antimalware devem ser configurados para monitorar e alertar a área de Segurança da Informação sobre suspeitas de comprometimentos, bem como para buscar automaticamente atualizações dos sistemas e de novas definições de vírus. Além dos pontos aqui apresentados, a Hostweb realizará a informação e conscientização dos seus colaboradores a fim de evitar possíveis infecções por softwares maliciosos, em acordo com a Política de Proteção Contra Malwares (SGI_PO_010) e demais normas.

18 USO DE ATIVOS, HARDWARE E SOFTWARE

Os ativos corporativos da Hostweb, nestes inclusos hardware e software de propriedade da Hostweb, deverão ser utilizados somente para as atividades em interesse da Hostweb, sendo vedado o uso destes ativos para propósitos não relacionados com o negócio da Hostweb, bem é vedado o acesso a contas ou serviços pessoais e particulares nos ativos da Hostweb.

É proibido por padrão o uso de equipamentos pessoais (tais como computadores e dispositivos móveis) para execução de atividades da Hostweb, sendo admitido excepcionalmente o uso de celular pessoal apenas para fins de autenticação de dois fatores.

Tendo em vista o uso internamente difundido de soluções de armazenamento em nuvem e em conformidade com as melhoras práticas de segurança da informação, adotamos solução de bloqueio por padrão de conexão de discos externos e mídia removível aos equipamentos de microinformática.

Atendendo às melhores práticas para prevenção de incidentes de segurança, a Hostweb possui lista de softwares pré-autorizados para instalação e uso em suas estações de trabalho, de acordo com as atividades executadas por cada colaborador.

Caso o colaborador necessite, para a execução de suas atividades funcionais, instalar software que não conste na lista de softwares pré-autorizados ou conectar mídia removível à sua estação de trabalho, deverá requisitar internamente esta excepcionalidade, conforme Política de Uso Aceitável de Ativos (SGI_PO_004), Política de Uso de Mídias Removíveis e Dispositivos Móveis (SGI_PO_005) e Política de Controle de Software (SGI_PO_014).

O descarte e encerramento do ciclo de vida útil de hardware, mídia removível e mídia física deve seguir e respeitar a Política de Uso Aceitável de Ativos (SGI_PO_004) e a Norma de Descarte e Destinação Segura de Equipamentos Eletroeletrônicos (SGI_NO_001).

19 GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

A Hostweb possui uma estratégia de monitoramento, observabilidade e resposta a incidentes de Segurança da Informação que abrange seus recursos, ativos e produtos críticos, em consonância com requisitos legais e as melhores práticas adotadas mundialmente.

A fim de fortalecer uma cultura de zelo à segurança da informação, bem como entendendo esta proteção como obrigação de todos os participantes em conjunto, a Hostweb adota uma postura proativa na prevenção, comunicação e tratamento de possíveis incidentes de segurança.

É obrigação de todos os colaboradores reportar incidente de segurança ao time de Tecnologia – Segurança com a maior brevidade possível, incluindo, mas não se limitando a:

- Equipamento perdido ou roubado;
- Vírus encontrado na estação de trabalho ou servidor;
- Software ou sistemas que não estejam funcionando normalmente;
- Quebra ou desrespeito às políticas e padrões da Hostweb;
- Identificação de comportamento que seja contra as diretrizes desta política.

Os procedimentos para reporte e tratamento de Incidentes de Segurança da Informação estão determinados no Processo de Gerenciamento de Incidentes (SGI_PR_002). Além dos colaboradores, orientamos clientes, fornecedores e terceiros envolvidos a também reportar incidentes que afetem a prestação dos serviços da Hostweb, sempre atendendo aos requisitos, responsabilidades e prazos convencionados em contrato.

Deve-se ainda, realizar testes dos controles de segurança e prevenção de incidentes e implementar melhorias de acordo com as análises de probabilidade e impacto e os resultados observados que deverão ser endereçados às respectivas áreas responsáveis pelas implementações.

20 PRIVACIDADE

A Hostweb entende que empreender o máximo de esforços para garantir a privacidade das informações e a segurança dos dados pessoais de nossos clientes, colaboradores e terceiros é parte fundamental da prestação de seus serviços.

Através da Política de Privacidade (SGI_PO_009), a Hostweb demonstra como, na qualidade de Controlador de Dados Pessoais, pode eventualmente coletar, usar ou de outra forma tratar informações e Dados Pessoais de pessoas naturais no desempenho de nossas atividades, sejam elas clientes, colaboradoras, parceiras ou terceiros.

Caso seja absolutamente necessária a coleta ou outra forma de tratamento de dados pessoais para a prestação dos serviços, todos os colaboradores da Hostweb são instruídos a limitar este tratamento estritamente ao mínimo necessário e adequado para atingir a

finalidade deste tratamento, respeitando as bases legais estabelecidas em acordo com a legislação em vigor.

A Hostweb se compromete a auxiliar no atendimento aos direitos do titular conforme determinado por nossa Política Geral de Proteção de Dados Pessoais (SGI_PO_008), sempre que viável e em acordo com as exigências legais.

21 TESTES DE SEGURANÇA

A Hostweb periodicamente realiza testes internos e externos e análise crítica periódica dos controles de segurança da informação conforme as respectivas finalidades, assegurando que estes atendem às necessidades da empresa, a exemplo das diretrizes específicas na Norma de Gestão de Acessos (SGI_NO_004), Política de Controles Criptográficos (SGI_PO_007), Processo de Backup e Restore Hostweb (SGSI_PR_004) e Plano de Continuidade de Negócios (SGI_PL_004).

22 CONTINUIDADE DE NEGÓCIOS

Visando assegurar a continuidade de suas operações mesmo nos casos mais extremos de impacto à segurança, a Hostweb possui um Plano de Recuperação de Desastres (SGI_PL_003) e Plano de Continuidade de Negócios (SGI_PL_004), no qual encontram-se estabelecidos os princípios básicos e a estrutura necessária para assegurar a resposta de emergência, retomada, restauração e recuperação permanente das operações e atividades essenciais da organização durante um evento crítico de interrupção de negócios.

23 PAPÉIS E RESPONSABILIDADES DO SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

O Sistema de Gestão de Segurança da Informação da Hostweb deverá ser gerido, aplicado, estruturado e mantido pelas equipes da Hostweb, cujas responsabilidades deverão ser definidas e divulgadas para toda a Hostweb.

23.1 Direção

Cabe à Direção da Hostweb:

23.1.1 Identificar, atribuir e delimitar responsabilidades com relação à segurança da informação na Hostweb, bem como responsabilidades para a verificação de conformidade com os requisitos da ISO27001 e demais normas de segurança da informação

23.1.2 Difundir e incentivar para todos os colaboradores uma cultura de Segurança da Informação;

23.1.3 Prover os recursos necessários para garantir a eficácia do Comitê de Gestão de Segurança da Informação;

23.1.4 Assessorar o Comitê quanto a qualquer decisão relacionada ao Sistema de Gestão de Segurança da Informação (SGI), bem como quanto à estratégia e ações para redução de riscos;

23.1.5 Apoiar as políticas e as diretrizes do SGSI da Hostweb;

23.1.6 Receber relatórios de violações da política e diretrizes do SGSI;

23.1.7 Realizar a análise crítica do SGSI e contribuir para a melhoria contínua da segurança da informação;

23.2 Comitê de Gestão de Segurança da Informação

O Comitê de Gestão de Segurança da Informação (CGSI) é um grupo multidisciplinar que reúne representantes de diversas áreas da Hostweb. É um órgão deliberativo, independente e de caráter permanente composto por indicados e aprovados pelas suas respectivas lideranças e vinculado às Diretorias. Este Comitê deve deliberar sobre assuntos referentes a temas estratégicos, métricas, riscos e eventos de segurança, documentações, controles organizacionais, planejamento e melhoria contínua do SGI. Cabe ao Comitê de Gestão de Segurança da Informação:

23.2.1 Promover a Segurança da Informação na organização, avaliando e aprovando as políticas de Segurança da Informação da Hostweb;

23.2.2 Analisar e deliberar sobre casos de violação desta política;

23.2.3 Monitorar ocorrências que possam impactar na segurança e, se necessário, aprovar iniciativas que melhorem o nível de segurança;

23.2.4 Propor ajustes, aprimoramentos e modificações na estrutura normativa e organizacional, submetendo à avaliação da Alta Direção da Hostweb;

23.2.5 Aprovar mecanismos de registro e controle de eventos e incidentes de Segurança da Informação, bem como, de não conformidades;

23.2.6 Acompanhar o andamento dos projetos e iniciativas relacionados à Segurança da Informação;

23.2.7 Realizar, sistematicamente, a gestão de riscos relacionados à Segurança da Informação, analisar e deliberar sobre a estratégia de proteção e mitigação dos mesmos;

23.2.8 Viabilizar e promover o planejamento, manutenção e melhoria contínua do SGSI.

23.3 Segurança

Cabe ao Time de Segurança:

23.3.1 Acompanhar o desenvolvimento, comunicação e gestão atualizadas as políticas, normas e os procedimentos de Segurança da Informação;

23.3.2 Elaborar e implementar controles técnicos e processuais alinhados às diretrizes desta política;

23.3.3 Receber, analisar e notificar as lideranças, bem como diligenciar para solucionar os casos de violação das políticas de Segurança da Informação;

23.3.4 Elaborar e conduzir periodicamente um programa de conscientização em temas de Segurança da Informação;

23.3.5 Conduzir a gestão, análise e o tratamento de riscos de Segurança da Informação;

23.3.6 Realizar a gestão das vulnerabilidades dos ativos da Hostweb, de acordo com a periodicidade e escopo definidas em norma própria;

23.3.7 Estabelecer mecanismos de registro, controle, prevenção, monitoramento, distribuição e escalonamento dos procedimentos de resposta de incidentes, eventos e não conformidades de Segurança da Informação;

23.3.8 Coordenar a análise, avaliação, seleção, implementação e testes de controles criptográficos e demais medidas técnicas de proteção às informações da empresa;

23.3.9 Coordenar projetos e iniciativas para assegurar que os objetivos de Segurança da Informação sejam atingidos;

23.4 Compliance, Auditoria Interna e Governança

Cabe à área de Governança:

23.4.1 Assegurar que as práticas e processos da empresa estejam alinhados aos requisitos da norma ISO27001, ISO27017, ISO27018 e demais normas e frameworks de Segurança da Informação e Governança Corporativa, contribuindo na implementação, manutenção e melhoria contínua do Sistema de Gestão de Segurança da Informação;

23.4.2 Avaliar a efetividade e adequação dos processos internos para atingir os objetivos de segurança da Informação da Hostweb, bem como acompanhar os indicadores de desempenho do SGI e relatar o desempenho do SGSI para a Direção da Hostweb;

23.4.3 Coordenar a estruturação, planejamento, redação, publicação e revisão dos procedimentos de gestão do SGI, a fim de auxiliar gestores, coordenadores e demais colaboradores da Hostweb em sua atuação;

23.4.4 Consolidar, manter e coordenar a elaboração e evolução, acompanhamento e avaliação do SGI, bem como realizar rondas, vistorias, auditorias e análise crítica, visando melhoria contínua;

23.4.5 Manter as áreas da Hostweb informadas sobre eventuais alterações legais e/ou regulatórias que impliquem responsabilidade e ações envolvendo Segurança da Informação, bem como acompanhar se as atividades executadas pelas áreas estão em compliance com estas alterações.

23.4.6 Auditar os processos operacionais, estratégicos e táticos, visando a conformidade das atividades executadas e a eficácia dos controles de Segurança da Informação.

23.4.7 Gerenciar e acompanhar o desempenho de processos, atividades e colaboradores e demais ações visando excelência em governança administrativa.

23.4.8 Auxiliar as áreas operacionais na estruturação, análise, redesenho, treinamento e gestão de seus processos de negócio.

23.5 Suporte Interno

O time de Suporte Interno é responsável por:

23.5.1 Realizar a instalação, manutenção preventiva e corretiva dos equipamentos de microinformática da Hostweb, bem como gerenciar estes ativos em controle próprio;

23.5.2 Atender às solicitações internas dos colaboradores referentes aos ativos de microinformática e softwares da Hostweb ou providenciar o encaminhamento à equipe responsável pela continuidade do tratamento, de acordo com as políticas e processos internos;

23.5.3 Realizar vistoria de mesa e tela limpa nos ambientes e estações de trabalho da Hostweb conforme solicitação da equipe de Governança.

23.6 Comitê Consultivo de Mudanças

É composto por representantes de áreas multidisciplinares (líderes e/ou analistas delegados) envolvidas no Processo de Gerenciamento de Mudanças. Cabe ao Comitê Consultivo de Mudanças:

23.6.1 Realizar Análise técnica e processual das mudanças normais;

23.6.2 Avaliar possíveis riscos decorrentes das mudanças normais a serem executadas

23.6.3 Aprovar ou reprovar mudanças normais.

23.7 Área de Gestão de Talentos (GETH)

Cabe à área de Gestão de Talentos (GETH):

23.7.1 Gerenciar as atividades de seleção e recrutamento de novos colaboradores cumprindo requisitos de segurança da informação e em conformidade com as regulamentações internas e leis vigentes.

23.7.2 Assegurar que os colaboradores assinem o termo de ciência e compromisso de Segurança da Informação, bem como termos de Sigilo e Confidencialidade e demais políticas que compõem o SGI.

23.7.3 Realizar em conjunto com representante Comitê de Gestão de Segurança da Informação a conscientização dos novos colaboradores sobre importância e boas práticas da Segurança da Informação.

23.8 Gestão

Cabe aos Gerentes das Áreas de Negócios que compõem a Gestão da Hostweb:

23.8.1 Cumprir e fazer cumprir a política, as normas e diretrizes de Segurança da Informação;

23.8.2 Assegurar que a sua área possua acesso e entendimento das políticas, das normas e diretrizes de Segurança da Informação;

23.8.3 Garantir que todas as diretrizes, procedimentos e controles operacionais da sua área, estejam documentados, detalhados e atualizados;

23.8.4 Comunicar imediatamente a área de Segurança da Informação eventuais casos de violação da política, de normas ou diretrizes;

23.8.5 Incentivar que esta política, demais normas e diretrizes de Segurança da Informação sejam cumpridos de acordo com os preceitos definidos para a sua área de atuação;

23.8.6 Armazenar evidências dos processos, assim como fornecê-las quando solicitado pelas áreas responsáveis por controles internos e auditoria;

23.8.7 Garantir na análise e elaboração de projetos internos, com clientes ou Terceiros, sempre que necessário e quando aplicável, que sejam realizadas avaliações específicas relacionadas à Segurança da Informação e proteção de dados pessoais ou sensíveis, com o objetivo de proteger os interesses e ativos críticos da Hostweb.

23.9 Colaboradores

Cabe a todos os Colaboradores da Hostweb, independentemente de seu cargo, função, vínculo contratual ou setor onde exerce suas atividades:

23.9.1 Conhecer, seguir e disseminar as diretrizes estabelecidas nesta política e demais diretrizes de Segurança da Informação;

23.9.2 Apoiar na implementação dos controles de Segurança da Informação em sua alçada de atuação;

23.9.3 Fazer uso apropriado de sistemas, recursos e serviços de tecnologia da Hostweb. Estes incluem, mas não se limitam a computadores, laptops, aparelhos telefônicos, celulares, correio eletrônico, sistemas, internet, entre outros;

23.9.4 Assegurar a correta classificação das informações sob sua responsabilidade;

23.9.5 Observar e respeitar o grau de confidencialidade definida pelo proprietário da informação;

23.9.6 a integridade e confidencialidade de dados pessoais ou sensíveis aos quais tiver acesso através da Hostweb, utilizando-os estritamente para o fim a que se destina;

23.9.7 Acessar apenas informações necessárias às suas atividades. Se porventura obtiver acesso a informações que não competem às suas atividades, deverá imediatamente comunicar a área de Segurança da Informação e ao seu líder;

23.9.8 Em caso de rescisão, realizar a devolução de todos os ativos de informação sob sua responsabilidade e garantir que não restam sob seu domínio, informações de propriedade da Hostweb;

23.9.9 Respeitar e seguir as diretrizes e procedimentos institucionais conforme Política de Propriedade Intelectual da Hostweb.

23.10 Jurídico

Cabe ao time de Jurídico:

23.10.1 Incluir na análise e elaboração de contratos de colaboradores, clientes e Terceiros, sempre que necessário e quando aplicável, cláusulas específicas relacionadas à Segurança da Informação, com o objetivo de proteger os interesses da organização;

23.10.2 Avaliar, quando solicitado pelas áreas ligadas ao tema, as políticas, as diretrizes, as normas e procedimentos de Segurança da Informação da Hostweb.

23.11 Terceiros

Cabe aos prestadores de serviço, contratados, subcontratados e demais terceiros envolvidos nas atividades da Hostweb:

23.11.1 Conhecer, seguir e disseminar as diretrizes da Hostweb estabelecidas na Política de Segurança da Informação para Terceiros;

23.11.2 Apoiar na implementação dos controles de Segurança da Informação em sua alçada de atuação na Hostweb;

23.11.3 Fazer uso apropriado de sistemas, recursos e serviços de tecnologia da Hostweb. Estes incluem, mas não se limitam a computadores, laptops, aparelhos telefônicos, celulares, correio eletrônico, sistemas, internet, entre outros;

23.11.4 Respeitar a correta classificação das informações que produza para a Hostweb;

23.11.5 Observar e respeitar o grau de confidencialidade definida pelo proprietário da informação na Hostweb;

23.11.6 Garantir a integridade e confidencialidade de dados pessoais ou sensíveis aos quais tiver acesso através da Hostweb, utilizando-os estritamente para o fim a que se destina;

23.11.7 Acessar apenas informações necessárias às suas atividades na Hostweb. Se porventura obtiver acesso a informações que não competem às suas atividades, deverá imediatamente comunicar ao gestor do seu contrato, para que o mesmo informe a área de Segurança da Informação da Hostweb;

23.11.8 Em caso de rescisão de contrato, realizar a devolução de todos os ativos de informação sob sua responsabilidade e garantir que não restam sob seu domínio, informações de propriedade da Hostweb;

23.11.9 Cumprir as melhores práticas e legislações vigentes relativas às diretrizes de Propriedade Intelectual e Propriedade Industrial do Brasil ou legislação local equivalente.

24 ATUALIZAÇÃO DESTA POLÍTICA

Esta Política de Segurança da Informação deverá ser revista e atualizada anualmente ou quando houver mudanças nos objetivos do negócio e ambiente de risco. A versão mais atual encontra-se publicada na Base de Conhecimento da Hostweb.

25 LEGISLAÇÃO E NORMAS REREFENCIADAS

A Hostweb compromete-se a atender rigorosamente a todos os requisitos aplicáveis relacionados à segurança da informação, incluindo requisitos legais, regulamentares, contratuais e outras obrigações relevantes. Este compromisso garante a proteção dos ativos de informação, promovendo a confiança de nossos clientes, parceiros e stakeholders no tratamento seguro das informações sob nossa responsabilidade.

O colaborador deverá sempre acessar este documento e os demais normativos da Hostweb através do repositório do Sistema de Gerenciamento de Segurança da Informação localizado no Diretório de Processos da Hostweb.

A presente Política de Segurança da Informação, bem como as demais normas internas que compõem o SGSI da Hostweb foram redigidas em conformidade aos preceitos legais, infralegais e paralegais a seguir:

- Constituição Federal Brasileira de 1988
- Código Civil Brasileiro
- ISO 27000 e normas derivadas
- Marco Civil da Internet (Lei n° 12.965/12)
- Lei de Crimes Informáticos (Lei n° 12737/12)
- Lei Geral de Proteção de Dados (Lei n° 13709/18)
- Lei da Propriedade Industrial (Lei n° 9.279/96)
- Lei de Software (Lei n° 9.609/98)
- Lei de Direitos Autorais (Lei n° 9.610/98)
- Resoluções ANPD
    - Resolução CD/ANPD n° 15, de 24 de abril de 2024 (Regulamento de Comunicação de Incidente de Segurança)
    - Resolução CD/ANPD n° 2, de 27 de janeiro de 2022
- Resoluções Anatel
    - Anexo da Resolução Anatel n° 740, de 21 de dezembro de 2020 (Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações)
    - Resolução Anatel n° 767, de 07 de agosto de 2024
- ABNT NBR ISO/IEC 27001:2022
- ABNT NBR ISO/IEC 27017:2015
- ABNT NBR ISO/IEC 27018:2019

26 AUDITORIA E SANÇÕES

Para garantir a conformidade das práticas da Hostweb com esta Política de Segurança da Informação, identificar potenciais desvios, corrigir falhas e melhorar os controles de segurança da informação, a Hostweb reserva-se o direito de realizar auditorias e monitoramentos de desempenho regulares ou eventuais.

Os colaboradores Hostweb possuem ciência de que tais auditorias poderão ocorrer a qualquer momento, sem aviso prévio, em conformidade com as leis e regulamentações aplicáveis. A realização de auditorias será conduzida de forma ética e respeitosa, preservando a privacidade e os direitos individuais, conforme definido nas normas internas e na legislação aplicável.

O não cumprimento dos itens descritos nesta Norma, ainda que por mero desconhecimento, sujeitará o infrator a sanções disciplinares, incluindo, a aplicação de advertência verbal ou escrita, demissão por justa causa ou rescisão contratual, bem como sujeitará o infrator às demais penalidades administrativas, cíveis e penais previstas na legislação brasileira.

27 CONTROLE DE VERSÕES

Versão	Data	Autor	Histórico
1.0	12/12/22	Felipe Duarte / Sérgio Uchoa	Redação e Revisão Inicial do Documento.
1.1	16/10/23	Felipe Duarte	Revisão do documento, consolidação de papéis e procedimentos.
1.2	18/12/23	Felipe Duarte	Revisão de papéis e responsabilidades
1.3	08/03/24	Ítalo Magalhães / Felipe Duarte	Novo padrão de cabeçalho, rotulação.
1.4	28/11/24	Felipe Duarte / CGSI	Revisão dos itens 1 a 5, acréscimo itens 5.2, 5.3, 26
1.5	20/10/25	Philipe Sales / Bruna Calíope / Jamylle Oliveira	Item 5.3 - SGI_POP_004, Item 14 - Acrescentado aplicabilidade de controle criptográfico, Item 23.3.9 - Área de Governança, Item 25 - versões da ISO, novo cabeçalho, rotulação.
1.6	06/08/26	Elaine Guedes /Philpe Sales	Item 27: Alterado local de armazenamento de Microsoft Sharepoint para Zoho Workdrive