Este documento deve:

1. Estar sempre atualizado;
2. Possuir cópia controlada e somente gerada através da área responsável pela divulgação dos instrumentos normativos;
3. Ser divulgado para todos os funcionários, terceiros e parceiros que possuem acesso a informações do GRUPO LUFT.

Índice

1. Sobre a política de segurança da informação

Para a LUFT, informações de natureza industrial, financeira, comercial ou contratual, decorrentes da pesquisa ou desenvolvimento e informações sobre funcionários representam ativos indispensáveis às atividades corporativas.

A política de segurança da informação é o documento que estimula um comportamento desejável para as práticas de segurança da informação e normatiza as regras de proteção da informação e do uso dos recursos tecnológicos da LUFT, garantindo assim a segurança de seus sistemas de informação através de uma política de proteção e métodos de trabalho adequados.

Baseada na norma ABNT NBR ISO/IEC 27002:2013, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como nas leis vigentes em nosso país, a política de segurança da informação da LUFT é uma diretriz de alto nível e exige a implementação de controles e processos em todas as áreas de negócio da empresa.

2. Campo de aplicação

A Política de Segurança da Informação aplica-se a todas as atividades da LUFT, inclusive aquelas exercidas por contratados e fornecedores. Abrangerá todos os métodos usados para criar, processar, enviar e reter informações e compromete e responsabiliza cada um, estando todos cientes de sua responsabilidade em manter-se atualizado sobre este documento e normas relacionadas.

3. Objetivos

O objetivo desta política é criar uma entidade confiável também conhecida como "*espaço de confiança"* específico para a LUFT, ou seja, uma unidade homogênea de sistemas de informação e telecomunicações em que a proteção da informação seja eficaz e eficiente.

Sendo assim, para garantir que funcionários da LUFT sigam os padrões de comportamento desejáveis e aceitáveis de acordo com a legalidade e boas práticas mundiais, a fim de mitigar riscos técnicos e jurídicos e que sejam prevenidas possíveis causas de incidentes e responsabilidade legal da empresa e seus funcionários internos, externos e parceiros, esta política de segurança da informação será norteada pelos princípios e métodos apresentados a seguir.

3.1. Princípios da segurança da informação

Padronização: a proteção dos sistemas de informação só é possível se cada componente da cadeia possuir o mesmo nível de proteção. Consequentemente, um nível padrão de segurança deve ser definido e implementado para todas as estações de trabalho, servidores, redes, aplicativos, tecnologias e serviços por onde circulam a informação.

Integração: todo projeto que afeta a informação deve levar em consideração os requisitos de segurança da mesma.

Aplicabilidade: todo dispositivo de segurança a ser configurado supõe um procedimento simples e uma estrutura compatível com a organização da empresa ou suas empresas subsidiárias.

Adequação: os dispositivos de segurança utilizados devem ser proporcionais aos riscos identificados e ao ambiente de aplicação.

Durabilidade: as medidas de segurança selecionadas devem usar tecnologias comprovadas, avançadas e fáceis de manter.

Monitoramento: os dispositivos de segurança selecionados devem ser capazes de reportar qualquer evento suscetível de ter impacto no bom funcionamento ou na proteção dos sistemas em questão.

Os princípios gerais para os sistemas de informação, tais como disponibilidade, confidencialidade, integridade e auditabilidade também são aplicáveis aos métodos utilizados para garantir sua segurança.

3.2. Métodos

Análise de risco preliminar: as ameaças e seus impactos potenciais sobre os vários componentes devem ser identificados e avaliados.

Classificação da informação: permite definir, depois de avaliar a sensibilidade das informações armazenadas ou trocadas, o tipo e o alcance das medidas de segurança e controles a serem utilizados.

Determinação das medidas de segurança e controle a utilizar: devem respeitar os princípios de aplicabilidade e durabilidade descritos acima.

Análise de segurança: Verificação da eficácia e, acima de tudo, a eficiência das medidas de segurança utilizadas.

6. Requisitos

Todas as normas aqui estabelecidas deverão ser aplicadas em toda a empresa e seguidas por todos os colaboradores no que se refere à proteção da informação e ao uso de recursos tecnológicos.

Esta política compromete e responsabiliza cada um, estando todos cientes de sua responsabilidade em manter-se atualizado sobre este documento e normas relacionadas, bem como de que os ambientes, telefones, sistemas, computadores e redes da empresa estão sujeitos a monitoramento e gravação.

A política de segurança da informação deverá ser comunicada a todos os funcionários internos, externos, terceiros, parceiros ou fornecedores que interagem com informações da LUFT.

A política de segurança da informação será revisada e atualizada periodicamente, no mínimo a cada 1 (um) ano, ou sempre que algum fato relevante ou evento ocorrer que motive a revisão antecipada da mesma, conforme análise e decisão do fórum responsável.

Visando a efetividade e real cultura de uso ético e legal dos recursos tecnológicos, esta política deverá ser comunicada e formalmente aceita por todos os colaboradores internos, externos e terceiros.

No caso de parceiros e sócios de empreendimentos, deverá ser comunicada e aceita formalmente sempre que a parceria envolver acesso às informações e/ou aos recursos tecnológicos da LUFT.

Deverá ser formado um Comitê responsável pela Gestão da Segurança cibernética e da Informação, o qual será formado por representantes das principais áreas da empresa, sendo pelo menos um representante de Tecnologia da Informação, Financeiro, Jurídico e Recursos Humanos.

Deverá constar em todos os contratos da LUFT o anexo ou cláusula de Confidencialidade, para acesso aos ativos de informação disponibilizados pela empresa.

O uso dos sistemas da LUFT só é permitido para as pessoas que formalizarem a ciência sobre a Política de Segurança da Informação.

A responsabilidade em relação à Segurança da cibernética e da Informação deve ser atribuída na fase de contratação dos colaboradores, de forma a ser incluída nos contratos e monitorada durante a vigência dos mesmos.

Para os colaboradores já contratados em período anterior a esta política, deverá ser-lhes entregue um Termo de Ciência e Responsabilidade para a respectiva assinatura.

Todos os colaboradores da LUFT devem passar pelo menos 1 vez por ano por treinamento e conscientização sobre os procedimentos de segurança cibernética e da informação e uso correto dos ativos disponibilizados pela empresa, com a finalidade de minimizar possíveis riscos de segurança, explicitar suas responsabilidades e comunicar os procedimentos para a notificação de incidentes.

Serão implementados recursos que garantem que todos os usuários de sistemas sejam autenticados com credenciais únicas e intransferíveis, permitindo a rastreabilidade de suas ações no uso dos referidos sistemas necessários.

Serão implementados os recursos necessários para garantir a proteção de autenticação de acordo com a criticidade do sistema ou recurso utilizado.

Serão implementados os recursos necessários para garantir um processo de autorização, isto é, garantir que os usuários possuam acesso somente ao recurso necessário para desempenho de suas atividades profissionais designadas, com a aprovação do responsável pela área em que o colaborador atua.

Não é permitido, portanto, o envio de informações confidenciais ou potencialmente confidenciais alheias às necessidades profissionais entre áreas, sem a prévia autorização do responsável da área responsável pela gestão da informação. (Por exemplo, enviar informações de clientes para uma área que não desempenha nenhuma atividade que necessite desta informação)."

Será criado e implementado um processo de descarte seguro de informações e recursos tecnológicos.

Serão criados e implementados controles apropriados e trilhas de auditoria ou registros de atividades em todos os pontos e sistemas que a empresa julgar necessário para reduzir os riscos dos seus ativos de informação.

Os ambientes de produção e desenvolvimento devem ser segregados e rigidamente controlados.

Um plano de contingência e continuidade do negócio deverá ser implementado e testado, no mínimo anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação, por meio da combinação de ações de prevenção e recuperação.

Os ativos críticos ou sensíveis devem ser mantidos em áreas seguras, protegidas por um perímetro de segurança definido, com barreiras de segurança apropriadas aos riscos identificados e ter o acesso controlado, registrado e monitorado. Para obter mais informações sobre as questões relativas a ativos, consultar a Norma de Uso de Ativos.

Todo ativo de informação deve ser protegido de divulgação, modificação, furto ou roubo, através da aplicação de controles.

Devem ser estabelecidas e comunicadas normas e responsabilidades pela propriedade e custódia dos ativos de informação.

Uma única área deve ser designada como responsável por emitir todos os documentos de identidade, físicos ou lógicos, utilizados na LUFT. Esta área deve buscar a convergência destes documentos para uma identidade única criando uma base de dados sob sua responsabilidade para consulta e identificação por todos os sistemas de controle de acesso físico e lógico da empresa.

Todas as pessoas devem ser distintamente identificadas, sejam visitantes, estagiários, parceiros, funcionários regulares, prestadores de serviços pessoa-física e prestadores de serviços pessoa-jurídica.

Quando razões tecnológicas ou determinações superiores tornarem impossível a aplicação dos requisitos previstos nesta norma ou ainda o uso apropriado de controles mínimos adequados à garantia da segurança dos ativos de informação, o responsável e/ou solicitante deverá documentá-las imediatamente à área de TI, para que possibilite a adoção de medidas alternativas que minimizem os riscos, bem como um plano de ação para corrigi-los, monitorá-los ou eliminá-los. A área de Tecnologia é responsável por endereçar o tema ao Comitê de segurança cibernética e da informação ou, eventualmente, para alguma decisão.

Atribuir na fase de contratação de terceirizados e parceiros, quando este necessitar ter contato com informações da instituição, a inserção de cláusula de responsabilidade, ciência da PSI e confidencialidade, exigindo o repasse das obrigações a seus empregados responsáveis pela prestação de serviços dentro da instituição.

O Proprietário da informação pode ser um diretor, gerente ou coordenador de uma determinada área ou projeto, o qual será o responsável pela manutenção, revisão e cancelamento de autorização à determinada informação ou conjunto de informações pertencentes à LUFT ou sob sua guarda.

A qualquer tempo, e em qualquer dos casos previstos, prevalecendo o descumprimento das regras expostas, a administração de segurança poderá bloquear temporariamente o acesso do usuário comunicando ao mesmo e ao gestor da área os respectivos motivos.

O uso de qualquer recurso da LUFT para atividades ilegais é motivo para demissão por justa causa e a empresa cooperará ativamente com as autoridades nesses casos.

A PSI da LUFT será complementada por Normas de Segurança da Informação (NSI) que tratem de assuntos relacionados ao uso de Correio Eletrônico, uso de Rede Corporativa, uso de Internet, entre outros, e serão consideradas partes integrantes desta PSI.

◗ 7. Da propriedade da informação e monitoramento

Toda informação produzida ou recebida pelos funcionários, sejam internos ou externos, como resultado da atividade profissional contratada pela LUFT, pertence à referida empresa. As exceções devem ser explícitas e formalizadas em contrato entre as partes.

A LUFT reserva-se do direito de monitorar e registrar todo o uso das informações geradas, armazenadas ou veiculadas na empresa. Para tanto, serão criados e implantados controles apropriados e trilhas de auditoria ou registros de atividades em todos os pontos e sistemas que a empresa julgar necessário para reduzir os riscos.

◗ 8. Das responsabilidades específicas

8.1. Dos funcionários em geral

Os funcionários da LUFT, em qualquer nível hierárquico, na sua esfera de competência, serão responsáveis em cumprir, fazer cumprir e zelar pela materialização e realização eficaz das normas e princípios da segurança da informação, no compromisso com os critérios legais e éticos que envolvem a Empresa.

É de inteira responsabilidade de cada funcionário qualquer prejuízo ou dano que vierem a sofrer ou causarem à empresa e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

As infrações a esta política de segurança da informação e suas normas adjacentes estarão sujeitas às penalidades estabelecidas em normas próprias da LUFT ou previstas em contrato de prestação de serviço, independente de aplicação das leis civis ou criminais.

Cabe a todos os funcionários da LUFT:

- Cumprir fielmente políticas, normas e procedimentos de segurança da informação estabelecidos neste documento;

- Buscar orientação do superior hierárquico, quando houver dúvidas relacionadas à segurança da informação;
- Assinar o Termo de Responsabilidade, formalizando a ciência da política e das normas de segurança da informação, bem como assumir a responsabilidade pelo seu cumprimento;
    - Proteger as informações contra o acesso, modificação, divulgação ou destruição não autorizada pela LUFT;
    - Assegurar que os recursos tecnológicos sejam utilizados somente para fins profissionais aprovados e de interesse da empresa;
    - Comunicar imediatamente a área de Recursos Humanos sobre qualquer descumprimento ou violação desta política e/ou de suas Normas e Procedimentos.

8.2. Dos gestores

Garantir na sua área a implementação de mecanismos necessários para o cumprimento da política de segurança da informação.

Cabe a todo gestor de área:

- Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os funcionários internos sob a sua gestão;
- Cumprir e fazer cumprir esta política, as normas e procedimentos de segurança da informação;
- Assegurar que suas equipes possuam acesso e conheçam esta política, bem como das normas e procedimentos aqui estabelecidos;
- Atribuir na fase de contratação de terceirizados e parceiros, quando este necessitar ter contato com informações da instituição, a inserção de cláusula de responsabilidade, ciência da POLÍTICA DE SEGURANÇA DA INFORMAÇÃO e confidencialidade, exigindo o repasse das obrigações a seus empregados responsáveis pela prestação de serviços dentro da instituição;
- Adaptar as normas, processos, procedimentos e sistemas sob sua responsabilidade para atender a esta POLÍTICA DE SEGURANÇA DA INFORMAÇÃO;
- Comunicar imediatamente ao Recursos Humanos e de TI eventuais violações da segurança da informação.

◗ 9. Das disposições finais

As infrações a esta PSI e suas normas adjacentes estarão sujeitas às penalidades estabelecidas em normas próprias da LUFT ou previstas em contrato de prestação de serviço, independente de aplicação das leis civis ou criminais.

A qualquer tempo, e em qualquer dos casos previstos, prevalecendo o descumprimento das regras expostas, a administração de segurança poderá bloquear temporariamente o acesso do funcionário, comunicando ao mesmo e ao gestor da área os respectivos motivos.

O uso de qualquer recurso da LUFT para atividades ilegais é motivo para demissão por justa causa e a empresa cooperará ativamente com as autoridades nesses casos.

A LUFT exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus funcionários, reservando-se o direito de punir os infratores, analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios e adotar as medidas legais cabíveis.

A política de segurança da informação da LUFT será complementada por normas de segurança da informação que tratarão do uso aplicado a segurança da informação de recursos tecnológicos ou serviços fornecidos.

Esta política entrará em vigor na data de sua divulgação, revogando e substituindo qualquer comunicação anterior sobre o assunto.

10. Documentos relacionados

Os documentos relacionados são apresentados no anexo A, Normas e procedimentos relacionados a segurança da informação:

LGPD - Aditivo ao contrato de trabalho

LGPD - Modelo de Cláusula de Privacidade e Proteção de Dados Pessoais

LGPD - Politica de privacidade

NOR 001 - Norma de acesso e utilizacao de e-mail

NOR 002 - Norma de acesso para Internet

NOR 003 - Norma de criação e utilização de senhas

NOR 004- Norma de gestão de acesso

NOR 005 - Norma de monitoramento de ativos

NOR 006- Norma de utilização aceitável de ativos

NOR 007 - Dispositivos Móveis

NOR 008 - Responsabilidades de TI

NOR 009 - Acesso Remoto

NOR 010 - Norma de classificação da informação

NOR 011 - Norma de penalidades

Política de segurança

Termo de gestão da utilização de contas com permissões privilegiadas

Termo de responsabilidade

Termo de utilização de contas com permissões privilegiadas

Este documento deve:

1. Estar sempre atualizado;
2. Possuir cópia controlada e somente gerada através da área responsável pela divulgação dos instrumentos normativos;
3. Ser divulgado para todos os funcionários, terceiros e parceiros que possuem acesso a informações do GRUPO LUFT.

11. Controle e histórico de versões

A tabela a seguir reflete as versões e suas respectivas datas de atualização.

NÚMERO DA VERSÃO	DESCRIÇÃO DA ATUALIZAÇÃO	DATA DA VERSÃO	RESPONSÁVEL

11. Aprovações

A tabela a seguir reflete as aprovações do documento e respectivas vigências.

NÚMERO DA VERSÃO	DOCUMENTO	DATA DA APROVAÇÃO	VIGÊNCIA

Emissor (es):
Revisor (es):
Aprovador (es):