Leograf Gráfica e Editora Ltda.

Política de Segurança da Informação

Versão 6.0 - 01 de setembro de 2020

INFORMAÇÕES CONFIDENCIAIS

Conteúdo

1 Objetivo

Este documento tem como objetivo explicar e estabelecer os requisitos de segurança da informação da Leograf Gráfica e Editora Ltda. para todos os colaboradores, prestadores de serviços e parceiros. A administração da organização adotou esta política de segurança para proteger a informação com o objetivo de atingir suas metas comerciais ou de conformidade com normas e leis aplicáveis.

2 Classificação do documento e alvo

Esta política se aplica a todos os colaboradores, prestadores de serviço e parceiros que utilizam, mantêm ou lidam com ativos de informação da organização.

3 Comitê de Segurança da Informação

O Comitê de Segurança da Informação tem por objetivo auxiliar na criação e revisão de políticas, normas e procedimentos gerais relacionados à segurança da informação. O comitê é formado por um grupo de gestores dos departamentos de Qualidade, Treinamentos, Tecnologia da Informação, Inkjet (dados variáveis) e Diretoria.

É responsabilidade do Comitê garantir a segurança da informação, a preservação dos ativos, a garantia de execução dos processos minimizando e mitigando riscos à organização. Para cumprimento deste propósito devem acontecer reuniões semestrais, exceto se convocadas por algum dos membros por demanda emergencial. As atas das reuniões serão assinadas por todos os membros presentes e arquivadas no departamento de Tecnologia da Informação.

O Comitê possui autonomia para debater e/ou recomendar quaisquer aspectos relacionados à segurança da informação, oferecendo subsídio à Diretoria no processo de tomada de decisão.

Caso haja necessidade, podem ser formadas comissões específicas para debater alterações dentro dos procedimentos contidos nesta política.

4 Responsabilidades dentro da Política de Segurança da Informação

4.1. Organizando a Segurança da Informação

Constitui-se nesta política a responsabilidade ao departamento de Tecnologia da Informação, conjuntamente com o Comitê de Segurança da Informação, de assegurar a seleção de controles de segurança adequados para proteger os ativos de informação e proporcionar confiança ao negócio onde a organização atua.

4.2. Papeis e Responsabilidades da Segurança da Informação

4.2.1 Gerente de Infraestrutura e Segurança

O Gerente de Infraestrutura e Segurança é responsável por coordenar e supervisionar o cumprimento das políticas e procedimentos em toda a organização no tocante à confidencialidade, integridade e segurança de seus ativos de informação.

O Gerente de Infraestrutura e Segurança trabalha juntamente com colaboradores da organização envolvidos em proteger os ativos de informação para aplicar as políticas definidas, identificar as áreas de atenção e implantar mudanças apropriadas de acordo com as necessidades. As responsabilidades especificas do Gerente de Infraestrutura e Segurança incluem:

Responsabilidades do Gerente de Infraestrutura e Segurança

- Tomar decisões de alto nível pertinentes às Políticas de Segurança da Informação e seu conteúdo. Aprovar, antecipadamente, exceções a estas políticas com base em análise caso-a-caso.
- Coordenar, anualmente, uma verificação de risco formal para identificar novas ameaças e vulnerabilidades e identificar controles apropriados para minimizar qualquer novo risco.
- Rever anualmente as políticas e procedimentos de segurança da informação para manter a adequação face às emergentes necessidades de negócio ou ameaças à segurança.
- Manter atualizado o Plano de Resposta a Incidentes conforme definido nesta política.
- Realizar as convocações para reuniões ordinárias do Comitê de Segurança de Informação.
- Completar as tarefas de acordo com os Procedimentos Periódicos de Segurança Operacional.
- Monitorar e analisar alertas de segurança e distribuir informações ao pessoal apropriado de segurança, técnico e da administração da unidade de negócios.
- Aplicação das políticas e procedimentos de segurança da informação de acordo com sua aplicabilidade a todos os ativos de informação.
- Administração das contas de usuários e gerenciamento de autenticação.

4.2.2 Premissa de Segurança da Informação

A proteção bem sucedida dos sistemas da organização requer que vários departamentos e grupos sigam consistentemente uma visão compartilhada de segurança.

O Comitê de Segurança da Informação trabalha com os gerentes, administradores e usuários de sistemas dos departamentos no desenvolvimento de políticas, normas e procedimentos de segurança para garantir a proteção dos ativos da organização.

O Comitê de Segurança da Informação possui a responsabilidade sobre o planejamento, a educação e a conscientização sobre o tema da segurança da informação. As responsabilidades específicas do Comitê de Segurança da Informação incluem:

Responsabilidades do Comitê de Segurança da Informação

- Criar novas políticas e procedimentos de segurança da informação quando necessário. Manter e atualizar políticas e procedimentos de segurança da informação existentes. Rever anualmente as políticas e auxiliar a administração com o processo de aprovação.
- Atuar pró-ativamente para implantação das políticas de Segurança da Informação.
- Criar e manter procedimentos de resposta a incidentes.
- Restringir e monitorar o acesso a áreas restritas e informação confidencial. Assegurar que os controles adequados estejam disponíveis onde houver informações confidenciais.

4.2.3 Departamento de Recursos Humanos

Devido ao seu relacionamento direto e constante com os funcionários, assim como sua posição única de ter a primeiras e últimas interações com todos os colaboradores, o Departamento de Recursos Humanos tem um papel importante no que se referem à segurança das informações dentro da organização, sendo os seguintes itens de sua responsabilidade:

Responsabilidades do Recursos Humanos

- Auxiliar o Comitê de Segurança da Informação com a publicação e divulgação das políticas de Segurança da Informação e orientação sobre o uso aceitável a todos os usuários de sistema relevantes incluindo prestadores de serviço.
- Trabalhar com o Comitê de Segurança da Informação na disseminação de informações de conscientização sobre segurança, utilizando diversos métodos de comunicação, de conscientização e educação dos funcionários (ex. pôsteres, cartas, memorandos, treinamento via web, reuniões, etc.).
- Trabalhar com o Comitê de Segurança da Informação para administrar sanções e ações disciplinares referentes a violações da Política de segurança da informação.
- Notificar o Departamento de Tecnologia da Informação quando qualquer funcionário for contratado ou desligado.

4.2.4 Departamento de Treinamentos

Devido à necessidade constante por capacitação e conscientização dos colaboradores, o Departamento de Treinamentos deve atuar realizando treinamentos conforme as responsabilidades descritas a seguir:

Responsabilidades do Departamento de Treinamentos

- Certificar–se de que os funcionários que são impactados e/ou lidam diretamente com os temas abordados nesta política recebam o treinamento adequado para execução de suas tarefas.
- Registrar os treinamentos realizados por meio de controles de presença.
- Desenvolver metodologias adequadas objetivando os resultados esperados dos treinamentos.
- Avaliar a eficácia dos treinamentos por meio de avaliações de satisfação dos colaboradores.

4.2.5 Usuários

Todos os usuários de recursos computacionais e de informação da organização devem estar cientes da importância fundamental de tais recursos e reconhecer sua responsabilidade pela manutenção segura dos mesmos. Os usuários devem protegê-los contra abusos que interrompam ou ameacem a viabilidade de todos os sistemas. As seguintes responsabilidades são específicas a todos os usuários de sistemas computacionais da organização:

Responsabilidades dos Usuários

- Entender as consequências de suas ações relacionadas às práticas de segurança computacional e agir de forma condizente. Aceitar a filosofia de que “Segurança é responsabilidade de todos" auxiliando a organização a garantir a preservação de seus ativos e sistemas.
- Manter-se cientes sobre o conteúdo das políticas de Segurança da Informação.
- Ler e assinar a o termo de confidencialidade das informações que lhes forem confiadas em razão de sua atividade profissional.
- Agir constantemente de forma a seguir as classificações de confidencialidade dos ativos de informação da organização, de acordo com a Política de Gestão de Ativos.

4.3. Segregação de Funções

Para todos os ambientes da organização, sejam eles de produção ou desenvolvimento, é obrigatória a implementação de segregação de funções. A segregação de funções determina que funções conflitantes e áreas de responsabilidade sejam segregadas para reduzir as oportunidades de modificação não autorizada, coibindo o mau uso dos ativos da organização intencional ou não intencionalmente. Para casos de exceção, seja por limitação técnica ou de negócio, é obrigatório o uso de controles adicionais de segurança e a aprovação do Gerente de Infraestrutura e Segurança.

4.4. Contato com as Autoridades Externas

Como parte do processo de comunicação interno e externo e do plano de resposta a incidentes de segurança da informação da organização, declara-se que qualquer comunicação relacionada à segurança da informação, junto às autoridades externas que incluem, mas não se limitam a entidades reguladoras, entidades de conformidade e governo, devem ser previamente autorizadas pela Diretoria.

4.5. Segurança da Informação no Gerenciamento de Projetos

Como parte da metodologia de gerenciamento de projetos da organização, recomenda-se que os projetos incluam a segurança da informação dentro do seu ciclo de vida. A inclusão tem como objetivo avaliar os riscos de segurança da informação, bem como propor controles adequados e acrescentar aos objetivos do projeto, aspectos de segurança de informação.

4.6. Conformidade Legal

Todos os ativos e sistemas de informação organização, assim como os seus funcionários e prestadores de serviço devem estar em conformidade com as obrigações legais, estatutárias, regulamentares ou contratuais relacionadas à segurança da informação estabelecido pela organização.

Com objetivo de prevenir violações, todas as informações armazenadas ou que trafeguem dentro dos perímetros físicos e lógicos da organização podem ser monitoradas, mediante o processo de aprovação instituído, revisado pelo Comitê de Segurança da Informação. Violações não serão toleradas e as sanções apropriadas serão aplicadas.

5 Seções da Política de Segurança da Informação

5.1. Política de Gestão de Ativos

Todos os ativos físicos e de informação da organização deverão ser classificados de acordo com o seu nível de confidencialidade, disponibilidade, integridade e controles legais. Uma vez classificados, devem ser respectivamente relacionados ao modo como são acessados, armazenados, movimentados e por fim descartados. Para detalhes e informações adicionais, consulte a Política de Segurança da Informação - Gestão de Ativos.

5.2. Política de Controle de Acesso

Todos os sistemas de informação da organização devem estar integrados a um sistema de controle de acesso definido pelo Departamento de Tecnologia da Informação.

A concessão de acessos (recursos ou sistemas) devem ser aprovados pelo gestor da informação. Além disso, deve ser instituída a segregação de função de acordo com nível funcional ou responsabilidade assim como uma revisão periódica dos acessos concedidos, a fim de evitar acessos indevidos. Para mais informações, consulte a Política de Segurança da Informação - Controle de Acesso.

5.3. Política de Criptografia

Quando pertinente, as informações da organização ou de parceiros e clientes que precisem ser protegidas contra acesso não autorizado ou estabelecido por normas externas ou internas de conformidade devem ser criptografadas conforme os padrões alinhados e definidos entre o responsável pela informação e seu detentor, de modo a garantir sua a confidencialidade, autenticidade e integridade. Para mais informações, consulte a Política de Segurança da Informação - Criptografia.

5.4. Política de Segurança Física e do Ambiente

É necessário estabelecer o perímetro de segurança física de modo a preservar o acesso somente a pessoas autorizadas. Além disso, deve ser instituído de modo obrigatório o uso de identificação visual (crachá) para visitantes, clientes, fornecedores e prestadores de serviço. Para controle e liberação de acesso de colaboradores, deve-se utilizar sistema de registro de acesso físico por meio de sistemas de catracas, torniquetes e biometria. Para mais informações, consulte a Política de Segurança da Informação - Segurança Física e do Ambiente.

5.5. Política de Gestão de Operações

O Departamento de Tecnologia da Informação, conjuntamente com o Comitê de Segurança da Informação, deve estabelecer as diretrizes para garantir a operação segura e correta dos recursos de processamento da informação. Para isso deve estabelecer procedimentos operacionais documentados e acessíveis aos usuários necessários.

Estes procedimentos operacionais devem incluir e não se limitar a, procedimentos de instalação e configuração de sistemas, procedimentos para manipulação de informação, procedimentos de cópias de segurança (backup) e procedimentos para gerenciamento de falhas de produção.

Para mais informações, consulte a Política de Segurança da Informação - Segurança de Operações.

5.6. Política de Gestão de Mudanças

Deve ser estabelecido um processo único de gestão de mudanças com o objetivo de controlar e garantir a autorização e documentação de toda mudança no ambiente que possa impactar no fluxo de processos da organização. Para mais informações, consulte a Política de Segurança da Informação - Gestão de Mudanças.

5.7. Política de Segurança nas Comunicações

O Departamento de Tecnologia da Informação, conjuntamente com o Comitê de Segurança da Informação, deve estabelecer as diretrizes para garantir a proteção das informações em redes e dos recursos de processamento da informação que as apoiam. Para isso deve estabelecer procedimentos operacionais documentados e acessíveis aos usuários necessários, que estabeleçam as responsabilidades e procedimentos sobre o gerenciamento de equipamentos de rede. Para mais informações, consulte a Política de Segurança da Informação - Segurança nas Comunicações.

5.8. Política Gestão de Sistemas da Informação e Infraestrutura

Todos os processos que envolvam aquisição, desenvolvimento ou manutenção de sistemas de informação ou alteração na infraestrutura da organização devem ser comunicados ao Departamento de Tecnologia da Informação, garantindo que os riscos relacionados sejam conhecidos e tratados. Para mais informações, consulte a Política de Segurança da Informação - Gestão de Sistemas da Informação e Infraestrutura.

5.9. Política de Gestão de Incidentes de Segurança da Informação

O processo de gestão de incidentes de segurança da informação tem como objetivo garantir que eventos de segurança da informação associados a ativos de informação da organização sejam comunicados ao Departamento de Tecnologia da Informação.

É de responsabilidade do Departamento de Tecnologia da Informação coordenar todas as atividades pertinentes ao processo de gestão de incidentes de segurança da informação. É dever de todos os usuários comunicar um incidente de segurança da informação para área responsável. Para mais informações, consulte a Política de Segurança da Informação - Gestão de Incidentes.

6 Regulamentos Externos

ISO 27000

7 Anexos

- Política de Controle de Acesso
- Política de Criptografia
- Política de Gestão de Ativos
- Política de Gestão de Incidentes de Segurança da Informação

- Política de Gestão de Mudanças
- Política de Gestão de Operações
- Política de Segurança Física e do Ambiente
- Política de Segurança nas Comunicações
- Política de Sistemas de Informação e Infraestrutura
- Politica de Mesa/Tela Limpa

8 Histórico de Revisões

Abaixo se encontra a tabela com o histórico de revisões deste documento.

REVISÃO	ELABORADO POR	REVISADO POR	APROVADO POR	DATA DA APROVAÇÃO
2.0	Priscila/Monica	R.Polito/Marcelo	Ricardo Barros	03/05/2016
3.0	Daniel/Marcelo	R.Polito/Priscila	Ricardo Barros	09/10/2017
4.0	Daniel/Marcelo	R.Polito/Priscila	Ricardo Barros	14/09/2018
5.0	Daniel/Marcelo	R.Polito	Ricardo Barros	20/09/2019
6.0	Daniel/Marcelo	R. Polito	Ricardo Barros	20/09/2020

Este termo deve ser assinado e arquivado no prontuário do colaborador.

TERMO DE CIÊNCIA E COMPROMETIMENTO

Via da Empresa

Recebi o Manual PSI – Política de Segurança da Informação, cujo propósito é esclarecer a política da empresa e os padrões de comportamentos esperados de seus colaboradores.

Comprometo-me a cumpri-lo integralmente e dar ciência do não cumprimento por terceiros e em casos de dúvidas, consultar meus superiores ou o Comitê de Segurança da Informação.

Li e compreendi,

_____

Nome

_____

Assinatura do Colaborador

Local: São Paulo, Data _____/_____/ 20___.

TERMO DE CIÊNCIA E COMPROMETIMENTO

Via do Colaborador

Recebi o Manual PSI – Política de Segurança da Informação, cujo propósito é esclarecer a política da empresa e os padrões de comportamentos esperados de seus colaboradores.

Comprometo-me a cumpri-lo integralmente e dar ciência do não cumprimento por terceiros e em casos de dúvidas, consultar meus superiores ou o Comitê de Segurança da Informação.

Li e compreendi,

_____

Nome

_____

Assinatura do Colaborador

Local: São Paulo, Data _____/_____/ 20___.

PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

TÍTULO: SEGURANÇA NAS COMUNICAÇÕES

HISTÓRICO DAS REVISÕES

Revisão Nº	Data	Descrição da Revisão
00	01/09/2017	Elaboração do documento
01	14/09/2018	Revisão 01
02	01/09/2019	Revisão 02
03	01/09/2020	Revisão 03

CONTEÚDO

DISTRIBUIÇÃO

Conforme Lista Mestre – documentos de segundo nível.

REVISÃO	ELABORADO POR	REVISADO POR	APROVADO POR	DATA DA APROVAÇÃO
03	Daniel Almeida Marcelo Schwed	Ricardo Polito	Ricardo Barros	10/09/2020

1 OBJETIVO

Este documento tem como objetivo destacar a importância da comunicação como um processo estratégico de gestão que permeia todas as ações da Leograf Gráfica e Editora Ltda.

Sistematizar todas as ações, produtos, fluxos e processos de comunicação em vigor ou a serem implementados na organização, tendo em vista incrementar e qualificar a interação com os seus respectivos públicos.

Padronizar diretrizes, condutas, posturas, valores e princípios de modo a garantir coerência e eficácia no processo de comunicação interno e externo.

2 DESCRIÇÃO

2.1 Aplicação

Esta política se aplica a todos os colaboradores, prestadores de serviço e parceiros que mantem negócios com a organização.

2.2 Seções da política e responsabilidades

2.2.1 Processo de Comunicação

Toda a comunicação interna e externa da organização deve ser realizada seguindo as seguintes diretrizes:

Clareza: As informações devem ser passadas de maneira clara evitando duplo sentido;

Formalidade: Toda a comunicação deve ocorrer de maneira formal e profissional;

Objetividade: Para o efetivo processo de comunicação, não devem ser abordados assuntos distintos no mesmo meio de comunicação ao mesmo tempo;

Relevância: As informações só devem ser repassadas às partes que estão diretamente relacionadas ao conteúdo da mensagem;

Sensibilidade: As informações devem ser ajustadas para garantir que os interlocutores do processo obtenham o mesmo grau de entendimento sobre o respectivo assunto.

A comunicação Institucional externa deve ser realizada e/ou aprovada pelo Departamento de Marketing com ciência da Diretoria.

2.2.2 Mensagens Eletrônicas

Para o uso adequado das ferramentas eletrônicas da organização, todos os funcionários devem seguir as orientações abaixo:

Todos os Sistemas de Comunicação Eletrônica utilizados nas operações da organização são de propriedade da Leograf Gráfica e Editora Ltda, bem como todas as mensagens neles armazenadas para uso corporativo.

As mensagens devem ser limitadas apenas às necessidades da operação dos negócios da organização.

O conteúdo das mensagens não pode possuir elementos que possam ser considerados ofensivos, destrutivos, difamatórios ou pejorativos, incluindo, mas não limitado a comentários ou imagens sexuais, calúnias raciais, ou outros comentários ou imagens que possam ofender a alguém por sua raça, nacionalidade, gênero, orientação sexual, crença religiosa, orientação política ou restrição física.

2.2.3 Direitos de Propriedade

É proibido carregar ou descarregar de sistemas internos ou de terceiros, material sujeito às leis de direito autoral ou classificados como confidenciais, sem autorização escrita por parte da organização.

Materiais sujeitos às leis de direito autoral, classificados como shareware ou freeware podem ser utilizados para os propósitos designados pelo detentor do respectivo direito autoral.

2.2.4 Direito de Privacidade

Caso não seja diretamente mencionado, não se deve assumir que qualquer mensagem seja privativa. Apesar da característica dos sistemas darem uma aparência de privacidade, incluindo senhas e a possibilidade de se apagar as mensagens, não sendo necessariamente privativas por duas razões: os Sistemas de Comunicação Eletrônica podem não ser seguros, pois a segurança dos arquivos eletrônicos de sistemas compartilhados em redes é, frequentemente, semelhante ao de um documento em um envelope não lacrado, geralmente respeitado, porém facilmente lido por alguém determinado a fazê-lo. Deve-se assumir que as mensagens podem ser ouvidas ou lidas por alguém que não seja o destinatário. Mesmo quando uma mensagem é apagada, está ainda pode ter uma cópia de segurança (backup) em algum lugar, ou é passível de ser recuperada.

As mensagens podem ser auditadas pela organização a qualquer momento conforme as diretrizes de monitoramento descritas nesta política.

2.2.5 Direito de Monitoramento

A organização se reserva ao direito de monitorar, acessar, recuperar e ler todas as mensagens, divulgando qualquer uma para as autoridades judiciais e policiais e terceiros caso considere necessário, sem aviso prévio ao remetente ou destinatário da mensagem.

Funcionários que têm sob sua responsabilidade profissional a integridade e segurança de dados podem revisar as mensagens recebidas ou enviadas por qualquer funcionário, desde que para os seguintes propósitos:

- Identificar e diagnosticar problemas de hardware ou software;
- Evitar má utilização dos sistemas;
- Determinar se houve violação de confidencialidade, segurança ou violação desta política;
- Investigar má conduta ou atividades não éticas, ilegais ou não apropriadas;
- Garantir o cumprimento dos direitos autorais, obrigações contratuais e licenças;
- Cumprir com as obrigações legais às quais a Organização está sujeita;
- Cumprir as requisições legais e regulamentadas de informações e proteger os interesses comerciais da Organização.

Nenhum outro tipo de monitoramento ou revisão pode ser feita sem a prévia aprovação da Diretoria da organização.

2.2.6 Boas Práticas de Comunicação

A Organização não autoriza a utilização de mensagens eletrônicas com as seguintes descrições:

- Linguagem que possa ser considerada ofensiva, destrutiva, difamatória ou pejorativa.
- Para fins pessoais (mensagens para amigos e familiares, cadastro em site da internet, passar mensagens a outros funcionários que não sejam relacionadas ao trabalho).
- Manter nos computadores da organização cópias ou instalação de programas que não sejam licenciados e que não estejam relacionados com os negócios.
- Divulgação ou compartilhamento de senha e/ou identificação de usuário com outras pessoas.
- Deixar seu computador sem supervisão quando estiver acessando a rede.

2.2.7 Falhas de Comunicação

Caso o funcionário receba mensagens eletrônicas com conteúdo que não esteja relacionado à sua atividade, deverá deletá-la e notificar à pessoa que enviou a mensagem sobre o erro.

Caso a pessoa insista em enviar mensagens de conteúdo inadequado, o funcionário deverá comunicar ao seu gestor sobre o problema para que as providencias sejam tomadas. O uso indevido do Sistema de Comunicação Eletrônica pode resultar em ação disciplinar, incluindo dispensa. O código de ética da organização deve mencionar as normas sobre a utilização de mensagens eletrônicas e dos recursos eletrônicos. Não é permitida a configuração de qualquer e-mail diferente do domínio *leograf.com.br* nos computadores da organização.

PSI – POLITICA DE SEGURANÇA DA INFORMAÇÃO

TÍTULO: CONTROLE DE ACESSO

HISTÓRICO DAS REVISÕES

Revisão Nº	Data	Descrição da Revisão
00	18/10/2017	Elaboração do documento
01	14/09/2018	Revisão 01
02	01/09/2019	Revisão 02
03	01/09/2020	Revisão 03

CONTEÚDO

DISTRIBUIÇÃO

Conforme Lista Mestre – documentos de segundo nível.

REVISÃO	ELABORADO POR	REVISADO POR	APROVADO POR	DATA DA APROVAÇÃO
03	Daniel Almeida Marcelo Schwed	Ricardo Polito	Ricardo Barros	10/09/2020

1 OBJETIVO

Este documento tem como objetivo explicar e estabelecer os requisitos de segurança da informação relacionados ao controle de acesso dos colaboradores e prestadores de serviço que utilizam as redes da organização.

A administração da organização adotou esta política para assegurar que todos os colaboradores, prestadores de serviço, fornecedores e outros parceiros estejam cientes dos seus papéis e responsabilidades em relação às permissões de acesso dentro da organização.

2 DEFINIÇÕES E ABREVIATURAS

TI – Tecnologia da Informação

3 DESCRIÇÃO

3.1 Aplicação

Esta política se aplica a todos os colaboradores, prestadores de serviço e parceiros que possuem acesso às redes internas da Organização.

3.2 Seções da política e responsabilidades

3.2.1 Gestão de Contas

Todos os colaboradores que necessitam de um acesso à rede interna da organização possuem uma conta com determinado nível de acesso vinculado ao departamento no qual estão inseridos. Esta conta é utilizada para acessar os compartilhamentos e *softwares* relacionados com a sua rotina de trabalho.

Todos os colaboradores que possuem contam recebem acesso a um e-mail corporativo que será utilizado para comunicação interna e externa a serviço da organização.

Toda conta de usuário dentro ambiente da organização está inclusa em uma unidade organizacional (*Organizational Unit*) que possui regras de acesso e direitos departamentais aos volumes compartilhados na rede, que por sua vez estão dentro das regras de acesso e direitos gerais dos domínios “leograf.local” ou “inkjetsys.local”.

Os usuários dos domínios “leograf.local” ou “inkjetsys.local” não possuem direitos de acesso entre domínios, sendo parte única e exclusiva de cada domínio.

3.2.2 Liberação de direito de acesso

Após o processo de seleção e contratação de novos colaboradores, o departamento de Recursos Humanos encaminha um e-mail ao Departamento de TI, no qual solicita

a liberação de acessos e ativos necessários para o exercício de suas funções profissionais.

Esta solicitação é direcionada por meio do sistema de gestão de incidentes e chamados, denominado *Zendesk,* com o qual o departamento de TI gerencia as solicitações conforme descrito na Política de Gestão de Incidentes de Incidentes de Segurança da Informação. Este gerenciamento deverá ser realizado classificando a solicitação por meio de *tags* e atribuindo responsabilidade de execução entre os colaboradores do setor de TI.

3.3 Revogação de direito de acesso

Durante o processo de desligamento dos colaboradores, o departamento de Recursos Humanos encaminha um e-mail ao Departamento de TI, no qual solicita a revogação de acessos e devolução de ativos utilizados durante exercício de suas funções profissionais.

Esta solicitação é direcionada por meio do sistema de gestão de incidentes e chamados, denominado *Zendesk,* com o qual o departamento de TI gerencia as solicitações, conforme Política de Gestão de Incidentes de Segurança da Informação. Este gerenciamento deverá ser realizado classificando a solicitação por meio de *tags* e atribuindo responsabilidade de execução entre os colaboradores do setor de TI.

3.3.1 Alteração de direitos e acesso

Os acessos às informações e aos recursos de processamento da informação são liberados, alterados ou revogados conforme a solicitação da gerência ou responsável pelo departamento. Nas ocorrências em que o acesso às informações solicitadas pertencer a outro departamento, o gerente ou responsável pela informação deve também autorizar, alterar, revogar ou impedir o acesso. Toda solicitação deve ser formalizada por e-mail direcionado ao endereço departamento de TI.

3.3.2 Liberação de acessos temporários

Em função da necessidade de acesso às redes internas da organização para a execução de trabalhos ou prestação de serviços específicos, o departamento de TI disponibiliza uma conta de acesso temporário, com duração padrão de 24h. Este acesso pode ser encerrado ou prorrogado mediante identificação de necessidade pelo departamento requisitante em função da atividade desenvolvida.

3.4 Gerenciamento de Usuário e Senha

O Departamento de TI é responsável por manter as diretrizes de senhas nos computadores, servidores e sistemas. Também é responsável por orientar os usuários no cadastramento de novas senhas.

A senha é de responsabilidade do usuário, de uso pessoal e intransferível, não sendo permitido o seu compartilhamento. A mesma poderá ser alterada a qualquer momento ou caso seja identificada uma falha de segurança.

Caso o usuário necessite de auxílio para alterar a senha, o Departamento de TI deve ser acionado. Na ocorrência de algum usuário identificar que outro usuário esteja compartilhando a senha, o mesmo deve comunicar por e-mail ao Departamento de TI. Não é permitido o uso e cadastro de usuário genérico ou padrão para acesso à internet, a rede e a sistemas.

A construção da senha do usuário deverá ser realizada seguindo as seguintes recomendações:

- Comprimento mínimo de 8 caracteres;
- Possuir 2 caracteres maiúsculos, 2 caracteres minúsculos, 2 caracteres especiais e 2 números;
- Diferir das 6 ultimas senhas utilizadas;
- As senhas deverão ser trocadas a cada 180 dias;
- Utilizar senhas de fácil memorização.

3.5 Requisição e devolução de ativos

Os ativos de informática da organização devem ser solicitados através de um e-mail pela gerência ou responsável do departamento, direcionado ao Departamento de TI. A devolução dos ativos de informática ocorre nos casos de quebra, descontinuidade do ativo, alteração de função, desligamento do funcionário ou encerramento de contrato de fornecedor ou prestador de serviço. Em caso de desligamento do funcionário, o Departamento de TI deve ser informado pela gerência ou responsável do departamento de Recursos Humanos através de um e-mail para solicitar quais ativos devem ser devolvidos.

3.6 Termo de Confidencialidade

Todos os funcionários devem assinar o documento “Termo de Confidencialidade e Responsabilidade” fornecido pelo Departamento de Recursos Humanos no ato da contratação. Nos contratos de clientes e fornecedores firmados com a organização deve obrigatoriamente constar uma cláusula de confidencialidade. Todos os contratos devem ser validados pelo departamento jurídico da organização.

4 ANEXOS

- Política de Gestão de Incidentes de Segurança da Informação
- Procedimento de Contratação
- Procedimento de Desligamento
- Termo de Confidencialidade e Responsabilidade para colaboradores

- Termo de Confidencialidade

PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

TÍTULO: CRIPTOGRAFIA

HISTÓRICO DAS REVISÕES

Revisão Nº	Data	Descrição da Revisão
00	01/09/2017	Elaboração do documento
01	14/09/2018	Revisão 01
02	01/09/2019	Revisão 02
03	01/09/2020	Revisão 03

CONTEÚDO

DISTRIBUIÇÃO

Conforme Lista Mestre – documentos de segundo nível.

REVISÃO	ELABORADO POR	REVISADO POR	APROVADO POR	DATA DA APROVAÇÃO
03	Daniel Almeida Marcelo Schwed	Ricardo Polito	Ricardo Barros	10/09/2020

1 OBJETIVO

Definir os métodos e procedimentos ao uso de criptografia no armazenamento de arquivos contendo dados confidenciais, seja eles de propriedade da Leograf Gráfica e Editora Ltda., clientes e parceiros no ambiente de desenvolvimento da rede “inkjetsys.local”.

2 DEFINIÇÕES E ABREVIATURAS

TI – Tecnologia da Informação

3 DESCRIÇÃO

3.1 Aplicação

Esta política se aplica a todos os colaboradores, prestadores de serviço e parceiros que utilizam, mantêm ou lidam com ativos de informação da organização devem seguir esta política.

3.2 Seções da política e responsabilidades

3.2.1 Regras Gerais de Utilização

Os controles criptográficos serão usados para assegurar a confidencialidade, a integridade e a autenticidade de informações críticas que se encontrem armazenadas, sob processo de transporte físico ou de transmissão eletrônica.

A escolha dos tipos, da qualidade e da força de algoritmos, assim como a definição de que tipo de controle criptográfico é apropriado para cada propósito e processo de negócio, tomará como base, sempre que possível, a necessidade e/ou definição pelo cliente e proprietário do ativo de informação.

A comunicação entre o proprietário da informação com o responsável pela detenção das informações criptografadas ocorre de maneira direta entre partes para disponibilização da chave de acesso, softwares e parâmetros de criptografia.

É proibida a implantação de controles criptográficos não autorizados pelo cliente ou pelo Departamento de Inkjet ou utilizá-los de forma distinta aos procedimentos estabelecidos para tal finalidade.

3.2.2 Responsabilidades

Compete ao Departamento de TI deliberar sobre os procedimentos de utilização e aplicação de criptografia na organização quando solicitado pelo cliente.

Compete aos proprietários e custodiantes de ativos de informação aplicar adequadamente os recursos criptográficos identificados para a proteção da informação sobre sua custódia, em conformidade com as determinações desta norma.

3.3 Procedimento de Criptografia

Quando o cliente solicita a criptografia após a transferência do ativo de informação, devem-se realizar as seguintes etapas:

- Determinar algoritmo de criptografia a ser utilizada conjuntamente com o cliente.
- O cliente deve definir a chave criptográfica
- Executar a cifração dos arquivos
- Informar proprietário da informação sobre o processo realizado
- Encaminhar chave ao proprietário ou ao responsável que utilizará os dados, quando solicitado.

Quando os dados são transferidos criptografados para os servidores da organização, deve-se realizar as seguintes etapas:

- Recebimento do ativo de informação criptografado por meio de comunicação segura
- Recebimento da chave criptográfica por outro meio
- No momento da utilização da informação realizar a decifração do ativo de informação

Após a utilização recrifrar o arquivo.

4 GLOSSÁRIO

Algoritmo: função matemática utilizada na cifração e na decifração de informações restritas.

Algoritmo Assimétrico: função matemática que utiliza chaves criptográficas distintas para cifração e decifração de informações restritas.

Algoritmo Simétrico: função matemática que utiliza a mesma chave criptográfica tanto para a cifração quanto para a decifração de informações restritas.

Ativo de Informação: os meios de armazenamento, transmissão e processamento da informação; os equipamentos necessários a isso; os sistemas utilizados para tal; os locais onde se encontram esses meios, e também as pessoas que a eles têm acesso.

Autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade.

Cifração: ato de cifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para substituir sinais de linguagem em claro, por outros ininteligíveis por pessoas não autorizadas a conhecê-la.

Chave ou chave criptográfica: valor que trabalha com um algoritmo criptográfico para cifração ou decifração.

Controle criptográfico: sistema, programa, processo, equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração.

Credencial: permissões, concedidas por gestor competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física como crachá, cartão e selo ou lógica como identificação de usuário e senha.

Credenciamento: processo pelo qual o usuário recebe credenciais que concederão o acesso, incluindo a identificação, a autenticação, o cadastramento de código de identificação e definição de perfil de acesso em função de autorização prévia e da necessidade de conhecer.

Custodiante de ativo de informação: refere-se a qualquer indivíduo ou unidade da organização que tenha a responsabilidade formal de proteger um ou mais ativos de informação. Ele é responsável por aplicar os níveis de controles de segurança em conformidade com as exigências de segurança da informação comunicadas pelos proprietários dos ativos de informação.

Decifração: ato de decifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para reverter processo de cifração original.

Informação restrita: toda a informação que deva ser mantida em sigilo por tempo determinado, com acesso restrito a um grupo credenciado de pessoas que tenham necessidade de conhecê-la, conforme determinado por Lei, norma de classificação da informação e procedimentos de tratamento da informação.

Proprietário de ativo de informação: refere-se à parte interessada da unidade da organização, indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação.

VPN: Virtual Private Network. Rede privada construída sobre uma infraestrutura de rede pública, com recursos para proteção dos dados transmitidos contra interceptações e capturas.

5 ANEXOS

- Controles Criptográficos

PSI – POLITICA DE SEGURANÇA DA INFORMAÇÃO

TÍTULO: GESTÃO DE ATIVOS

HISTÓRICO DAS REVISÕES

Revisão Nº	Data	Descrição da Revisão
00	19/09/2017	Elaboração do Documento
01	14/09/2018	Revisão 01
02	01/09/2019	Revisão 02
03	01/09/2020	Revisão 03

CONTEÚDO

DISTRIBUIÇÃO

Conforme Lista Mestre – documentos de segundo nível.

REVISÃO	ELABORADO POR	REVISADO POR	APROVADO POR	DATA DA APROVAÇÃO
03	Daniel Almeida Marcelo Schwed	Ricardo Polito	Ricardo Barros	10/09/2020

1 OBJETIVO

Este documento tem como objetivo explicar e estabelecer os requisitos de segurança para: identificar os ativos, sejam físicos ou lógicos, da Leograf Gráfica e Editora Ltda. e definir as devidas responsabilidades pela gestão dos mesmos. Esta política também visa assegurar que as informações recebam um nível adequado de proteção de acordo com sua importância para a organização

2 DEFINIÇÕES E ABREVIATURAS

TI – Tecnologia da Informação

3 DESCRIÇÃO

3.1 Aplicação

Esta política se aplica a todos os colaboradores, prestadores de serviço, fornecedores e parceiros que utilizam, mantêm ou lidam com ativos de informação da organização. Exceções da política serão permitidas somente quando aprovadas antecipadamente por escrito pelo Gerente de Infraestrutura e Segurança.

3.2 Responsabilidade pelos ativos

3.2.1 Inventário dos Ativos

A organização, por meio do Departamento de TI, tem a responsabilidade de gerir o inventário dos ativos da organização, conforme o Inventário de Ativos, anexo a este documento.

3.2.2 Uso responsável dos ativos

O Departamento de TI é responsável pelos ativos em questão e têm a responsabilidade de estabelecer, por meio desta política, as diretrizes do seu uso responsável visando à proteção e manutenção dos mesmos.

- Ativos físicos
    - Manter a preservação dos ativos;
    - Comunicar o Departamento de TI imediatamente após o extravio, perda, furto, roubo, dano para garantir que as providências cabíveis sejam tomadas;
    - Comunicar o Departamento de TI sobre qualquer tipo de comportamento incomum que pode ser causado pela contaminação do dispositivo por um vírus ou agente externo.

- Ativos de Informação
  - Assegurar a proteção e sigilo das informações confiadas em função das atividades exercidas;
  - Comunicar o Departamento de TI imediatamente após o extravio, perda, furto, roubo, dano para garantir que as providências cabíveis sejam tomadas;
  - Caso o ativo seja utilizado em algum dispositivo eletrônico, o mesmo deve ser mantido com a tela bloqueada na ausência do usuário;
  - Não é recomendado salvar nenhum ativo na área de trabalho. O usuário deve salvar o ativo em um compartilhamento da rede, devidamente protegida pelos sistemas de segurança descritos na Política de Segurança de Informação.

3.2.3 Devolução de Ativos

- O Departamento de TI, com suporte da área de Recursos Humanos, tem a responsabilidade de estabelecer um processo que defina as diretrizes/controles para assegurar que todos os colaboradores, prestadores de serviço, fornecedores ou parceiros, devolvam os ativos da organização, após o encerramento de suas atividades, do contrato ou do acordo.
- Para casos de uso de ativos pessoais (ou que não pertençam a organização) utilizados em atividades da organização, o Departamento de TI tem a responsabilidade de assegurar em seus processos que o conteúdo de direito da organização, seja transferido para um local apropriado e em seguida removido de modo seguro e permanente do dispositivo.

3.3 Classificação da informação

- Todos os ativos de informação da organização devem receber uma classificação, sendo o responsável por esta tarefa o gestor da área. A classificação deve levar em consideração o seu valor, requisitos legais, sensibilidade e criticidade para a organização. A classificação precisa estar visível e de fácil identificação.
- O gestor da informação deve classificar toda informação e deve reavaliá-la logo após a sua alteração. Esta reavaliação deve ser feita embasada nos critérios descritos acima, sempre que o responsável ou a diretoria considerarem necessário.
- Os ativos de informação na organização devem ser classificados conforme a matriz abaixo:

Classificação	Definição
Pública	Aplica-se a todas as informações que podem ser divulgadas interna ou externamente a organização. A divulgação não autorizada não deve impactar séria ou negativamente a organização.
Uso Interno	Aplica-se a todas as informações que podem ser divulgadas internamente a organização. A sua divulgação externa não autorizada pode afetar negativamente a organização e/ou seus funcionários.
Confidencial	Aplicam-se as informações comerciais, sensíveis e informações de clientes utilizadas estritamente dentro da organização. A divulgação não autorizada pode impactar séria ou negativamente a organização, parceiros de negócio e/ou seus clientes.

- Informações que não se enquadram em nenhum dos itens acima devem ser classificadas como CONFIDENCIAL e devem, portanto, ter os mesmos controles de acesso.

3.3.1 Rótulos e tratamento da informação

- Todos os ativos (físico ou de informação) da organização e/ou de terceiros devem receber uma classificação e devem ser rotulados quando pertinente. A rotulagem deve refletir o esquema de classificação estabelecido na seção 3.3 desta política. Todo arquivo de terceiros é considerado CONFIDENCIAL e deve receber tratativa conforme o item 3.3.2.
- O Departamento de TI, em conjunto do Departamento de Sistemas Inkjet, tem a responsabilidade de estabelecer um processo que defina as diretrizes/controles para assegurar a rotulagem dos ativos de informação da organização e/ou de terceiros. Este processo deve ser de conhecimento de todos aqueles que se utilizam dessas informações.

3.3.2 Tratamento dos ativos

- Objetivando assegurar a proteção de acesso adequado para cada classificação de ativos de informação, definem-se as diretrizes para acesso, processamento, armazenamento e transmissão, conforme matriz abaixo:

Classificação	
PÚBLICA	
Acessada	▪ Sem restrição de acesso.

Armazenada	▪ Sem restrição para armazenamento.
Transmitida	▪ Sem restrição para transmissão, desde que autorizado, pelo gestor responsável pela informação.

Classificação	
USO INTERNO	
Acessada	▪ Deve haver um controle de acesso baseado em permissões de grupo/usuário. ▪ Deve haver um controle de acesso que permita apenas acesso interno.
Armazenada	▪ Deve ser armazenada apenas em ambientes internos da organização. ▪ Exceções, devem ser autorizadas pelo Departamento de TI.
Transmitida	▪ Deve ser transmitida apenas em ambientes internos da organização. ▪ Exceções, devem ser autorizadas pelo gestor da informação.

Classificação	
CONFIDENCIAL	
Acessada	▪ Deve haver um controle de acesso baseado em permissões de usuário. ▪ Deve haver um controle de acesso que permita apenas acesso interno.
Armazenada	▪ Deve ser armazenada apenas em ambientes internos da organização. ▪ Deve ser armazenada de modo seguro (criptografado ou outro método existente), quando requisitado pelo cliente. *Consultar a Política de Criptografia* para mais informações.
Transmitida	▪ Deve ser transmitida apenas em ambientes internos da organização ▪ Deve ser transmitido de modo seguro (criptografado ou outro método existente), quando requisitado pelo cliente. *Consultar a Política de Criptografia* para mais informações.

É recomendado que todo ativo de informação seja enviado ou entregue por um sistema de comunicação seguro ou por outro método de entrega que possa ser precisamente rastreado e que tenha sido aprovado pelo Departamento de TI.

3.4 Tratamento de mídias

3.4.1 Mídias impressas

- Materiais impressos contendo informações CONFIDENCIAIS devem ser protegidos por controles de acesso físicos apropriados conforme descrito nas seções 3.3.1, 3.3.2, desta política.
- Relatórios impressos contendo informações CONFIDENCIAIS devem ser mantidos, armazenados ou arquivados fisicamente somente dentro de instalações seguras da organização, e somente pelo tempo mínimo considerado necessário pelo terceiro e/ou responsável pela informação.
- Sob nenhuma circunstância os materiais impressos contendo informações CONFIDENCIAIS devem ser removidos de qualquer instalação da organização sem prévia autorização do responsável pela informação.
- Toda mídia impressa contendo informações CONFIDENCIAIS devem ser armazenadas em um local seguro.
- As demandas definidas pelo cliente no momento da contratação dos serviços devem ser seguidas minuciosamente respeitando as necessidades especificas para a execução dos trabalhos.
- Todo material finalizado contendo informações CONFIDENCIAIS deixam de ser responsabilidade da organização no momento que são retirados da organização. Caso seja necessária alguma exceção a esta regra, é de responsabilidade do gestor responsável pela informação avaliar e autorizar os impactos desta operação.

3.4.2 Mídias Eletrônicas

- Informações CONFIDENCIAIS não devem ser em nenhum momento copiadas em mídias removíveis, quaisquer sejam elas.
- Mídias eletrônicas contendo informações CONFIDENCIAIS de terceiros podem ser admitidas dentro do ambiente da organização apenas para recepção de dados. A informação é, então, incorporada dentro das redes seguras e a mídia é devolvida ao terceiro ou destruída.

3.4.3 Mídias em trânsito

O uso de mídias físicas para transferência de arquivos só deve ser utilizado em caráter de exceção, pois o procedimento padrão é utilizar a troca de arquivos online via FTP (File Transfer Protocol) ou qualquer outro sistema seguro utilizado pelo

cliente. Somente nos casos explicitamente solicitados por clientes são utilizadas mídias físicas.

Toda mídia deve ser embalada e transportada de maneira segura de forma que o acesso não autorizado seja inibido.

Os arquivos preferencialmente devem ser gravados em mídias que não possibilitem alterações ou limpeza dos dados. Quando necessário, os arquivos deverão conter bloqueios por senhas.

3.4.4 Descarte de mídias

a. O Departamento de TI tem a responsabilidade de estabelecer um processo, nesta política, que defina as diretrizes/controles para descarte de mídias de acordo com a matriz de classificação de ativos.

b. O descarte de mídias deve ser realizado conforme o procedimento abaixo:

- A mídia de armazenamento deve ser perfurada pela equipe de manutenção acompanhada pelo departamento de TI;
- Após a destruição, deve ser elaborado o Registro de Destruição de Mídias com evidências conforme documento anexo;
- Por fim, deve ser alimentado uma planilha de controle, com os registros das destruições.

c. Antes do equipamento de informática ou comunicação ser enviado a um fornecedor para troca, manutenção ou descarte, todas as informações confidenciais devem ser destruídas ou removidas de acordo com métodos aprovados contidos nesta política.

d. Mídias removíveis de armazenamento de dados, tais como: floppy, discos óticos ou fitas magnéticas não podem ser doados para caridade ou de outra forma reciclados.

e. O controle das mídias danificadas deve ser feito por meio do Inventário de Mídias Destruídas

3.4.5 Descarte de Materiais Impressos

- Departamento de Qualidade tem a responsabilidade de estabelecer um processo, nesta política, que defina as diretrizes/controles para descarte e destruição de materiais impressos de acordo com a matriz de classificação de ativos
- É de responsabilidade do departamento de Qualidade, quando solicitado pelo cliente, elaborar o “Laudo de Destruição de Materiais”, com evidências. Este processo pode ocorrer com o acompanhamento físico do cliente conforme agendamento.
- Recipientes usados para armazenamento de mídias a serem destruídas (como recipientes que contenham papel a ser fragmentado) devem ser armazenados em

local controlado para evitar o acesso ao seu conteúdo antes do processo de destruição.

- Após executada a destruição e descaracterização do material, este é encaminhado para o setor de aparas. Além disso, é encaminhado um e-mail para o cliente com o Laudo de Destruição.
- Registro das destruições de material físico deve ser mantido pelo departamento de Qualidade por meio de uma planilha eletrônica.

4 ANEXOS

- Política de Segurança da Informação
- Política de Criptografia
- Política de Gestão nas Comunicações
- Anexo – Inventário de Ativos
- Registro de descarte de Disco Rígido/Destruição de mídia
- Inventário de HDs Danificados
- Planilha de destruição de materiais impressos

PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

TÍTULO: GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

HISTÓRICO DAS REVISÕES

Revisão Nº	Data	Descrição da Revisão
00	19/09/2017	Elaboração do documento
01	14/09/2018	Revisão 01
02	01/09/2019	Revisão 02
03	01/09/2020	Revisão 03

CONTEÚDO

DISTRIBUIÇÃO

Conforme Lista Mestre – documentos de segundo nível.

REVISÃO	ELABORADO POR	REVISADO POR	APROVADO POR	DATA DA APROVAÇÃO
03	Daniel Almeida Marcelo Schwed	Ricardo Polito	Ricardo Barros	10/09/2020

1 OBJETIVO

Assegurar que os eventos de segurança da informação sejam tratados de forma efetiva, permitindo o registro, investigação e tomada de ação corretiva adequados e em tempo hábil para mitigar os impactos sobre os sistemas de informação da Leograf Gráfica e Editora Ltda.

2 DEFINIÇÕES E ABREVIATURAS

TI – Tecnologia da Informação

3 DESCRIÇÃO

3.1 Aplicação

Esta política se aplica a todos os colaboradores, prestadores de serviço e parceiros que utilizam, mantêm ou lidam com ativos de informação da organização.

3.2 Seções da política e responsabilidades

3.2.1 Funções e Responsabilidades

É responsabilidade de qualquer integrante do Departamento de TI quando identificar um incidente, notificar os demais membros da equipe para que as ações necessárias sejam tomadas.

É de responsabilidade do Gerente de Infraestrutura de Tecnologia atribuir um nível de prioridade conforme explicado na seção 3.2.4 desta política.

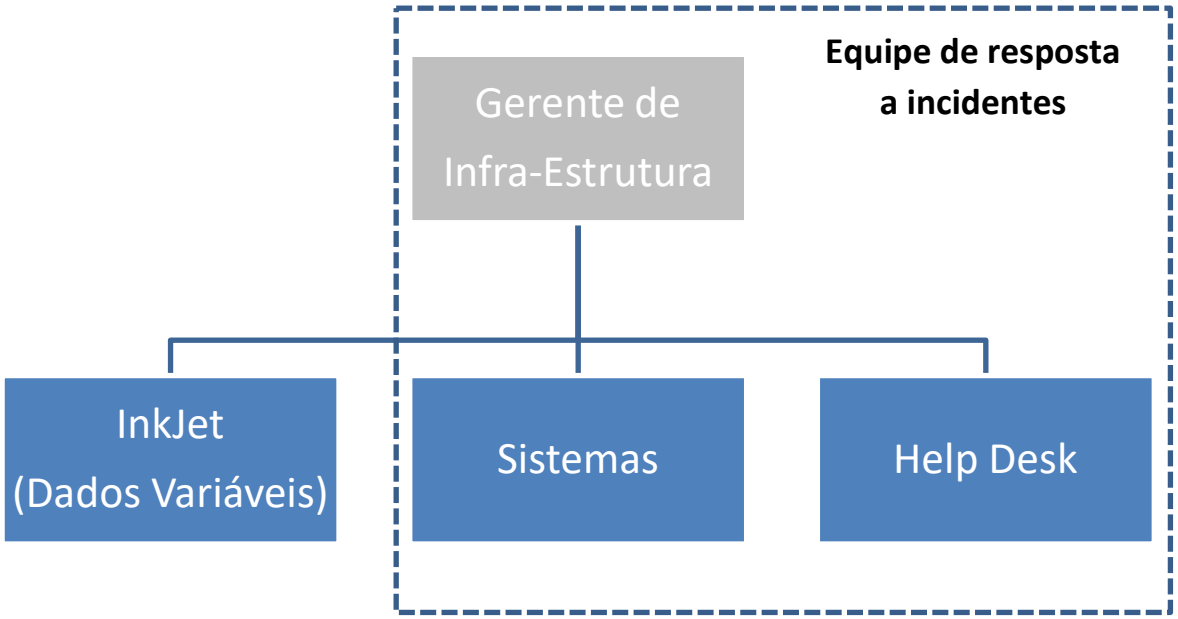
É de responsabilidade de todos os integrantes da equipe de resposta a incidentes determinar a escala de disponibilidade para solução do incidente.

Uma vez corrigido, o Gerente de Infraestrutura de Infraestrutura de Tecnologia deve documentar o ocorrido, registrando todas as informações pertinentes para que possa ser criado um histórico de incidentes para uma possível recorrência.

3.2.2 Equipes para Respostas a Alertas

A equipe do Departamento de TI opera regularmente em horário comercial (8h00 às 18h00), de segunda a sexta-feira, sendo que sempre existe um integrante que fica de prontidão nos finais de semana. Os membros da equipe podem ser encontrados via telefone celular ou residencial, cadastrados para este fim.

Caso ocorra um incidente, independentemente do horário, o gerente de infraestrutura de TI deve ser comunicado e tomar as medidas cabíveis, conforme a avaliação e classificação dos incidentes, presente nesta política.



.

3.2.3 Análise de Risco

As vulnerabilidades são possíveis fragilidades de um ativo ou grupo de ativos que podem ser exploradas por uma ou mais ameaças, resultando assim na quebra de um ou mais princípios da segurança da informação. Ao serem identificadas as vulnerabilidades ou pontos fracos, estes deverão ser classificados, identificando os riscos aos qual o ambiente está exposto e assim definindo medidas de segurança apropriadas para sua correção.

As ameaças podem ser consideradas como agentes externos ou internos ao ativo de informação, pois se aproveitam de sua vulnerabilidade para quebrar os princípios básicos da informação a confidencialidade, integridade ou disponibilidade.

Com relação à segurança, os riscos são compreendidos como condições que criam ou aumentam o potencial de danos e perdas, sendo medidos pela possibilidade de um evento vir a acontecer e produzir perdas.

Para evitar possíveis perdas de informação, o Gerente de Infraestrutura de TI tem a responsabilidade gerir os riscos, onde os mesmos são identificados e classificados, determinando medidas de segurança para reduzi-los ou elimina-los.

RISCO = (Ameaça) x (Vulnerabilidade) x (Valor do Risco)

A classificação de risco deverá ser feita conforme estabelecido nesta política, respeitando os prazos para resolução e os fluxos de resposta e comunicação.

3.2.4 Avaliação e Classificação

A classificação dos incidentes ocorre por meio de dois indicadores principais: o impacto e a urgência. Cada um destes indicadores possui três níveis distintos: alto, médio e baixo.

A combinação entre a urgência para resolução do incidente, o impacto do incidente nos negócios e seu efeito provocado nos prazos e atividades define sua prioridade.

Código de Prioridade	Descrição	Prazo para solução
1	Crítico	1 hora
2	Alto	8 horas
3	Médio	24 horas
4	Baixo	48 horas
5	Muito baixo	Planejado

Impacto	Urgência: Baixo	Urgência: Médio	Urgência: Alto
Alto	3	2	1
Médio	4	3	2
Baixo	5	4	3

- **Crítico:** incidentes que comprometem gravemente a segurança dos ativos físicos e de informação da organização, necessitando de tratamento imediato.
- **Alto:** incidentes que podem comprometer a segurança dos ativos físicos e de informação da organização, porém com menor potencial de impacto adverso que os eventos críticos.
- **Médio:** incidentes que não possuem concomitantemente impacto e urgência altos.
- **Baixo e Muito Baixo:** incidentes que não afetam significativamente as operações da organização

Os critérios supracitados possuem caráter subjetivo, sendo responsabilidade do Gerente de Infraestrutura de TI, baseado em sua experiência profissional, determinar a categoria mais adequada em cada situação.

Os incidentes observados, bem como a solução adotada devem ser cadastrados em uma ferramente de controle a fim de facilitar a sua solução em caso de recorrência. Este processo receberá o nome de base de conhecimento aprimorando, assim, o tempo de resposta da equipe de TI.

3.2.5 Plano de Resposta a Incidentes

O Gerente de Infraestrutura de TI possui plena autonomia para decidir perante situações imprevistas ou inesperadas. Suas ações em uma situação de emergência devem contemplar as seguintes etapas:

- Definir equipe responsável por executar cada uma das atividades previstas no Plano;
- Procedimentos a serem seguidos imediatamente após a ocorrência de um incidente que possui potencial de impactar a organização de maneira adversa;
- Definir a instalação reserva, com especificação dos bens de informática nela disponíveis, na qual os sistemas passarão a funcionar;
- Estabelecer a escala de prioridade dos aplicativos, de acordo com seu grau de interferência nos resultados operacionais e financeiros da organização. Quanto maior a influência do aplicativo na capacidade de funcionamento da instituição, na sua situação econômica e na sua imagem, mais crítico ele será;
- Priorizar os arquivos, programas, para que os aplicativos críticos entrem em operação no menor tempo possível, mesmo que parcialmente;
- Identificar empresas responsáveis por oferecer serviços, equipamentos, suprimentos ou quaisquer outros bens necessários para a restauração;
- Procedimento necessário para restaurar os serviços computacionais na instalação reserva;
- Notificar o Comitê de Segurança da Informação sobre o ocorrido e as ações adotadas;
- Monitorar a situação até o retorno à normalidade das operações.
- Definir condições para ativação do Plano de Continuidade.

3.2.6 Estratégias de Comunicação

O monitoramento das redes, servidores e sistemas é realizado continuamente pela equipe do Departamento de TI. Caso seja identificada uma anomalia por um membro da equipe, o mesmo deve informar o Gerente de Infraestrutura do Departamento de TI explicando sobre o ocorrido. Após esta etapa, cabe a ele determinar quais deverão ser as ações a serem tomadas pela equipe de pronto atendimento.

Devido ao caráter emergencial deste processo, todas ações mitigadoras e/ou corretivas devem ser tomadas até que o problema seja resolvido. O Comitê de Segurança da Informação, conforme estabelecido na Politica de Segurança da Informação, deve ser notificado por meio de e-mail ou reunião para debater o ocorrido.

Deve-se, então, elaborar um documento formalizando o ocorrido e as ações que foram tomadas para sua resolução, para prevenir que o incidente ocorra novamente.

3.2.7 Controle Contra Códigos Maliciosos

Para prevenção e proteção contra ações indesejadas de códigos maliciosos, a organização possui três níveis de segurança. O primeiro sistema de segurança é o Firewall que está posicionado na entrada dos links de internet e analisa toda a entrada e saída do trafego de rede. O segundo sistema de segurança é uma SUITE de controle lógico e antivírus com a finalidade de controlar os servidores e/ou estações (end points). O terceiro sistema de segurança é o Anti-Spam responsável por controlar o conteúdo das mensagens eletrônicas na organização.

Não é autorizada a instalação de qualquer software por usuários de dados computacionais. Somente o Departamento de TI realiza ou autoriza a instalação ou atualização.

3.2.8 Sistemas de Firewall

Toda a rede da Organização é monitorada e coberta por dois níveis de firewall no ambiente do domínio “leograf.local”, também monitorada e coberta por três níveis de firewall no ambiente do domínio “inkjetsys.local”.

Toda e qualquer atividade maliciosa dentro do ambiente de rede pode ser detectada pelo sistema de firewall. Se ainda assim houver, em um caso extremo de uma invasão ou brecha de segurança, o isolamento dos servidores atacados é feito imediatamente. Desse modo verifica-se o resultado do ataque e trata-se imediatamente os danos causados

3.2.9 Plano de Continuidade

O objetivo do Plano de Continuidade do Negócio é manter a integridade e a disponibilidade dos dados da organização, bem como a disponibilidade dos serviços quando da ocorrência de situações fortuitas que comprometam o bom andamento dos negócios.

Possui ainda como objetivo, garantir que o funcionamento dos sistemas informatizados seja restabelecido no menor tempo possível a fim de reduzir os impactos causados por fatos imprevistos. O Plano prevê a possibilidade de dar continuidade nas operações produtivas em um ambiente de backup conforme fluxo em anexo.

Visando garantir a correta execução do Plano de Continuidade o Gerente de Infraestrutura de TI deve definir e monitorar:

- Riscos a que está exposta a instituição, probabilidade de ocorrência e os impactos decorrentes (tanto aqueles relativos à escala do dano como ao tempo de recuperação);
- Consequências que poderão advir da interrupção de cada sistema computacional e operacional;

- Identificação e priorização de recursos, sistemas e processos críticos;
- Tempo limite para recuperação dos recursos, sistemas, processos;
- Alternativas para recuperação dos recursos, sistemas, processos, mensurando os custos e benefícios de cada alternativa.

a. Registro e Documentação

Para registrar as informações e ações adotadas pelo Gerente de Infraestrutura de TI, deve ser utilizado o Documento Plano de Contigencia Operacional (PCO)

4 ANEXOS

- Fluxo de operações para continuidade do negócio
- Plano de Contingencia Operacional

PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

TÍTULO: GESTÃO DE MUDANÇAS

HISTÓRICO DAS REVISÕES

Revisão Nº	Data	Descrição da Revisão
00	19/09/2017	Elaboração do Documento
01	14/09/2018	Revisão 01
02	01/09/2019	Revisão 02
03	01/09/2020	Revisão 03

CONTEÚDO

DISTRIBUIÇÃO

Conforme Lista Mestre – documentos de segundo nível.

REVISÃO	ELABORADO POR	REVISADO POR	APROVADO POR	DATA DA APROVAÇÃO
03	Daniel Almeida Marcelo Schwed	Ricardo Polito	Ricardo Barros	10/09/2020

1 OBJETIVO

Fornecer métodos e procedimentos padrão de forma a atender aos requisitos da Gestão de Mudanças que suportam as operações da Leograf Gráfica e Editora Ltda. A Gestão de Mudanças possui os seguintes objetivos:

- Estabelecer processos claramente definidos para garantir a padronização das mudanças;
- Melhorar a eficiência através do monitoramento de mudanças;
- Reduzir o risco associado à conclusão de mudanças;
- Reduzir o impacto das mudanças no setor de TI e da organização.

2 DEFINIÇÕES E ABREVIATURAS

TI – Tecnologia da Informação

3 DESCRIÇÃO

3.1 Aplicação

Esta política se aplica a todos os colaboradores, prestadores de serviço e parceiros que podem ser impactados por meio de quaisquer mudanças necessárias ao desenvolvimento da organização.

3.2 Seções da política e responsabilidades

3.2.1 Equipe da Gestão de Mudanças

A Gestão de Mudanças deverá ser avaliada e executada por uma comissão formada pelos membros do Comitê de Segurança da Informação e pelas demais partes interessadas (*stakeholders*) relacionadas aos impactos da mudança proposta.

A comissão deverá ser dividida em grupo de implementação, Gerente de Mudanças e Diretor responsável por revisar, aprovar e monitorar a mudança. É responsabilidade do grupo de implementação a execução das tarefas necessárias para a conclusão da mudança demandada. Cabe ao Gerente de Mudanças documentar as ações adotadas e definir os cronogramas de implementação. Por fim, é papel da diretoria a avaliação final do resultado obtido por meio da mudança.

3.2.2 Processo de Gestão de Mudanças

Todas as mudanças realizadas por meio desta política nos setores de TI e Inkjet (dados variáveis) dentro da organização devem ser documentadas. Para isso, deverão ser seguidas as seguintes etapas:

- **Solicitação Formal:** Todos os pedidos de mudança deverão ser documentados.

- **Análise e justificativa:** O Gerente de Mudanças deverá trabalhar juntamente com o solicitante para desenvolver uma justificativa específica para a mudança identificando como ela pode afetar a infraestrutura, operações comerciais e industriais.
- **Categorização e Priorização**: O Gerente de Mudanças avaliará a urgência e o impacto da mudança na infraestrutura, produtividade do usuário final e custo.
- **Planejamento e Aprovação:** O Gerente de Mudanças deverá registrar o planejamento e aprovação da implementação da mudança.
- **Implementação**: Este processo inclui a definição do calendário de implementação da mudança, o desenvolvimento dos requisitos técnicos, a revisão das etapas de implementação específicas e a conclusão da mudança de forma a minimizar o impacto na infraestrutura e nos usuários finais.
- **Revisão Pós-implementação:** Após a implementação da mudança, o Termo de Encerramento deverá ser elaborado, contendo os resultados e as avaliações sobre os objetivos estabelecidos para aquela mudança.

3.3 Categorização da Mudança

As possíveis mudanças contempladas por esta Política são categorizadas em três grupos principais:

- **Mudanças pré-aprovadas:** esta categoria engloba mudanças e alterações que são solicitadas por meio do canal de comunicação com o Departamento de TI. Estas mudanças não apresentam impacto significativo nos processos ou na organização como um todo. O gestor responsável possui autonomia para executá-las sem a prévia autorização do comitê.

- **Mudanças emergenciais:** esta categoria representa o conjunto de mudanças que devem ser realizadas de maneira rápida objetivando a mitigação dos impactos adversos gerados por algum incidente. Esta mudança não demanda autorização prévia do comitê ou da Diretoria em função de sua característica emergencial. Após a execução das atividades corretivas, deve ser elaborada a documentação de registro do ocorrido**.**

- **Mudanças planejadas:** são mudanças que impactam significativamente nos processos administrativos e/ou produtivos necessitando seguir o ritual completo apresentado na Política de Gestão de Mudanças. Em função de suas características e possíveis impactos, esta categoria necessita da mais rigorosa documentação, planejamento e controle das atividades.

3.4 Fluxo de tarefas

3.4.1 Solicitação

A solicitação de mudança deverá ser feita por meio de uma ata de reunião ou de um e-mail ao endereço encaminhado ao Departamento de TI. Este e-mail criará uma tarefa na ferramenta Zendesk. É de dever do solicitante fornecer todas as informações necessárias para que a comissão de Gestão de Mudanças possa identificar as necessidades associadas àquela mudança.

É dever do gerente de Infraestrutura de TI determinar e avaliar as solicitações, descartando-as quando julgar serem irrelevantes para a necessidade em questão.

3.4.2 Categorização e Priorização

As solicitações devem então ser categorizadas com base em sua natureza, em um dos três grupos: mudanças pré-aprovadas, mudanças emergenciais e mudanças planejadas, conforme citado na seção 3.3 desde documento. Para cada uma dessas mudanças, contidas nos três grupos supracitados, deverá haver uma tratativa diferenciada. As mudanças de pré-aprovadas ou de rotina devem ser cadastradas no Zendesk e implementadas conforme demanda sem a necessidade documentação adicional ou aprovação do comitê.

Considerando a natureza das mudanças emergenciais, elas devem ser implementadas o mais rápido possível e a documentação deverá ser elaborada após sua implementação, de forma a registrar um histórico das soluções adotadas.

As mudanças planejadas devem seguir o ritual completo apresentado na Política de Gestão de Mudanças para que possam ser implementadas na organização. Os itens subsequentes desta política versam sobre as demais etapas do processo.

3.4.3 Formação da Comissão

Uma vez que a mudança seja classificada como planejada, é formada a comissão de Gestão de mudanças. O Gerente de Mudanças é escolhido levando em consideração as características da mudança a ser implementada.

3.4.4 Análise e Justificativa

Durante a criação da requisição formal de mudança, o Gerente de Mudanças deve coletar informações adicionais a fim de auxiliar na definição dos parâmetros da mudança. Essa informação adicional deve incluir a identificação de outros requisitos técnicos e/ou requisitos específicos ligados a ela.

A análise de viabilidade da mudança proposta deve ser norteada pela avaliação de impactos na segurança e possíveis melhorias nos processos internos.

3.4.5 Criação da Solicitação e Aprovação

A solicitação de mudança deve ser o documento padrão elaborado pelo Gerente de Mudanças e deve conter todas as informações relevantes sobre a proposta, bem como:

- Informações do solicitante;
- Justificativa, Objetivos e Resultados Esperados;
- Alinhamento Estratégico;
- Informações de todos os membros da comissão que implementará a mudança;
- Escopo e não-escopo da mudança;
- Premissas e Restrições;
- Riscos envolvidos;
- Cronograma de Implementação;
- Marcos de validação e controle;
- Análise de custo/benefício e orçamento, caso necessário;

A solicitação formal deve então ser encaminhada ao comitê para ser debatida e validar a possibilidade de aprovação.

3.4.6 Implementação e Documentação

Uma vez aprovada, a comissão deve finalizar o planejamento, revisando todos os comentários e recomendações para que as tarefas sejam finalizadas com sucesso. Deve-se, também, criar um cronograma apropriado para implementação da mudança e informar todas as partes interessadas.

A implementação deve ser feita dentro do prazo proposto e de acordo com o plano previamente elaborado. O processo deve, em geral, seguir as seguintes etapas:

- Elaboração do planejamento de implementação;
- Implementação da mudança conforme previamente descrito;
- Validação da mudança;
- Solução de possíveis problemas causados;
- Escrita de um breve resumo sobre os resultados;
- Atualizar o documento de Proposta de mudança com os resultados.

3.4.7 Alteração da Proposta de Mudança

Quando houver necessidade de alteração de escopo, cronograma ou demanda, deve-se utilizar o Termo de Alteração a fim de solicitar a alteração na proposta previamente aprovada. O Termo de Alteração deverá conter as seguintes informações:

- Título da alteração;
- Solicitante;
- Descrição;

- Benefícios;
- Medidas necessárias;
- Impactos nas condições originais da mudança;

Todas as Alterações de Proposta de Mudança deverão ser avaliadas, sendo aprovadas ou reprovadas conjuntamente com o Gerente de Mudanças e Diretor responsável pelo acompanhamento da mudança.

3.4.8 Revisão Pós-implementação

Após a implementação, deve-se elaborar uma avaliação a fim de determinar se a mudança teve o resultado esperado. Para pequenas mudanças, esta avaliação pode consistir apenas em verificar se o resultado apresentou a funcionalidade desejada. Para mudanças de grande impacto, isso pode consistir em monitorar a área em questão por meio de dados e *logs* a fim de determinar se o resultado esperado foi atingido.

Para o encerramento do processo de implementação da mudança, deverá ser elaborado o Termo de Encerramento, contendo as seguintes informações:

- Motivo de encerramento;
- Entregas Realizadas;
- Classificação de Aceite;
- Pendencias;
- Considerações dos Stakeholders.

Os documentos elaborados durante o processo de Gestão de Mudanças deverão ser armazenados em uma pasta dentro do departamento responsável.

3.5 Regulamentos externos

- PMBOK

4 REGISTROS

5 ANEXOS

- Solicitação de mudança;
- Termo de alteração de Escopo;
- Termo de Encerramento;

PSI – POLITICA DE SEGURANÇA DA INFORMAÇÃO

TÍTULO: GESTÃO DE OPERAÇÕES

HISTÓRICO DAS REVISÕES

Revisão Nº	Data	Descrição da Revisão
00	19/09/2017	Elaboração do Documento
01	14/09/2018	Revisão 01
02	01/09/2019	Revisão 02
03	10/09/2020	Revisão 03

CONTEÚDO

DISTRIBUIÇÃO

Conforme Lista Mestre – documentos de segundo nível.

REVISÃO	ELABORADO POR	REVISADO POR	APROVADO POR	DATA DA APROVAÇÃO
03	Daniel Almeida Marcelo Schwed	Ricardo Polito	Ricardo Barros	10/09/2020

1 OBJETIVO

Este documento tem como objetivo descrever os processos operacionais dentro fluxo de trabalho relacionado à segurança da informação dentro de ambientes onde estão sendo tratados dados confidenciais na Leograf Gráfica e Editora Ltda.

2 DEFINIÇÕES E ABREVIATURAS

TI – Tecnologia da Informação

3 DESCRIÇÃO

3.1 Aplicação

Esta política se aplica a todos os colaboradores, prestadores de serviço e parceiros que utilizam, mantêm ou lidam com dados confidenciais na organização.

3.2 Seções da política e responsabilidades

3.2.1 Fluxo de Processo com Dados Confidenciais

Todos os materiais impressos que possuem dados confidenciais, segundo a classificação da Política de Gestão de Ativos, devem seguir o procedimento descrito a seguir, a fim de garantir a segurança da informação.

O arquivo e as artes contendo as informações não confidenciais é recebido pela recepção do Departamento de Pré-impressão. A comunicação com o Departamento de Pré-impressão da organização pode ser realizada por meio de e-mail, sistemas de upload de arquivos ou sistemas de FTP. O material é analisado e tratado conforme as necessidades para o processo de impressão. Todos estes ajustes são informados e somente são executados com autorização do cliente. Após esse processo é gerada uma prova, que é encaminhada ao cliente para aprovação do início do processo de fabricação.

Após a liberação da prova por parte do cliente, o material começa a ser confeccionado conforme o procedimento padrão de fabricação. Uma vez impresso, o material é encaminhado ao setor de Inkjet.

Concomitantemente a este processo, os dados confidenciais, são recebidos diretamente pelo Departamento de Inkjet (Dados Variáveis) por meio de um canal de comunicação seguro e as informações contidas são classificadas, conforme descrito na Política de Gestão Ativos. Os dados são então armazenados e tratados dentro da rede “inkjetsys.local”, conforme todos os níveis de segurança necessários. Quando solicitado, os dados podem ser criptografados conforme descrito na Política de Criptografia.

A impressão dos dados confidenciais na mídia pré impressa é realizada e o material segue para o processo de finalização e armazenamento dentro da área segura do Departamento de Inkjet, sendo retirado apenas para sua expedição.

Depois de finalizado o trabalho, os arquivos contendo os dados confidenciais são deletados.

3.2.2 Premissas de Segurança

O ambiente de produção do Departamento de Inkjet é isolado dos demais ambientes produtivos da organização. Leitura biométrica é utilizada como forma de controle de acesso para esse ambiente sendo, também, monitorado por câmeras. O acesso a esta área é concedido ou revogado conforme descrito na Política de Gestão de Segurança Física e do Ambiente e na Política de Controle de Acesso.

Todos os colaboradores que trabalham em ambientes controlados são proibidos de utilizar o celular durante a permanência neste ambiente. Os celulares devem ser armazenados em um armário específico para este fim.

A retirada dos materiais finalizados do ambiente seguro do Departamento de Inkjet é feita por meio de um Protocolo de Acompanhamento. Este documento deve conter as seguintes informações:

- Número da Ordem de Produção
- Data
- Hora
- Cliente
- Quantidade
- Responsável pela Liberação
- Responsável pelo Recebimento

O controle destes protocolos é armazenado pelo período de seis meses, conforme regulamento interno.

3.2.3 Procedimentos em Caso de Falha de Produção

Caso ocorra alguma falha durante o processo produtivo, o material deve ser segregado e identificado. O fato ocorrido deve ser informado à gerência do Departamento de Inkjet, juntamente com o Departamento de Qualidade para que as medidas corretivas cabíveis sejam adotadas.

Caso seja necessário realizar a reimpressão, é gerada uma Ordem de Produção de retrabalho aprovada pelo gestor da produção.

O cliente deverá ser notificado podendo receber, se solicitado, a parte do lote do material que foi danificada ou a mesma pode ser encaminhada para destruição, conforme descrito na Política de Gestão de Ativos.

3.2.4 Procedimentos para Formatação de Computadores, Servidores e Mídias de Armazenamento

Quando houver a necessidade de se realizar a formatação de um computador, servidor ou mídia de armazenamento as seguintes etapas devem ser seguidas.

a. Preparação

- Backup dos arquivos pessoais dos usuários da máquina, quando necessário;
- Backup dos drivers;
- Backup de configurações de aplicativos;
- Listar aplicativos que estão instalados na máquina;

b. Processo de Formatação

- Verificar o particionamento do HD;
- Se necessário criar as partições de maneira correta;
- Instalar, configurar e atualizar o sistema operacional;
- Instalar os drivers;
- Instalar e configurar os programas necessários;

c. Pós-Formatação

- Restaurar o backup dos arquivos dos usuários;
- Testar todos os programas instalados;
- Testar conexões de rede e internet;
- Verificar ativação/registro do sistema operacional se necessário;
- Mapeamento de redes para o usuário, de acordo com Política de Gestão de Acesso

3.2.5 Procedimentos de Backup

É de responsabilidade do Gerente de Infraestrutura de TI, quando necessário, prever a realização de testes periódicos de restauração, no intuito de averiguar os processos de backup e estabelecer melhorias.

A administração dos backups também deve ser orientada para que seus trabalhos respeitem as janelas para execução, inclusive realizando previsão para a ampliação da capacidade dos dispositivos envolvidos no armazenamento.

As mídias defeituosas serão encaminhadas para destruição conforme descrito na Política de Gestão de Ativos.

As solicitações de restauração de arquivos deverão ser abertas formalmente através de ferramentas de abertura de chamados. A solicitação deverá conter os nomes dos arquivos e pastas que deverão ser recuperados, o motivo da restauração e a data do arquivo que se pretende ter acesso.

3.2.6 Procedimento de Controle de Configurações/Alarmes

É de responsabilidade do Gerente de Infraestrutura de TI revisar as configurações gerais e de alarme da ferramenta de monitoramento Pulseway, descrita no POP - Gestão de Sistemas da Informação objetivando a redução da vulnerabilidade dos sistemas internos da organização a novas ameaças.

Para realização desta atividade devem ser seguidas as seguintes etapas de execução:

- Identificar o parâmetro a ser alterado/monitorado;
- Documentar na ferramenta de registro (Zendesk) o detalhamento da alteração a ser realizada contendo as seguintes informações: ferramenta, alteração, motivo e vulnerabilidade identificada;
- Realizar a alteração;
- Monitorar o resultado desta configuração/alarme.

Este processo deve ser realizado pelo responsável quando forem identificadas possíveis vulnerabilidades dos sistemas internos.

3.2.7 Treinamento de Colaboradores

Quando houver mudanças nas políticas ou procedimentos, treinamentos específicos devem ser realizados para capacitar e informar os colaboradores relacionados. É de responsabilidade do Departamento de Treinamentos desenvolverem metodologias e práticas para aplicação e registro destes treinamentos. Os treinamentos devem ser documentados por meio de controles de presença. É recomendada a aplicação de avaliação do treinamento baseados nos seguintes critérios:

- Metodologia utilizada
- Conteúdo
- Aplicabilidade
- Avaliação de Satisfação.

4 REGISTROS

5 ANEXOS

- Protocolo de Acompanhamento

PSI – POLITICA DE SEGURANÇA DA INFORMAÇÃO

TÍTULO: GESTÃO DE SISTEMAS DE INFORMAÇÃO E INFRAESTRUTURA

HISTÓRICO DAS REVISÕES

Revisão Nº	Data	Descrição da Revisão
00	01/09/2017	Elaboração do Documento
01	14/09/2018	Revisão 01
02	01/09/2019	Revisão 02
03	01/09/2020	Revisão 03

CONTEÚDO

DISTRIBUIÇÃO

Conforme Lista Mestre – documentos de segundo nível.

REVISÃO	ELABORADO POR	REVISADO POR	APROVADO POR	DATA DA APROVAÇÃO
03	Daniel Almeida Marcelo Schwed	Ricardo Polito	Ricardo Barros	10/09/2020

1 OBJETIVO

Este documento tem como objetivo definir os processos de gerenciamento dos sistemas de informação e infraestrutura da Leograf Gráfica e Editora Ltda.

2 DEFINIÇÕES E ABREVIATURAS

TI – Tecnologia da Informação

3 DESCRIÇÃO

3.1 Aplicação

Esta política se aplica a todos os colaboradores, prestadores de serviço e parceiros que utilizam os sistemas de informação e a infraestrutura da Organização.

3.2 Seções da política e responsabilidades

3.2.1 Correções (*Patch Management*)

Para minimizar as ameaças de vulnerabilidade, a organização deve ter sistemas configurados adequadamente, utilizar os softwares mais recentes e instalar as atualizações de software recomendadas. Cabe ao Gerente de Infraestrutura de TI avaliar e manter a integridade de softwares em um ambiente de rede, por meio de um procedimento de atualização de correções.

O gerenciamento é considerado crítico para servidores de aplicativos que controlam a infraestrutura central ou de negócios, como servidores de arquivos, impressão, servidores que controlam o serviço de diretório do Active Directory, o DNS e o WINS.

É responsabilidade do Gerente de Infraestrutura de TI garantir que os servidores devem usar versões de softwares com atualizações mais recentes. O procedimento para atualização das correções deve ser realizado conforme as etapas descritas a seguir:

a. Fase 1: Avaliar o Ambiente (continuamente)

O Departamento de TI monitora os servidores regularmente por meio do software Pulseway para identificar qualquer vulnerabilidade no ambiente que possa ser considerada crítica. Se um servidor for considerado em situação não segura, ele será atualizado por prioridade.

b. Fase 2: Identificar Novas Atualizações

O processo de implantação de uma atualização em todos os servidores começa após a divulgação de boletins de atualização, que são identificados pelo software Pulseway, notificando os membros do Departamento de TI.

As atualizações são classificadas de acordo com os seguintes critérios de gravidade:

- **Crítica.** Uma vulnerabilidade cuja exploração pode permitir a propagação de um vírus (worm) da Internet sem a ação do usuário. Devem ser executadas em até 30 dias.
- **Importante.** Uma vulnerabilidade cuja exploração pode causar o comprometimento da confidencialidade, da integridade ou da disponibilidade dos dados do usuário, ou o comprometimento da integridade ou da disponibilidade de recursos de processamento. Devem ser executadas em até 60 dias.
- **Moderada.** Uma atualização corretiva sem impacto de vulnerabilidade. Para esta categoria não define-se um prazo máximo de execução.

c. Fase 3: Avaliar e Planejar a Implantação da Atualização

O Gerente de Infraestrutura de TI deve avaliar todos os impactos que a atualização ocasionará na rede interna de computadores e em sua utilização pelos usuários. Visando reduzir tais impactos adversos, o Gerente de TI programa as atualizações para serem realizadas durante a madrugada, pois neste período há menor volume de atividades.

3.2.2 Revisão de Firewall

a. Definição e Revisão das Regras de Firewall

Todo o tráfego deve passar pelo firewall, a eficácia de um firewall pode ser severamente comprometida se existirem rotas alternativas para dentro da rede. Caso não seja possível eliminar todos esses caminhos, eles devem ser documentados e fortemente vigiados através de outros mecanismos de segurança.

É recomendável que os servidores com acesso externo (Web, FTP, correio eletrônico, etc.) estejam em um segmento de rede separado e com acesso altamente restrito. A principal importância desta ação é proteger a rede interna contra-ataques provenientes dos servidores externos - uma precaução contra a eventualidade de que um destes servidores seja comprometido.

Em alguns casos, é possível identificar na rede interna grupos de sistemas que desempenham determinadas tarefas comuns, tais como desenvolvimento de software, web design e administração financeira. Nestes casos, recomenda-se o uso de suítes de segurança para controlar o acesso aos servidores, com o propósito de aumentar a proteção dos sistemas internos e conter a propagação de ataques bem-sucedidos.

Quando o cliente não possui um meio de comunicação seguro para transferência de arquivos e/ou banco de dados contendo informações sensíveis, é disponibilizado um serviço SFTP para sua recepção pois estas informações exigem um nível maior de segurança e exclusividade.

Todas as regras de firewall ativas e inativas na empresa devem ser revisadas periodicamente a cada 6 meses pelo Gerente de Infraestrutura de TI. Esta ação tem importante papel na prevenção de novos riscos de segurança da informação.

Para os arquivos não classificados como confidenciais (sensíveis), é disponibilizado um meio de comunicação por FTP.

b. Distribuição e Arranjo de Redes

A rede da organização é composta por dois firewalls de Borda (Watchguard M300 e Palo Alto PA-500), um Switch Core (H3C 7506), treze Switches de borda. A descrição de cada um destes sistemas é feita a seguir.

- **Watchguard M300:** Este firewall faz o 1º nível de segurança, recebe os links externos compostos por dois links de 100 Mbps de dois provedores distintos (TIM/Intelig e WCS) que possuem abordagens distintas e tem sua "última milha" por caminhos diferentes até sua chegada ao Datacenter Leograf. Este firewall também gerencia três antenas WiFi AP200 da Watchguard que cobrem o departamento comercial e faz o "Load Balance" dos links externos até a entrega dos serviços de internet ao 2º nível de firewall. As conexões VPN entre as unidades e o acesso externo VPN SSL é fornecido e gerenciado por este equipamento.

- **Palo Alto PA-820:** Este firewall faz o 2º nível de segurança e o enlace entre a WAN e a LAN. Todas as regras de segurança de rede estão neste equipamento que executa bloqueios por aplicação e não por portas.

- **H3C 7506:** Este switch é o gateway de toda a rede, que possui lâminas de fibra para fazer a conexão com todos os treze switches de borda departamentais e lâminas Gigabit Ethernet para atender a todos os servidores do datacenter. Nele estão contidas as rotas ao servidor DHCP e descritas as VLAN que determinam as oito redes lógicas da rede Leograf.

- **Treze Switches de borda:**

Nos racks que atendem os departamentos e/ou áreas existem (13) treze swicthes compostos por equipamentos HP4200G ou HP4800G, que entregam a rede definida por áreas em suas respectivas VLAN's.

Ainda dentro desta estrutura existe logicamente "enclausurado" o domínio "inkjetsys.local" que possui um 3º nível de firewall feito por um Palo Alto PA-200 que monitora todo tráfego de entrada e saída desta rede. Possui também três VLAN's exclusivas e dois servidores, que definem o domínio "inkjetsys.local" e entregam outra faixa DHCP para as VLAN's de desenvolvimento e produção.

Para assegurar o monitoramento da rede e de todos os servidores do ambiente uma suíte de segurança da Kaspersky, o Endpoint Security for Business Advanced é utilizada. Essa suíte integra antivírus com monitoramento de atividade de rede e

diversas outras funções de segurança. E para ter controle “absoluto” sobre o hardware e o sistema operacional dos servidores, utiliza-se o Pulseway.

Com estes aplicativos as informações em tempo real via push info são apresentadas no celular ou via dashboard de toda a atividade dos servidores e da rede.

Com o pulseway sabe-se instantaneamente quando um ou um pacote de atualizações está disponível para cada tipo de ambiente, podendo agir imediatamente ou de modo programado, em grupo ou individualmente para cada caso.

Ainda com o intuito de manter um ambiente com o maior nível de segurança, existe, em modo cluster, um sistema de gerenciamento de conteúdo e ANTI-SPAM para servidores de e-mails da Watchguard, denominado XCS170. Este sistema filtra todas as mensagens que são entregues aos servidores de e-mail e bloqueia até 98% de todo conteúdo indesejável e nocivo vindo da internet.

3.2.3 Controle de Redes

Os controles de redes deverão ser realizados através de regras de bloqueios no firewall, com configuração de perfil do usuário no computador, configuração de extensão de arquivos em e-mails e rotinas de verificação de portas abertas e reputação na internet. Devem ser usadas as ferramentas abaixo, habilitadas para garantir o controle e segurança da rede:

IPS (Intrusion Prevention System): realiza a inspeção dos pacotes usando assinaturas de ataques conhecidos para identificar códigos maliciosos e bloqueá-los.

Controle de aplicações (Application Control): permite a granularidade do controle de acesso a aplicações como: Skype, TeamViewer, Messenger, Logmein, Facebook, Twitter, Instagram etc. O controle de aplicações funciona também para bloquear aplicações indesejadas que atravessam sistemas de segurança quando sua conexão seja criptografada ou usa a mesma porta de um outro serviço. As assinaturas são atualizadas automaticamente pelo fabricante.

Controle de reputação (Reputation): bloqueia ou libera automaticamente páginas com reputação ruim, para HTTP e para HTTPS (para HTTPS depende do DPI habilitado—Deep Inspection) conforme sua configuração. Limitar um acesso a um site que possui uma má reputação é extremamente importante, pois se o mesmo está com uma reputação ruim, provavelmente está vulnerável a ataques.

Aplicação do Safe Search: controla a pesquisa de conteúdo impróprio nos principais mecanismos de busca da internet, impedindo que um usuário consiga encontrar sites com pornografia, crimes cibernéticos, entre outros O filtro é baseado no próprio projeto safesearch. Por exemplo: o usuário busca as palavras "PORNOGRAFIA" ou "PEDOFILIA" no site do Google, mas será impedido de localizar conteúdos impróprios após habilitação do Safe Search.

As redes da Pré-Impressão e Wireless devem conter os bloqueios abaixo:

- Bloqueio ao acesso de redes sociais;
- Bloqueio ao acesso de softwares de mensagens instantâneas;

- Bloqueio ao acesso de sites de transferência de arquivos;
- Bloqueio ao acesso à rede ponto a ponto;
- Bloqueio de upload e download em nosso FTP de arquivos com extensões consideradas perigosas.

Os e-mails não podem trafegar com arquivos com extensões consideradas perigosas. Caso o usuário necessite receber ou enviar um arquivo com extensão bloqueada, o seu gestor deve solicitar através de um e-mail ao Departamento de TI a liberação do mesmo temporariamente.

Os perfis dos usuários nos computadores devem ser cadastrados como “Usuário Padrão” ou “Convidado” tendo acesso diferenciado do usuário “Administrador local”. Somente o Departamento de TI possuirá a senha do usuário “Administrador local” dos computadores. A rede da impressão do Departamento de Inkjet (inkjetsys.local) somente poderá ter acesso liberado aos sites, FTP’s ou ferramentas para transmissão de dados seguras dos clientes, ficando restrito todo e qualquer acesso externo.

3.2.4 Instalação e Proteção dos Equipamentos

A sala onde estão instalados os servidores, equipamentos de telefonia e internet, deve ser refrigerada e monitorada por câmeras. O acesso à sala de servidores, equipamentos de telefonia e internet só pode ser feito pelo departamento de TI ou com o acompanhamento e/ou autorização deste. Para a proteção de equipamentos deverá haver rede elétrica estabilizada, geradores e nobreak com a duração da bateria de aproximadamente 1 hora e meia.

4 REGISTROS

5 ANEXOS

Watchguard M300 (https://rdgroup.co.za/images/wg/wg_firebox_m200-m300_ds.pdf):

Palo Alto PA-820 (https://www.paloaltonetworks.com/products/secure-the-network/next-generation-firewall/pa-820)

H3C 7506 (https://www.hpe.com/h20195/v2/getpdf.aspx/4aa3-0717enw.pdf)

HP4200G (http://h20564.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c02531507) ou HP4800G (http://h20564.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c02547913)

PA-200 (https://www.paloaltonetworks.com/products/secure-the-network/next-generation-firewall/pa-200)

CCM GMC Inspire (https://www.gmc.net/br/produtos/gmc-inspire)

Kaspersky Endpoint Security for Business Advanced (https://www.kaspersky.com.br/small-to-medium-business-security/endpoint-advanced)

PSI – POLITICA DE SEGURANÇA DA INFORMAÇÃO

TÍTULO: SEGURANÇA FÍSICA E DO AMBIENTE

HISTÓRICO DAS REVISÕES

Revisão Nº	Data	Descrição da Revisão
00	19/09/2017	Elaboração do Documento
01	14/09/2018	Revisão 01
02	01/09/2019	Revisão 02
03	01/09/2020	Revisão 03

CONTEÚDO

DISTRIBUIÇÃO

Conforme Lista Mestre – documentos de segundo nível.

REVISÃO	ELABORADO POR	REVISADO POR	APROVADO POR	DATA DA APROVAÇÃO
03	Daniel Almeida Marcelo Schwed	Ricardo Polito	Ricardo Barros	10/09/2020

1 OBJETIVO

Este documento tem como objetivo descrever os dispositivos de segurança das instalações físicas da empresa Leograf Gráfica e Editora Ltda.

2 DEFINIÇÕES E ABREVIATURAS

TI – Tecnologia da Informação.

3 DESCRIÇÃO

3.1 Aplicação

Esta política se aplica a todos os colaboradores, prestadores de serviço e parceiros que tem ou necessitam de acesso às dependências comuns ou restritas da organização.

3.2 Seções da política e responsabilidades

3.2.1 Controle de Entrada Física

O controle de entrada física para colaboradores e visitantes é realizado por meio de monitoramento de câmeras, equipamentos de controle de acesso e portões de entrada com sistema de “torniquetes” e catracas.

A solicitação para liberação de acesso de visitantes só pode ser realizada pela diretoria, gerência ou responsáveis pelos departamentos.

A Recepção é responsável por realizar o cadastramento de visitantes, clientes, fornecedores e prestadores de serviço. Sempre um funcionário deverá acompanhar o visitante, cliente ou fornecedor, sendo responsável pela circulação dos mesmos nas dependências da organização. Para os prestadores de serviço é solicitada a presença de um técnico de segurança do trabalho durante a execução do trabalho ou prestação do serviço.

A entrada de visitantes, clientes, fornecedores e prestadores de serviço podem ser previamente autorizadas quando solicitada por e-mail, devendo este ser encaminhado à Recepção (recepcao@leograf.com.br) com nome do visitante, nº documento de identidade e nome da organização.

É responsabilidade do setor de Recepção cadastrar o visitante em sua primeira visita. O cadastramento deverá ser realizado por meio do software UNIS registrando as seguintes informações:

- Nome completo;
- Documento (RG ou CPF);
- Foto;

- Contato Interno.

Todos os visitantes, clientes, fornecedores e prestadores de serviços devem ser identificados por meio de crachás, disponibilizados no momento do cadastramento. Os crachás devem ser utilizados em local visível durante a permanência do mesmo nas dependências da organização.

Após o cadastramento, a Recepção deverá informar o contato interno da chegada do mesmo.

3.2.2 Segurança em escritórios, salas e instalações

A segurança dos departamentos, salas e instalações com acesso restrito da organização será realizada através de um sistema de controle de acesso com equipamentos de liberação de portas e sistema de monitoramento por câmeras. Somente o responsável pelo departamento pode autorizar ou restringir o acesso. A solicitação deve ser formalizada via e-mail e encaminhada para o departamento em questão para realizar o cadastro e liberação.

3.2.3 Classificação de risco por departamento

Em função da confidencialidade das atividades exercidas por determinados departamentos, é definida uma classificação especial de controle de acesso. Estes departamentos possuem um sistema de liberação de acesso por meio de leitura biométrica dos indivíduos autorizados.

É de responsabilidade da diretoria, em conjunto com o comitê de segurança da informação, determinar a classificação de risco dos departamentos.

Os departamentos considerados de risco para a organização são:

- Inkjet – dados variáveis;
- Tecnologia da Informação;
- Datacenter;
- Jurídico;
- Financeiro.

Caso o departamento de TI, a Diretoria ou o Comitê considerem pertinente, outros departamentos podem ser adicionados ou removidos desta lista.

3.2.4 Acesso a áreas de entrega e de carregamento

Todos devem se identificar antes de entrar nas dependências da organização. Somente pessoas e veículos autorizados podem ter acesso aos locais de entrega e carregamento.

É responsabilidade da Portaria realizar a liberação de todos os veículos que entram nas dependências da organização. Devem ser registradas informações relevantes para liberação de entrada dos veículos por meio de uma planilha de controle de entradas e saídas.

3.2.5 Sistema de monitoramento por câmeras

A organização conta com um sistema de vigilância com câmeras distribuídas no parque gráfico e nos setores administrativos. Este sistema possui autonomia de gravação com retenção das imagens por 15 dias, podendo ser recuperadas por meio de uma central de monitoramento, mediante solicitação.

A organização se resguarda do direito de utilizar-se do sistema de vigilância quando necessário, visando coibir atos ilícitos dentro das suas dependências.

4 REGISTROS

5 ANEXOS

- Documento de controle de entrada e saída de veículos.

PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

TÍTULO: MESA E TELA LIMPA

HISTÓRICO DAS REVISÕES

Revisão Nº	Data	Descrição da Revisão
00	19/09/2017	Elaboração do Documento
01	14/09/2018	Revisão 01
02	01/09/2019	Revisão 02
03	01/09/2020	Revisão 03

CONTEÚDO

DISTRIBUIÇÃO

Conforme Lista Mestre – documentos de segundo nível.

REVISÃO	ELABORADO POR	REVISADO POR	APROVADO POR	DATA DA APROVAÇÃO
03	Daniel Almeida Marcelo Schwed	Ricardo Polito	Ricardo Barros	10/09/2020

1 OBJETIVO

Este documento tem como objetivo descrever os procedimentos de utilização dos recursos da empresa, bem como dispor de seus objetos pessoais e tratamento de objetos e documentos sobre as mesas, assim como a disposição da área de trabalho de seus computadores nas instalações físicas da empresa Leograf Gráfica e Editora Ltda.

2 DEFINIÇÕES E ABREVIATURAS

TI – Tecnologia da Informação.

3 DESCRIÇÃO

3.1 Aplicação

Esta política se aplica a todos os colaboradores, e parceiros que se utilizam das salas, mesas e escritórios da organização.

3.1.1 Responsabilidades

Uma Política de Mesa Limpa e Tela Limpa se refere a práticas relacionadas a assegurar que informações sensíveis, tanto em formato digital quanto físico, e ativos fiquem desprotegidos em espaços de trabalho pessoais ou públicos quando não estão em uso, ou quando alguém deixa sua área de trabalho, seja por um curto período de tempo ou ao final do dia.

Uma vez que informações e ativos em uma área de trabalho estão em um de seus lugares mais vulneráveis, sujeitos a divulgação ou uso não autorizado, a adoção da Política de Mesa Limpa e Tela Limpa é uma das principais estratégias a se utilizar na tentativa de reduzir os riscos de brechas de segurança. E, felizmente, muitas das práticas requerem baixa tecnologia e fáceis de implementar, tais como:

Uso de áreas com trancas: gavetas com trancas, armários de pastas, cofres e salas de arquivo devem estar disponíveis para armazenar mídias de informação ou dispositivos facilmente transportáveis quando não em uso, ou quando não houver ninguém tomando conta deles. Além da proteção contra acesso não autorizado, esta medida também pode proteger a informação e ativos contra desastres tais como incêndios, terremotos, inundações ou explosões;

Proteção de dispositivos e sistemas de informação: computadores e dispositivos similares devem estar posicionados de tal forma a evitar que transeuntes tenham a chance de olhar as telas, e configurados para usar protetores de tela ativados por tempo e protegidos por senha, para minimizar as chances de que alguém tire vantagem de equipamentos desacompanhados.

Adicionalmente, sistemas de informação deveriam ter sessões encerradas quando não em uso. Ao final do dia os dispositivos deveriam ser desligados, especialmente aqueles conectados em rede;

Restrições ao uso de tecnologias de cópia e impressão: o uso de impressoras, scanners e câmeras, por exemplo, deve ser controlado, pela redução de sua quantidade ou pelo uso de funções de código que permitam que somente pessoas autorizadas tenham acesso ao material enviado a elas. E, qualquer informação enviada a impressoras deveria ser recolhida tão rapidamente quanto possível;

Adoção de uma cultura sem papel: documentos não devem ser impressos desnecessariamente, e lembretes não devem ser deixados em monitores ou sob teclados. Lembre-se, mesmo pequenos pedaços de informação podem ser o suficiente para pessoa mal-intencionadas descobrirem aspectos de sua vida, ou dos processos da Leograf, que possam ajudá-los a comprometer informações;

Descarte de informações deixadas em salas de Reunião e Diretoria: todas as informações em quadros brancos devem ser apagadas e todos os pedaços de papel usados durante a reunião devem estar sujeitos a um descarte apropriado;

3.1.2 Controle

Assegurar que as informações do negócio sensíveis ou críticas, por exemplo, em papel ou em mídia de armazenamento eletrônicas, sejam guardadas em lugar seguro (idealmente em um cofre, armário ou outras formas de mobília de segurança) quando não em uso, especialmente quando o escritório está desocupado;

Assegurar que os computadores e terminais sejam mantidos desligados ou protegidos com mecanismo de travamento de tela e teclados controlados por senha, token ou mecanismo de autenticação similar quando sem monitoração e protegida por tecla de bloqueio, senhas ou outros controles, quando não usados;

Garantir que sejam evitados o uso não autorizado de fotocopiadoras e outra tecnologia de reprodução (por exemplo, scanners, máquinas fotográficas digitais);

Garantir que os documentos que contêm informação sensível ou classificada sejam removidos de impressoras imediatamente.

3.1.3 Informações Adicionais

A ISO 27001, um framework popular de segurança da informação, e a ISO 27002, um código de prática detalhado, dá orientação, por meio do controle de segurança – Política de Mesa Limpa e Tela Limpa. Vejamos com mais detalhes:

Adotar política de mesa limpa de papéis e mídias de armazenamento removíveis e uma política de tela limpa para os recursos de processamento da informação.

Assegurar que a Política de Mesa Limpa e Tela Limpa protegida leve em consideração a classificação da informação, requisitos contratuais e legais, e o risco correspondente e aspectos culturais da Leograf. Convém que as seguintes regras sejam consideradas:

Uma Política de Mesa Limpa e Tela Limpa protegida reduz o risco de acesso não autorizado, perda e dano da informação durante e fora do horário normal de trabalho. Cofres e outras formas de recursos de armazenamento seguro também podem proteger informações armazenadas contra desastres como incêndio, terremotos, enchentes ou explosão.

A Leograf adotou o controle de chaves, através de um claviculário, para todas as gavetas, gaveteiros e portas de seu site.

Considerar o uso de impressoras com função de código PIN, permitindo dessa forma que os requerentes sejam os únicos que podem pegar suas impressões, e apenas quando estiverem próximas às impressoras.

PSI – POLITICA DE SEGURANÇA DA INFORMAÇÃO

TÍTULO: SANÇÕES POR DESCUMPRIMENTO DA PSI

HISTÓRICO DAS REVISÕES

Revisão Nº	Data	Descrição da Revisão
00	19/09/2017	Elaboração do Documento
01	14/09/2018	Revisão 01
02	01/09/2019	Revisão 02
03	01/09/2020	Revisão 03

CONTEÚDO

DISTRIBUIÇÃO

Conforme Lista Mestre – documentos de segundo nível.

REVISÃO	ELABORADO POR	REVISADO POR	APROVADO POR	DATA DA APROVAÇÃO
03	Daniel Almeida Marcelo Schwed	Ricardo Polito	Ricardo Barros	10/09/2020

1 OBJETIVO

Este documento tem como objetivo descrever as sanções previstas em nosso regulamento interno para o descumprimento ou falta de atenção as políticas internas.

2 DEFINIÇÕES E ABREVIATURAS

TI – Tecnologia da Informação.

3 DESCRIÇÃO

3.1 Aplicação

Esta política se aplica a todos os colaboradores que conhecem as normas e regulamentos internos, bem como as políticas de segurança internas.

3.2 Seções da política e responsabilidades

3.2.1 Caracterização

O horário de trabalho cumpre papel de atender as necessidades da empresa e, ainda, garantir os direitos de seus colaboradores. O não cumprimento das normas de horário constitui falta grave junto as regras de relacionamento trabalhista e sua legislação, passível de punição. Por este motivo, deve ser observado seu cumprimento conforme o disposto pela Leograf, ou, salvo caráter excepcional já apontado, quando alterado mediante prévio aviso feito pela administração.

Os colaboradores que forem considerados inadimplentes com o cumprimento de suas responsabilidades ou culpados de procedimentos inadequados sofrerão as sanções de acordo com a legislação trabalhista vigente.

Corrupção é definida como abuso de poder ou autoridade para obter vantagens para si. O suborno é qualquer tipo de vantagem patrimonial ou extrapatrimonial, direta ou indireta, a qualquer agente público (independentemente do nível hierárquico), de maneira a obter decisão favorável aos seus negócios. Isto inclui dar ou receber dinheiro (independentemente do valor), outra vantagem como forma de indução á prática de qualquer ato desonesto, ilegal ou de quebra de confiança na prática de suas funções, de modo a influenciar qualquer decisão deste funcionário, garantir vantagem ou induzi-lo a usar sua influência sobre um órgão governamental para ajudar a conseguir, manter e encaminhar negócios. A política da Leograf é evitar quaisquer pagamentos que possam ser caracterizados na definição acima. Os

colaboradores que eventualmente receberem pedidos para realizar este tipo de pagamento devem reportar estes incidentes á Diretoria da Leograf. Atos de corrupção entre partes privadas são atos que não envolvem funcionários públicos. Tais atos são rigorosamente proibidos na Política de Integridade e Transparência nos Negócios.

É proibido realizar qualquer pagamento corrupto por meio de intermediários e realizar qualquer pagamento a um terceiro tendo conhecimento de que a totalidade ou parte do pagamento irá direta ou indiretamente para um terceiro envolvido posteriormente beneficiado seja funcionário público ou não. Todas as decisões comerciais devem ser baseadas no mérito. Além disso, é recomendável a inclusão de cláusulas anticorrupção nos contratos firmados com os parceiros comerciais.

As informações confidenciais necessárias ao seu trabalho devem ser usadas apenas com essa finalidade. Essas informações devem ser compartilhadas apenas com outros colaboradores que precisem delas para seu trabalho e que tenham autorização de acesso às mesmas.

3.2.2 Sanções

As sanções são advertência, seguida de suspensão e demissão por descumprimento subsequente de toda e qualquer norma e regulamento da empresa.