1. OBJETIVO

Direcionar com informação e conhecimento, através das políticas de segurança, os usuários de ativos e serviços da informação da Destaque, para garantia de preservação da confidencialidade, integridade e disponibilidade.

2. APLICAÇÃO

Este procedimento é aplicado a todos que utilizem ativos e serviços de informação da Destaque Gestão Documental.

3. DESCRIÇÃO

3.1 POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO - PSI

3.1.1 POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO

A DESTAQUE EMPREENDIMENTOS EM INFORMÁTICA tem como missão entregar, com descontração e interesse, soluções inteligentes e seguras para a organização de massa documental física e de material digital.

Esta política tem por proposito estabelecer diretrizes e normas de Segurança da Informação que permitam aos colaboradores e partes interessadas da DESTAQUE adotar padrões de comportamento seguro, adequados às suas metas e necessidades;

Esta política se aplica a todos os usuários da informação da DESTAQUE, incluindo qualquer indivíduo ou organização que possui ou já possuíram vínculo com a DESTAQUE, tais como prestadores de serviço, colaboradores, que possuíram, possuem ou virão a possuir acesso às informações da DESTAQUE e/ou fizeram, fazem ou farão uso de recursos computacionais compreendidos na infraestrutura DESTAQUE.

O objetivo da gestão de Segurança da Informação da DESTAQUE é garantir a gestão sistemática e efetiva de todos os aspectos relacionados à segurança da informação, provendo suporte as operações críticas do negócio e minimizando riscos identificados e seus eventuais impactos a instituição.

As violações, mesmo que por mera omissão ou tentativa não consumada desta política, bem como demais normas e procedimentos de segurança, serão passíveis de penalidades que incluem advertência verbal, advertência por escrito, suspensão não remunerada e a demissão por justa causa;

Os casos omissos serão avaliados pelo Comitê Gestor de Segurança da Informação para posterior deliberação.

As diretrizes estabelecidas nesta política e nas demais normas e procedimentos de segurança, não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças. Desta forma é obrigação do usuário da informação da DESTAQUE adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir proteção as informações da DESTAQUE.

3.1.2 POLÍTICA DE CLASSIFICAÇÃO DA INFORMAÇÃO

Para efeitos de classificação da informação, a DESTAQUE utiliza as seguintes categorias:

- Informação pública
- Informação de uso interno
- Informação confidencial

O manuseio da informação da DESTAQUE deverá obedecer às regras definidas para cada classificação.

O descarte da informação deve ser realizado de forma a impedir a recuperação da mesma, independente do seu formato de armazenamento original.

3.1.3. POLÍTICA DE CONTROLE DE ACESSO FÍSICO E DIGITAL

A DESTAQUE fornece a seus usuários autorizados contas de acesso que permitem o uso de ativos de informação, sistemas de informação e recursos computacionais como, por exemplo, rede corporativa e sistemas internos.

As senhas associadas às contas de acesso a ativos/serviços de informação ou recursos computacionais da DESTAQUE são de uso pessoal e intransferível, sendo dever do usuário zelar por sua guarda e sigilo.

A autorização e o nível permitido de acesso ativos/serviços de informação da DESTAQUE é feita com base em perfis que definem o nível de privilégio dos usuários.

São consideradas áreas restritas os locais onde informações de clientes são armazenadas e/ou manipuladas (CEDOC e Galpão).

O acesso físico aos datacenters é registrado, monitorado e arquivado. Com equipe 24/7 oferecendo suporte para responder a possíveis incidentes de segurança.

3.1.4. POLÍTICA DE PROTEÇÃO CONTRA AMEAÇAS E CÓDIGOS MALICIOSOS

A DESTAQUE disponibiliza ferramenta corporativa Kaspersky para proteção dos seus ativos/serviços de informação e recursos computacionais, incluindo estações de trabalho e dispositivos móveis, contra ameaças e códigos maliciosos tais como vírus, cavalos de Tróia, worms, ferramentas de captura de tela e dados digitados, softwares de propaganda e similares.

Mesmo com a existência de ferramentas para proteção contra códigos maliciosos, os usuários da DESTAQUE devem adotar um comportamento seguro, reduzindo a probabilidade de infecção ou propagação de códigos maliciosos.

Serviços em nuvem são atualizados e monitorados continuamente, se mantendo sempre com os últimos patches de segurança.

3.1.5. POLÍTICA DE ACESSO REMOTO

O acesso remoto a ativos/serviços de informação e recursos computacionais da DESTAQUE é restrito a usuários que necessitem deste recurso para execução das atividades profissionais, como atividade de suporte ao sistema McFile.

O acesso remoto a ativos/serviços de informação e recursos computacionais da DESTAQUE poderá ser concedido a terceiros ou prestadores de serviço, caso seja necessário para suas atividades laborais.

Toda informação que é acessada, transmitida, recebida ou produzida através do acesso remoto a ativos/serviços de informação ou recursos computacionais da DESTAQUE está sujeita monitoramento, não havendo por parte do usuário qualquer expectativa de privacidade.

Acesso à infraestrutura em nuvem deve ser liberado para IPs de colaboradores que necessitem do mesmo para exercer suas funções laborais em acesso remoto.

3.1.6. POLÍTICA DE RESPOSTAS A INCIDENTES DE SI

Todas as ocorrências que possam vir a ter impacto negativo sobre a confidencialidade, integridade ou disponibilidade dos ativos/serviços de informação ou recursos computacionais da DESTAQUE serão caracterizadas como um incidente de segurança da informação, devendo as referidas ocorrências serem tratadas de

maneira a minimizar qualquer tipo de impacto e recuperar as características de segurança da informação dos itens afetados.

Nenhum tipo de informação sobre incidentes e ocorrências de segurança da informação poderá ser divulgado para entidades ou pessoas externas à DESTAQUE sem aprovação expressa e formal do Comitê Gestor de Segurança da Informação.

Todos os incidentes de segurança da informação ou suspeitas devem ser imediatamente comunicados a área de segurança da informação seja por colaboradores, fornecedores, parceiros de negócios entre outros.

3.1.7. POLÍTICA DE USO ACEITÁVEL DOS ATIVOS DE INFORMAÇÃO

A DESTAQUE fornece para seus usuários equipamentos para o desempenho de suas atividades profissionais.

O departamento de TI poderá, a seu critério exclusivo, permitir o uso de mídias removíveis ou com capacidade de armazenamento removível a seus colaboradores para execução de atividades profissionais.

A DESTAQUE disponibiliza para seus usuários espaço para armazenamento remoto de arquivos na nuvem, através de sua solução corporativa;

O uso de equipamentos de impressão e scanner deve ser feito exclusivamente para a impressão/reprodução/digitalização de documentos que sejam de interesse da DESTAQUE ou que estejam relacionados com o desempenho das atividades profissionais do usuário.

As instalações de processamento de informações da DESTAQUE serão mantidas em áreas seguras, cujo perímetro é fisicamente isolado contra o acesso não autorizado, danos e quaisquer interferências de origem humana ou natural.

3.1.8. POLÍTICA DE USO DE E-MAIL E ACESSO À INTERNET

A DESTAQUE fornece serviços de e-mail e acesso à internet para seus usuários autorizados exclusivamente para o desempenho de suas atividades profissionais.

O serviço de e-mail e de internet da DESTAQUE é continuamente monitorado, não existindo qualquer tipo de expectativa de privacidade por parte dos usuários.

O monitoramento do serviço de e-mail e de internet da DESTAQUE tem como objetivos proteger a organização, atestar o respeito às regras de segurança da informação da empresa, bem como produzir evidências relativas à eventual violação das mesmas e/ou à legislação em vigor.

A publicação de conteúdo referente à DESTAQUE em mídias e redes sociais é feita por setores e usuários que possuem essa responsabilidade específica, sendo os demais usuários proibidos de publicar qualquer tipo de informação em nome da organização.

Não é permitida a publicação de qualquer tipo de imagem, foto, vídeo, áudio relacionado ao ambiente corporativo da DESTAQUE sem a expressa autorização da organização, excetuando-se material divulgado em canais oficiais.

3.1.9. POLÍTICA DE PROTEÇÃO DE INFORMAÇÕES PESSOAIS EM NUVEM

Após o fechamento do contrato com o cliente, durante o treinamento o responsável é informado sobre as tratativas para inclusão, alteração e/ou bloqueio de usuários. Caso o cliente solicite a exclusão de dados de PII do sistema, deverá ser formalizado através de e-mail ao suporte da ferramenta para que seja providenciada a exclusão dos dados.

A Destaque garante que as informações recebidas para execução dos serviços prestados não serão utilizadas para nenhuma outra finalidade, e garante sua confidencialidade através de contrato de sigilo firmado com colaboradores, clientes e fornecedores. Em caso de utilização das informações para marketing, a mesma só será utilizada após o aceite formal do cliente.

Os usuários são responsáveis pela limpeza dos computadores, garantindo que os arquivos e documentos temporários são apagados ou destruídos. A mesma sistemática é utilizada para os arquivos de clientes que são digitalizados e posteriormente disponibilizados no sistema McFile.

Sempre que houver acessos não autorizado às informações e, equipamentos ou instalações de processamento que resultem em perda, divulgação ou alteração de PII, a Destaque comunica o cliente em um prazo de até 24h úteis.

3.1.10. POLÍTICA DE USO E CONTROLE DE CRIPTOGRAFIA

A Destaque usa de ferramenta de segurança Kaspersky para aplicação de criptografia nos discos de máquinas Windows suportadas.

Dados em trânsito nos sites e servidores em nuvem são protegidos através do protocolo HTTPS, com certificado TLS 1.3.

Arquivos e bancos de dados são armazenados e trafegados com criptografia AES 256.

3.1.11. CAPACITAÇÃO E CONSCIENTIZAÇÃO

Os empregados, estagiários e terceiros autorizados devem ser capacitados para a utilização dos recursos de informação e para a aplicação dos conceitos de segurança, de forma a garantir

níveis adequados de confidencialidade, integridade e disponibilidade das informações da Destaque.

3.1.12. CANAL DE SUGESTÕES E DENUNCIAS

É disponibilizado urna de sugestões e denúncias para os colaboradores da Destaque. Relato deve ser feito com depósito de papel na urna e de forma anônima.

Todos as mensagens depositadas serão avaliadas mensalmente em reunião dos gestores da DESTAQUE.

3.1.13 Política de Segurança Uso de Inteligência Artificial

IA, ou Inteligência Artificial, é um campo da ciência da computação que desenvolve sistemas capazes de realizar tarefas que normalmente requerem inteligência humana, como aprender, resolver problemas e tomar decisões autônomas.

Como forma de garantir a segurança da informação na utilização dos recursos de Inteligência Artificial, é ressaltado aos colaboradores que a IA utiliza toda informação inserida como forma de aprendizado. Para isso os colaboradores são orientados nos seguintes itens: Não compartilhar informações sensíveis; Uso apropriado da ferramenta; Verificação de informações; Validação das informações; Treinamento e familiarização; Respeito às normas de propriedade intelectual; Segurança da informação; Feedback e melhoria contínua.

3.1.14 Política de Segurança Durante Desenvolvimento

Está definido dentro do escopo dessa Política, as tratativas para segurança da informação durante o processo de melhorias e adequações do sistema McFile.

Ressaltando que a Destaque é detentora de licença do fornecedor McFile com direito a alterações em seu código fonte.

Além da avaliação de risco realizada de acordo com a metodologia de avaliação de risco e tratamento de riscos, o Gestor de Tecnologia da Informação deve realizar periodicamente a avaliação dos itens:

- Os riscos relacionados a mudanças não autorizadas no ambiente de desenvolvimento
- Vulnerabilidades técnicas dos sistemas de TI utilizados no desenvolvimento
- Atualizações de ferramentas de desenvolvimento

Como forma de garantir a segurança do desenvolvimento e que não impacte na segurança do ambiente de operação, são realizados testes conforme descrito em PR Garantia da Qualidade em atualizações McFile .

4.1 GESTÃO DA SEGURANÇA

Na Destaque a gestão da Segurança da Informação ocorrerá através do SGSI – Sistema de Gestão de Segurança da Informação.

O SGSI será gerenciado pelo Comitê Gestor de Segurança da Informação, CGSI.

4.1.1 MEMBROS DO CGSI:

- Alta Direção
- Gestores

4.1.2 COMPETÊNCIAS DO CGSI:

- Difundir a cultura de Segurança da Informação;
- Propor programas de treinamento em Segurança da Informação;
- Propor projetos e iniciativas relacionados à melhoria da Segurança da Informação.

5. Formulários

6. Glossário

Ameaça: Causa potencial de um incidente, que pode vir a prejudicar a DESTAQUE;

Ativo: Tudo aquilo que possui valor para a DESTAQUE;

Ativo de informação: Patrimônio intangível da DESTAQUE, constituído por suas informações de qualquer natureza, incluindo de caráter estratégico, técnico, administrativo, financeiro, mercadológico, de recursos humanos, legal natureza, bem como quaisquer informações criadas ou adquiridas por meio de parceria, aquisição, licenciamento, compra ou confiadas a DESTAQUE por parceiros, clientes, empregados e terceiros, em formato escrito, verbal, físico ou digitalizado, armazenada, trafegada ou transitando pela infraestrutura computacional da DESTAQUE ou por infraestrutura externa contratada pela organização, além dos documentos em suporte físico, ou mídia eletrônica transitados dentro e fora de sua estrutura física.

COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO – CGSI: Grupo de trabalho multidisciplinar permanente, efetivado pela diretoria da DESTAQUE, que tem por finalidade tratar questões ligadas à Segurança da Informação.

Confidencialidade: Propriedade dos ativos da informação da DESTAQUE, de não serem disponibilizados ou divulgados para indivíduos, processos ou entidades não autorizadas.

Controle: Medida de segurança adotada pela DESTAQUE para o tratamento de um risco específico.

Disponibilidade: Propriedade dos ativos da informação da DESTAQUE, de serem acessíveis e utilizáveis sob demanda, por partes autorizadas.

Gestor da Informação: Usuário da informação que ocupe cargo específico, ao qual foi atribuída responsabilidade sob um ou mais ativos de informação criados, adquiridos, manipulados ou colocados sob a responsabilidade de sua área de atuação.

Incidente de segurança da informação: Um evento ou conjunto de eventos indesejados de segurança da informação que tem possibilidade significativa de afetar as operações ou ameaçar as informações da DESTAQUE.

Integridade: Propriedade dos ativos da informação da DESTAQUE, de serem exatos e completos.

Risco de segurança da informação: Efeito da incerteza sobre os objetivos de segurança da informação da DESTAQUE.

Segurança da informação: A preservação das propriedades de confidencialidade, integridade e disponibilidade das informações da DESTAQUE.

Usuário da informação: Empregados com vínculo empregatício de qualquer área da DESTAQUE ou terceiros alocados na prestação de serviços a DESTAQUE, indiferente do regime jurídico a que estejam submetidos, assim como outros indivíduos ou organizações devidamente autorizadas a utilizar ou manipular qualquer ativo de informação da DESTAQUE para o desempenho de suas atividades profissionais.

Vulnerabilidade: Causa potencial de um incidente de segurança da informação, que pode vir a prejudicar as operações ou ameaçar as informações da DESTAQUE.

7. Histórico de Alterações

DATA	REVISÃO	HISTÓRICO
14/10/2020	01	Aprovação do procedimento
07/12/2020	02	Adição de política de segurança de uso e controle criptografia
19/12/2024	03	Adição de política de segurança uso de inteligência artificial e política de segurança durante desenvolvimentos