POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

HIPER TÊXTIL

Versão: 2023

Direcionado a: Uso Interno / Registro / Eventual Compartilhamento com autoridades

I - OBJETIVOS GERAIS

Instituir as regras e procedimentos de segurança da informação voltados à proteção de ativos imateriais da HIPER TÊXTIL, tais como segredos de negócio, propriedade intelectual, informações confidenciais de qualquer natureza e, em especial, a segurança de dados pessoais.

II - OBJETIVOS ESPECÍFICOS

Efetivar medidas técnicas, organizacionais e gerenciais voltadas à confidencialidade, integridade e disponibilidade das informações, incluindo aquelas de natureza pessoal.

Estabelecer rotinas de avaliação, revisão e atualização das medidas de segurança da informação.

Orientar sócios, diretoria, empregados, prestadores de serviços e fornecedores a seguirem as diretrizes de segurança da informação da HIPER TÊXTIL.

III - GLOSSÁRIO

Para perfeita compreensão dos termos da Política de Segurança da Informação a HIPER TÊXTIL estabelece, a seguir, os seguintes conceitos úteis:

IV - PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

Cada atividade que envolver tratamento de dados de qualquer natureza deverá observar o estrito cumprimento dos princípios da confidencialidade, integridade, disponibilidade, segurança e autenticidade.

V - DIRETRIZES PARA A SEGURANÇA DA INFORMAÇÃO

No emprego das diretrizes para efetivação de segurança da informação, as diversas áreas e os profissionais, empregados ou prestadores de serviços, da HIPER TÊXTIL, deverão se atentar às recomendações a seguir expostas acerca de rotinas operacionais.

5.1 Do Dever de Diligência

É responsabilidade de cada colaborador da HIPER TÊXTIL, incluindo quadro de sócios, diretoria, corpo de empregados, prestadores de serviços, temporários e outros, tomar ciência dos termos e diretrizes dessa Política de Segurança, bem como de se manter atualizado acerca de suas eventuais alterações.

Em caso de dúvida acerca de quaisquer das disposições aqui contidas, ou em como agir em frente a situações práticas, os colaboradores deverão buscar orientação de seus superiores hierárquicos, em especial quanto ao uso, edição e descarte de materiais de arquivo, equipamentos de estrutura de TI e dados armazenados.

O não cumprimento das diretrizes de segurança da informação é considerado falha grave e poderá ensejar até mesmo a demissão por justa causa do empregado ou resolução do contrato para o caso de prestadores de serviços.

5.2 Da Titularidade das Informações

Todas as informações elaboradas, obtidas ou processadas pela HIPER TÊXTIL, salvo as de natureza pessoal, são de exclusiva propriedade da empresa, razão pela qual o uso não autorizado ou em desconformidade com as políticas de segurança de informação ou de governança de proteção de dados serão considerados ilícitos contratuais.

As informações de natureza pessoal (dados pessoais) serão tratadas com ainda maior diligência pelos colaboradores da HIPER TÊXTIL, visto que são de titularidade de terceiros e que a eventual exposição desses dados pode acarretar risco às liberdades e direitos individuais.

5.3. Adequação de parceiros e fornecedores a LGPD

5.4. Responsabilidades da área de TI

Organizar a logística da TI da organização, configurar os equipamentos, instalar softwares e implementar os controles necessários para cumprir os requerimentos de segurança estabelecidos pela política de segurança da informação.

5.5. Política de treinamento aos colaboradores

Cumprir fielmente a Política, as Normas e os Procedimentos de Segurança da Informação da HIPER TÊXTIL; o Buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à segurança da informação; o Assinar Termo de Responsabilidade, formalizando a ciência e o aceite da Política e das Normas de Segurança da Informação, bem como assumindo responsabilidade por seu cumprimento;

5.6. Assegurar a confidencialidade, integridade e disponibilidade das informações da Organização, mediante utilização de mecanismos de segurança da informação, balanceando fatores de risco, tecnologia e custo;

5.7. Garantir a proteção adequada das informações e dos sistemas contra acesso, modificação, destruição e divulgação não autorizados;

5.8. Assegurar que os ativos de informação sejam utilizados apenas para as finalidades aprovadas pela Organização, estando sujeitos à monitoração e auditoria;

5.9 Garantir o cumprimento dessa Política e das Normas Corporativas de Segurança da Informação da Organização.

VI – DOS AGENTES DE SEGURANÇA DA INFORMAÇÃO

6.1 Dos Colaboradores

Cabe a todos os funcionários (funcionários, estagiários e prestadores de serviços) cumprir fielmente a Política de Segurança da Informação e:

- Buscar orientação do gestor imediato em caso de dúvidas;
- Conhecer e cumprir as normas e orientações estabelecidas nesta Política e demais Regulamentos que compõem a Política de Segurança da Informação da HIPER TÊXTIL;
- Informar as situações que comprometam a segurança das informações na HIPER TÊXTIL, através de contato direto com os responsáveis pela segurança da informação;
- Toda informação criada, modificada no exercício das funções e qualquer informação contida em mensagens do correio eletrônico corporativo deve ser tratada como referente ao negócio da HIPER TÊXTIL, não devendo ser considerada como pessoal, particular ou confidencial, mesmo que arquivadas na sua pasta pessoal;
- Garantir que seja conhecida e cumprida a proibição de compartilhamento ou negociação de credencias (ID, senhas, crachás, tokens e similares).

6.2 Da Diretoria e Supervisão

Cabe às Diretorias, Gerências e Coordenações cumprir e fazer cumprir esta Política e:

- Revisar e atualizar os treinamentos de proteção
- Realizar auditoria dos processos de proteção visando garantir a melhoria contínua;
- Garantir que suas equipes possuam acesso e conhecimento desta Política de Segurança da Informação;
- Comunicar imediatamente eventuais casos de violação de segurança da informação através do canal de denúncia.

6.3 Da Área de Tecnologia da Informação

Cabe a área de Tecnologia da Informação:

- Propor ajustes, melhorias, aprimoramentos e modificações desta Política;

- Convocar, coordenar, lavrar atas e prover apoio às reuniões que discutam a respeito desta Política;
- Prover todas as informações de gestão de segurança da informação solicitadas por Gestores;
- Buscar as melhores tecnologias visando garantir a proteção;
- Implementar e garantir que as ferramentas de apoio a divulgação de políticas estejam sendo cumprida;
- Garantir que os softwares estejam habilitados e funcionando de acordo com as políticas definidas;
- Garantir que as atualizações de softwares estejam de acordo com a política;
- Gerenciar, coordenar, orientar, avaliar e promover a implantação das ações, atividades e projetos relativos à Segurança da Informação na HIPER TÊXTIL, promovendo ações de interesse da empresa, programas educacionais e de conscientização do capital humano.

6.4 Do Encarregado de Tratamento de Dados Pessoais

Cabe a equipe responsável pelo tratamento dos dados:

- Validação de medidas técnicas e operacionais de segurança, mecanismo de consentimento;
- Promover ajustes, correções e melhoria;
- Promover testes de segurança, disponibilidade e acessibilidade de informações
- Certificar de que os processos e operações com tratamento de dados pessoais tenham sido auditados;
- Manter os registros de tratamento de dados.

VII – ORIENTAÇÕES OPERACIONAIS

7.1 Da Rede Interna e do Uso da Internet

- Material sexualmente explícito não pode ser exposto, armazenado, distribuído, editado ou gravado através do uso dos recursos computacionais da rede corporativa.
- Somente os empregados que estão devidamente autorizados a falar em nome da empresa para os meios de comunicação podem escrever em nome da empresa em sites de BatePapo (Whastapp) ou Grupos de Discussão (fóruns, newsgroups). Em caso de dúvidas, procurar a área de Comunicação.
- Todos os arquivos devem ser gravados na unidade de rede (F:), pois arquivos gravados no computador (local) não possuem cópias de segurança (backup) e podem ser perdidos. O espaço em disco é controlado por departamento, por isso, os usuários devem administrar seus arquivos gravados, excluindo os arquivos desnecessários. Importante citar que não é responsabilidade da área de TI a recuperação de arquivos que não respeitem a regra acima citada.
- Não é permitida a gravação de arquivos particulares (músicas, filmes, fotos, etc..) nos drivers de rede, pois ocupam espaço comum limitado do departamento.

- A internet deve ser utilizada para fins corporativos, enriquecimento intelectual ou como ferramenta de busca de informações, tudo que possa vir a contribuir para o desenvolvimento de atividades relacionadas à empresa.
- O acesso às páginas e web sites é de responsabilidade de cada usuário ficando vedado o acesso a sites com conteúdos impróprios.
- O uso da internet para assuntos pessoais deve ser restrito, sem comprometer as atividades dos usuários.
- É vedado qualquer tipo de download. Como também o upload de qualquer software licenciado à empresa ou de dados de propriedade da empresa ou de seus clientes, sem expressa autorização do gerente responsável pelo software ou pelos dados.
- Os acessos à internet serão monitorados através de identificação e autenticação do usuário.

7.2 Do Uso da Rede ou da Internet por Visitantes

A rede de visitantes é separada da rede interna, sem acesso a dados da empresa e da rede interna. O acesso é realizado por um sistema de voucher com limitação de tempo e tráfego de navegação. O histórico da navegação é armazenado em um registro específico.

7.3 Da Estrutura de Tecnologia da Informação

Armazenamento interno: São escolhidas as melhoras tecnologias do mercado para prover a segurança de dados, como antivírus, firewall, backup e controle de acesso.

Armazenamento externo: São escolhidas empresas que possuem as melhoras tecnologias do mundo em segurança para nos apoiar. Todas as empresas terceiras que armazenam dados da HIPER TÊXTIL, são regidas por contrato de segurança de dados, nos mesmos moldes que a HIPER TÊXTIL cuida dos seus dados internos.

7.3.1 Dos Servidores e equipamentos de apoio

- Os sistemas devem possuir controle de acesso de modo a assegurar o uso apenas por usuários autorizados. O responsável pela autorização deve ser claramente definido e ter registrado a aprovação concedida.
- Cópia de segurança (Backup) deve ser testada e mantida atualizada para fins de recuperação em caso de desastres.
- Não enviar informações confidenciais (autorizadas) para e-mails externos sem proteção. No mínimo, o arquivo deve contar com a proteção de uma senha “robusta”.

7.3.2 Da Rede e sua Segurança

- O acesso à internet dentro das estruturas da empresa se dá através cabo de rede dedicado à estação de trabalho ou através de conexão Wi-Fi protegida por senha e protocolo WPA2.
- Pastas de arquivos compartilhados localmente ou em nuvem só podem ser acessados por usuários do domínio corporativo.

- Deve haver uma rede Wi-Fi isolada específica para visitantes, a fim de evitar que acesso à rede corporativa seja concedido a pessoas não autorizadas.

7.3.3 Das Estações de Trabalho

- As estações de trabalho, incluindo equipamentos portáteis, e informações devem ser protegidos contra danos ou perdas, bem como o acesso, uso ou exposição indevidos.
- As estações de trabalho possuem códigos internos, os quais permitem que seja identificada na rede. Desta forma, tudo que for executado na estação de trabalho é de responsabilidade do funcionário.
- O acesso a estação de trabalho deverá ser encerrado no final do expediente, desligando o equipamento.
- Quando se ausentar da mesa, deverá bloquear a estação de trabalho com senha. Esta ação aplica-se a todos os funcionários com estações de trabalho, incluindo equipamentos portáteis.
- Informações sigilosas, corporativas ou cuja divulgação possa causar prejuízo à HIPER TÊXTIL, só devem ser utilizadas em equipamentos com controles adequados.
- Os usuários devem utilizar apenas softwares licenciados pela área de Infraestrutura e TI, nos equipamentos da empresa.
- A área de Infraestrutura de TI deverá estabelecer os aspectos de controle, distribuição e instalação de softwares utilizados.

7.3.4 Do Uso de Dispositivos Móveis

A HIPER TÊXTIL não fornece chips a DM para os colaboradores. Não vedada o colaborador utilizar seu DM particular para uso em trabalho.

7.3.5 Da Utilização de Serviços de Terceiros (Cloud/Datacenter)

A responsabilidade de segurança cloud, é compartilhada pelo fornecedor e pela empresa. Cabe o fornecedor garantir a segurança da infraestrutura e a empresa praticar as recomendações de segurança do fornecedor.

7.3.6 Da Política de Uso de Dispositivos Próprios (*BYOD*)

- Notebooks particulares para serem usados dentro da rede das empresas abrangidas neste documento, precisam ser avaliados pelo pessoal responsável de TI.
- Equipamentos de terceiros devem ser levados ao suporte para serem verificadas atualização do antivírus e existência de vírus.
- É responsabilidade da área contratante encaminhar os terceiros sob sua responsabilidade para esta verificação.

7.4 Da Importância do *Backup*

Temos backup realizados por fornecedores, backup internos e backup automáticos na nuvem. Isso depende de cada sistema. A responsabilidade da segurança de backup externos é do fornecedor, dos backups internos a empresa.

VIII – DIRETRIZES GERENCIAIS

8.1 Da Política de Controle de Acesso à Informação

- Temos hoje o documento assinado pelo colaborador ao entrar na empresa chamado COMPROMISSO DE SIGILO PROFISSIONAL E CONFIDENCIALIDADE DE INFORMAÇÕES". A solicitação de acesso as informações são realizadas pelos líderes de cada área.
- Todo usuário deve ter uma identificação única, pessoal e intransferível, qualificando-o como responsável por qualquer atividade desenvolvida sob esta identificação. O titular assume a responsabilidade quanto ao sigilo da sua senha pessoal.
- Utilizar senha de qualidade, com pelo menos oito caracteres contendo números, letras (maiúsculas e minúsculas) e caracteres especiais (símbolos), e não deverá utilizar informações pessoais fáceis de serem obtidas como, o nome, o número de telefone ou data de nascimento como senha.
- Utilizar um método próprio para lembrar-se da senha, de modo que ela não precise ser anotada em nenhum local, em hipótese alguma.
- Não incluir senhas em processos automáticos de acesso ao sistema, por exemplo, armazenadas em macros ou teclas de função.
- A distribuição de senhas aos usuários de TI (inicial ou não) deve ser feita de forma segura. A senha inicial, quando gerada pelo sistema, deve ser trocada, pelo usuário de TI no primeiro acesso.
- A troca de uma senha bloqueada só deve ser liberada por solicitação do próprio usuário.

8.2 Da Revisão de Controles

- As evoluções e revisões da Política de Segurança da Informação e da Política de Continuidade de Negócios são avaliadas pelos decisores na quarta reunião semanal de lideranças do mês, cujo foco é "Identificação e Mitigação de Riscos"

IX – DA SEGURANÇA TÉCNICA

9.1 Dos Encarregados pela Segurança da Informação

A responsabilidade operacional pela implementação de políticas de segurança da informação e monitoramento de riscos é o Analista de TI responsável pela alta disponibilidade de nosso software Rafael Andrade – rafael.andrade@headstecnologia.com.br

9.2. Dos Registros de Atividades

Toda e qualquer exceção necessária aos procedimentos padrão e políticas de segurança de informação, continuidade de negócios ou comunicação de incidentes, deve ser registrada através de envio de e-mail para lgpd@panosul.com.br

9.3 Da Avaliação e Gerenciamento de Riscos

A avaliação e gerenciamento de riscos em geral, incluindo aqueles mais relevantes para uma empresa de tecnologia que são os riscos relacionados à segurança da informação, são tratados com periodicidade mínima mensal e máxima bimestral na quarta reunião semanal de lideranças do mês, intitulada “Reunião de Identificação e Mitigação de Riscos”.

Os tópicos principais desta reunião ficam registrados na ata, para acompanhamento de execução das decisões tomadas.

X – DO PLANO DE RESPOSTA A INCIDENTES

No propósito de viabilizar agilidade, detecção, repressão e reparação de danos em caso de incidentes, a HIPER TÊXTIL se estrutura no seguinte formato.

10.1 Canal de Denúncias

Trata-se de veículo pelo qual eventuais vulnerabilidades, riscos ou incidentes não percebidos pela HIPER TÊXTIL poderão ser comunicados.

E-mail:lgpd@panosul.com.br

10.2 Plano de Investigação de Incidentes

Detectada uma vulnerabilidade, risco, ameaça ou incidente, o Encarregado e o responsável pela Segurança de Informação da HIPER TÊXTIL avaliarão os fatos, relatando o incidente e avaliando a extensão dos danos a fim de se apurar as medidas técnicas repressivas cabíveis, bem como as comunicações a serem promovidas a fim de minimizar e reparar danos.

10.3 Aviso de Incidentes

Em se detectando que o incidente teve gravidade média ou alta, o Encarregado providenciará a comunicação da Alta Direção e das Autoridades Cabíveis, em especial a Autoridade Nacional de Proteção de Dados Pessoais caso se note que dados de natureza pessoal tenham sido violados de qualquer forma.

10.4 Notificações a Titulares, Autoridade e eventuais Terceiros

Em sendo apurado que dados pessoais de titulares que representem algum tipo de risco, ainda que em menor grau, tenham sido violados, o Encarregado da HIPER TÊXTIL cuidará de formalizar a notificação dos titulares, disponibilizando canal para obtenção de informações adicionais e cuidando de prestar atualizações, apoio e suporte contínuo.

XI – DO PLANO DE CONTINUIDADE DOS NEGÓCIOS

Para garantir a continuidade dos negócios e das informações, a HIPER TÊXTIL mantém uma política exclusiva e específica: a Política de Continuidade de Negócios.

São tecnologias, estratégias, procedimentos padrão que somadas ao treinamento e preparo dos profissionais da empresa, que visam oferecer a seus clientes a segurança na continuidade das operações, mesmo em casos de falhas técnicas.

Obviamente, as falhas ocorridas por conta de terceiros, como em concessionárias de telefonia, de energia não são de responsabilidade da HIPER TÊXTIL. Mesmo assim, ela procura sempre colaborar decisivamente com esses fornecedores e parceiros para que o problema seja solucionado rapidamente e que seus clientes nunca sejam prejudicados por interrupções.

XII – DISPOSIÇÕES GERAIS

Em complemento às definições, princípios, diretrizes e políticas já tratadas, a HIPER TÊXTIL cuidará de observar as seguintes disposições gerais e finais.

Da Vigência

Este Programa de Governança em Proteção de Dados Pessoais e as políticas que o instruem entram em plena vigência a partir de 01 de janeiro 2023.

Autores:

Rafael Andrade, email: rafael.andrade@headstecnologia.com.br

Rafael Andrade, e:mail:rafael.andrade@headstecnologia.com.br

Brusque, 29 de novembro de 2022.