POLÍTICA SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

O Letsbank tem o compromisso de ser um banco inovador, com excelência em crédito corporativo, profundo conhecimento das atividades dos nossos clientes e setores em que atuam, bem como um dos líderes de oferta de soluções financeiras digitais.

Em conformidade com a legislação vigente, com as melhores práticas de mercado e com sua filosofia de transparência e respeito, por meio desta **Política Segurança da Informação e Cibernética** ("**Política**"), o Letsbank revela seu total comprometimento em adotar processos e políticas internas que assegurem o efetivo cumprimento, de forma abrangente, de normas e boas práticas relativas ao mercado financeiro brasileiro.

Aplicação

Nesta Política detalhamos como o Letsbank trata o gerenciamento dos mecanismos e atividades para garantir a segurança das informações e segurnaça cibernética dos ativos, clientes, colaboradores e todas os dados que permeiam as atividades do Letsbank.
Essa Política se aplica a todas as atividades do Letsbank.

Objetivo

A Política de Segurança da Informação e Cibernética tem o objetivo de estabelecer diretrizes e padrões de utilização e segurança aos recursos de tecnologia com base nas melhores práticas, normas e leis vigentes, além de garantir a confidencialidade, integridade, disponibilidade, autenticidade, legalidade e auditabilidade da informação necessária para realização dos negócios do Letsbank.

Também tem como objetivo a proteção dos ativos de informação e formar a base para o estabelecimento de procedimentos de Segurança da Informação e cibernética do Letsbank e empresas do grupo.

Introdução

Cabe a cada colaborador do Letsbank seguir esta Política de Segurança da Informação e Cibernética afim de garantir a tríade da Segurança da Informação:

- **Confidencialidade**: Assegurar que a informação é acessível somente por pessoas autorizadas e que a privacidade do titular dos dados seja garantida.

- **Integridade**: Garantir que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

- **Disponibilidade**: Assegurar que todos os usuários autorizados tenham acesso à informação e ativos associados, quando e se necessário.

  Podemos incluir ainda:

- **Autenticidade**: o sistema deve ter condições de garantir de que a informação e/ou a identidade dos usuários, são quem dizem ser através de métodos de autenticação.

- **Legalidade**: Valor legal das informações dentro de um processo de tratamento dos dados.

Atribuições e Responsabilidades

Esta Política de Segurança da Informação e Cibernética deve ser divulgada e monitorada a fim de que as instruções contidas neste documento sejam seguidas por todos os colaboradores.

Cabe o envolvimento de todas as áreas da empresa garantir o cumprimento dos requisitos previstos nesta Política de Segurança da Informação e Cibernética, a violação de alguma das normativas estará sujeita às regras internas da instituição e resultará a aplicação das medidas administrativas e legais cabíveis.

A responsabilidade pela segurança da informação é atribuída aos colaboradores através de ações coordenadas.

Tal processo envolve as seguintes áreas os quais devem atender aos requisitos a seguir listados:

Diretoria

- Promover a divulgação desta política a todos os administradores, funcionários, prestadores de serviços, consultores e fornecedores.
- Aprovar a política de Segurança da Informação e Cibernética anualmente ou sempre que ocorrer alterações.

- Divulgar ao público resumo contendo as linhas gerais da política de segurança cibernética.

- Prover recursos de gestão para monitorar os serviços a serem prestados.

Gestão, Desenvolvimento & Gente

- Divulgação das contratações / remanejamentos ou desligamentos de colaboradores.

- Solicitação da remoção dos acessos no momento do desligamento ou remanejamento de colaboradores.

- Informar transferência de colaboradores entre áreas aos envolvidos, para a concessão de acessos necessários e revogação de acessos da área anterior.

Contribuir para melhorias desta Política de Segurança da Informação e Cibernética.

Infraestrutura/Segurança da Informação/Suporte

- Controlar os acessos aos recursos tecnológicos do grupo tais como: Redes, Sistemas, Computadores, Servidores e Banco de Dados.

- Revisar periodicamente os acessos a redes e sistemas dos colaboradores.

- Garantir a guarda (backup) e integridade da informação.

- Auxiliar o cumprimento das normas internas.

- Avaliar a adequação e a suficiência dos controles e procedimentos de segurança existentes, a mitigação dos riscos e aderência às Políticas, Manuais de Procedimentos, Regulamentações, apontando deficiências e irregularidades que possam comprometer a segurança e o desempenho organizacional.

DevOps

- Adotar as melhores práticas de implementação e administração de sistemas e aplicações.

- Garantir aplicação de frameworks de segurança durante todo o processo de CI /CD bem como na produção do ambiente de Cloud.

- Garantir a guarda (backup) e integridade da informação.

- Segmentar os ambientes de Produção, Homologação e QA e outros correlacionados.

- Manter controle de versionamentos.

Desenvolvimento

- Adotar as melhores práticas de segurança e qualidade nos desenvolvimentos de sistemas e aplicações.

- Garantir aplicação de frameworks de segurança durante todo o processo de desenvolvimento.

- Adotar Privacy by Design desde a concepção do projeto, produto ou serviço, integrá-la desde a criação (a mantendo posteriormente, durante a execução).

- Seguir a documentação “Desenvolvimento de Software (verificar).

Compliance

- Controle das alçadas em relação à disponibilização de acessos.

- Validar e adequar as políticas de acordo com normas, leis e padrões vigentes garantido respaldo jurídico na implementação destes documentos.

- Monitoramentos de acessos e informações.

- Promover a divulgação desta política a todos os administradores, funcionários, prestadores de serviços, consultores e fornecedores.

- Divulgar ao público a política e outros documentos que sejam de divulgação pública.

Demais áreas, colaboradores e prestadores de serviços, consultores e fornecedores

- Cumprir as diretrizes contidas nesta Política de Segurança da Informação e Cibernética e outras políticas internas.

- Reportar qualquer desvio de conduta ou falha de segurança para os superiores e a área de Segurança da Informação si@letsbank.com.br.

- Registrar a solicitações via ferramenta de chamados e informar qualquer alteração de função para que seus acessos sejam devidamente ajustados.

- Garantir o sigilo dos dados e informações manuseadas para proteger a privacidade dos dados dos titulares em cumprimento a LEI Nº 13.709 (LGPD).

- Ter ciência e efetuar a leitura da nossa Política de Privacidade e Proteção de Dados e em caso de dúvidas entrar em contato através do e-mail lgpd@letsbank.com.br.

- Aos fornecedores externos com papel de Operador que realizarem o tratamento de dados pessoais em nome do **Letsbank**, devem seguir todas as instruções e normativas estabelecidas pelo **Letsbank**.

- Cumprir as leis e normas vigentes no território nacional e no país de onde estiver exercendo suas atividades profissionais.

PARAGRAFO ÚNICO: Todos os Colaboradores devem, após a leitura da Política, assinar via formulário online do Teams o “Termo de Responsabilidade e Ciência da Política de Segurança da Informação e Cibernética”.

Controles e Políticas

Gestão e Revisão de Acessos

Estabelecer política com base nas melhores práticas do mercado para adoção de Gestão e Revisão de Acessos, com objetivo de assegurar a proteção e bom uso dos recursos, ativos e dados do **Letsbank**, garantindo que periodicamente e sempre que ocorrer alguma mudança nas funções do colaborador seus acessos estejam de acordo com as suas atividades e funções atribuídas.

Periodicamente não menos que 1 vez por ano, uma revisão de acessos deve ser realizada para garantir que as informações e acessos estejam de acordo com o necessário para a

execução das atividades correspondentes a função de cada colaborador.

Deve sempre que ocorrer algum encerramento de contrato realizar a revogação imediata de acessos do colaborador.

Classificação e Tratamento da Informação

Toda informação de propriedade do **Letsbank** deve ser classificada e vinculada a um Gestor do Ativo de Informação.

Assim, será classificada para indicar a necessidade, prioridades e o nível esperado de proteção quando do tratamento da informação.

A informação possui vários níveis de sensibilidade e criticidade, desta forma, alguns itens podem necessitar de um nível adicional de proteção ou um tratamento especial ou diferenciado.

A informação poderá ser classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para a organização.

A classificação da informação poderá ser realizada:

- Pelo responsável por cada departamento. Pois ele que conhece melhor as informações do seu departamento;
- Validada após a classificação do gestor pela equipe de Compliance;
- Informar a equipe de S.I, para parametrizar os acessos e/ou monitorar a informação.

Níveis de Segurança

- **Pública** – Esta informação pode ser utilizada por todos sem causar danos ao **Letsbank**.
- **Interna** – Esta informação é aquela que o **Letsbank** não tem interesse em divulgar, cujo acesso por parte de indivíduos externos a ela deve ser evitado. Entretanto, caso esta informação seja disponibilizada ela não causa danos sérios à organização.

- **Confidencial** – Informação interna, restrita ao **Letsbank** ou grupo seleto, cuja divulgação pode causar danos financeiros ou à imagem. Sua integridade deve ser preservada a qualquer custo e o acesso bastante limitado e seguro. Essa divulgação pode gerar vantagens a eventuais concorrentes e perda de clientes.

- **Sensível** - Informações que contenham informações pessoais de clientes ou de negócios realizados pelo **Letsbank**.

BYOD (Bring Your Own Device)

Qualquer acesso a rede por meio de equipamentos de não propriedade do **Letsbank** deve ser aprovado pela equipe de Segurança da Informação e Suporte de TI, não é autorizado o uso dentro da rede corporativa de equipamentos pessoais.

Transferência da Informação

Todas os dados corporativos devem ser armazenados em diretórios de rede ou Cloud disponibilizados por TI, cabe a cada colaborador zelar pelas informações tratadas por ele e garantir a devida guarda em locais seguros na rede.

Todas as informações geradas, manuseadas e armazenadas no ambiente de uso tecnológico do **Letsbank** são de sua propriedade, independentemente da origem, conteúdo ou propósito, incluindo o conteúdo dos e-mails e mensageria, neste caso específico, independentemente de tratarem assuntos privados.

PARAGRÁFO ÚNICO: Os recursos tecnológicos disponibilizados pelo **Letsbank** são de uso exclusivo para o exercício de atividades profissionais.

Descarte de Informações

O descarte de informações física ou lógica deve seguir os devidos cuidados para evitar vazamento de informações ou perda de dados sensíveis.

Para maiores esclarecimentos consultar Procedimento de Classificação de Informação.

Antivírus e criptografia

Todos os computadores contêm antivírus instalado e devidamente atualizados, por padrão são realizadas varreduras para garantir a integridade e segurança dos equipamentos.

O ambiente tecnológico do **Letsbank** é resguardado pelas melhores práticas e ferramentas de segurança disponíveis no mercado.

São adotadas criptografia em dispositivos móveis, rede, conexões e outros meios que trafeguem dados e informações do negócio.

Todo e-mail que contenha informações consideradas sensíveis deve ser enviado adotando a criptografia da ferramenta office 365.

Vírus e malwares

São programas que podem afetar os equipamentos de diferentes maneiras, desde pequenas interferências até a destruição dos servidores, banco de dados e serviços.

O uso de software ilegal (“pirata”) está diretamente associado à propagação de vírus.

O **Letsbank** não utiliza nenhum software ilegal e proíbe a seus colaboradores esta utilização.

Caso necessite utilizar algum software específico, favor solicitar ao seu gestor que deverá obter a aprovação da Diretoria, após a aprovação a área suporte providenciará a aquisição do software. Caso seja necessário homologar a solução favor entrar em contato com a área suporte que poderá lhe auxiliar nos testes funcionais.

A Internet também é meio de propagação, e por esse motivo, os usuários não devem abrir arquivos ou links recebidos de desconhecidos ou em situação suspeita (phishings).

Embora o **Letsbank** possua programas antivírus instalado em todo seu parque tecnológico, com atualização automática e verificação em tempo real, o contato com arquivos contaminados pode trazer sérios problemas ao ambiente computacional.

No caso de dúvida qualquer e-mail suspeito deverá ser enviado para a análise da área de segurança da informação. Mande para o e-mail si@letsbank.com.br.

Gerenciamento de Vulnerabilidades

Periodicamente são realizados escaneamento de vulnerabilidades nos sites, sistemas e aplicativos para que a confidencialidade, integridade e disponibilidade sejam garantidas.

Testes de intrusão também são executados em todo o ambiente tecnológico do **Letsbank** e são aplicadas as melhores práticas de remediação e correção, caso ocorra algum desvio.

E-mail

O correio eletrônico (e-mail) do **Letsbank** deve ser utilizado exclusivamente para fins profissionais.

Todo o conteúdo e mensagens armazenadas/trafegadas pelo e-mail são de propriedade da Instituição e podem ser objeto de monitoramento pelo Compliance e Auditoria.

Cada colaborador possui espaço para arquivar mensagens, que deve ser administrado racionalmente pelo próprio colaborador, principalmente em relação à eliminação de mensagens descartáveis e gravação de arquivos anexados, que impactam o espaço geral. As mensagens e arquivos importantes devem ser gravados nas ferramentas disponíveis.

Toda a informação veiculada através de e-mail deve ser tratada pelos colaboradores como informação confidencial e de propriedade da Instituição, incluindo eventuais e-mails pessoais.

Os colaboradores são responsáveis pelas mensagens enviadas em seu nome.

Para troca de arquivos confidenciais, utilizar o e-mail criptografado e/ou sistema de criptografia de arquivos, dúvidas entrar em contato com suporte@letsbank.com.br.

Acesso à Internet

A Internet está disponível a todos os colaboradores do **Letsbank** e deve ser utilizada como recurso para as atividades profissionais na Instituição.

É proibido download de programas da internet sem o conhecimento da área Segurança de TI. Sempre deve-se considerar que grande parte do material disponibilizado na internet é protegida por leis de direitos autorais. Alguns sites são automaticamente bloqueados por programas de controle de acesso, sendo que em caso de necessidade de algum site especifico o colaborador deve informar a área de suporte justificando a necessidade para que seja liberado o acesso.

Não é permitido instalar programas provenientes da Internet nos computadores e/ou notebooks do **Letsbank** sem expressa anuência da área de Suporte, exceto os programas

oferecidos por órgãos públicos federais, estaduais e/ou municipais. Os usuários devem se assegurar de que não estão executando ações que possam infringir direitos autorais, marcas, licença de uso ou patentes de terceiros.

Quando navegando na Internet, é proibido a visualização, transferência (downloads), cópia ou qualquer outro tipo de acesso a sites:

- De conteúdo pornográfico ou imagens e vídeos relacionados a sexo;
- Que defendam atividades ilegais;
- Que menosprezem, depreciem ou incitem o preconceito de qualquer tipo;
- Que permitam a transferência (downloads) de arquivos e/ou programas ilegais;
- Programas de compartilhamento de arquivos (P2P, Torrent, IRC entre outros); ou
- Qualquer conteúdo que infrinja a leis vigentes ou contenham conteúdo ofensivo.

O **Letsbank** possui recursos de monitoramento dos acessos. O Compliance pode analisar aleatoriamente ou de forma direcionada todos os acessos.

Segurança física

O **Letsbank** mantém uma estrutura física e de ambiente de acordo com as melhores práticas do mercado, para isto possui recursos de infraestrutura e processos capazes de prover e manter a disponibilidade, integridade e confidencialidade com objetivo de prevenir acesso físico não autorizado, danos às instalações, fraude ou sabotagem, entre outras ameaças.

Os controles abaixo descritos destinam-se a proteção e segurança física dos ambientes da organização:

O acesso ao Datacenter (Ambiente é todo em Cloud, mas temos equipamentos On premise nos escritórios (Firewall, DC, Roteadores)) é restrito aos colaboradores da área de infraestrutura, suporte, segurança da informação e facilities. Todos os racks onde se encontram os equipamentos permanecem trancados e as chaves em posse da área de TI.

Somente pessoas autorizadas previamente pelos gestores e, quando for o caso, por Segurança da Informação, mediante identificação, podem ter acesso às dependências do

Letsbank. Nenhum terceiro, prestador de serviço, visitante e/ou cliente poderá acessar os perímetros seguros sem estar acompanhado por colaboradores autorizados, sendo de total responsabilidade do colaborador acompanhante a observação das orientações descritas neste documento;

Entende-se por perímetro seguro todos os locais de trabalho dos colaboradores do Letsbank. Estão fora do perímetro, os banheiros e as salas de reunião;

O Letsbank possui nobreaks capazes de garantir a continuidade de negócios em qualquer evento relacionado à interrupção de energia elétrica no Datacenter e NOC;

Todos os acessos a corredores e perímetros seguros possuem câmaras de circuito interno (CFTV) que operam 24 horas por dia, em todos os dias da semana;

O Datacenter é provido de recursos de detecção de incêndio;

Todo o cabeamento da rede de computadores do Letsbank é estruturado e certificado de acordo com normas internacionais;

A rede WIFI corporativa do Letsbank está disponível apenas para equipamentos autorizados e com segurança 802.1x habilitada e autenticação forte

O Datacenter possui controle e monitoramento ambiental (temperatura e umidade).

Senhas de acesso

Os Colaboradores do Letsbank possuem senhas individuais e personalizadas para acesso às informações que, de acordo com a atividade de cada colaborador, permitem incluir, excluir, alterar e consultar dados.

As senhas devem respeitar os padrões de complexidade e políticas dos sistemas, aplicativos, banco de dados ou softwares que o colaborador deseja utilizar.

Privacidade dos dados

O Letsbank segue as melhores práticas do mercado de segurança da Informação, leis e normativas vigentes.

A privacidade e proteção do titular dos dados é o foco no desenvolvimento dos nossos produtos, nos processos e planejamento do negócio do Letsbank.

A LEI Nº 13.709 (LGPD) e a RESOLUÇÃO CMN Nº 4.893, norteiam nossas ações e são as bases para que nosso ambiente tecnológico esteja de acordo com as principais leis nacionais e seguimos as melhores práticas internacionais e disponíveis no mercado, constantemente nos adequamos as atualizações dessas diretrizes.

Caso tenha alguma dúvida sobre nossa Política de Privacidade e Proteção de Dados entre em contato através do e-mail lgpd@letsbank.com.br.

Plano de continuidade de negócios

O Plano de Continuidade de Negócios, tem por objetivo assegurar, em caso de incidente, a recuperação dos grupos de processos de negócios das operações e de suporte crítico em que o Departamento/Área participa, bem como o retorno à normalidade.

Cada equipe terá um elemento colaborador que será o responsável da equipe e articulação com os “Gestores de Áreas”, “Equipe de Continuidade de Negócios” e “Equipe de Gestão de Incidentes”, em caso de ativação do Plano de Continuidade de Negócios.

O Plano de Continuidade de Negócios deve ser divulgado para todos os agentes responsáveis citados anteriormente e realizados teste periódicos no ambiente de contingência.

Vigência e Atualização

Esta Política entra em vigor na data de sua publicação e poderá ser atualizada pelo **Letsbank**, periodicamente, sendo que a versão em vigor será sempre a mais recente. Para verificar a data da versão em vigor, verifique a “Última atualização” no final deste documento.

Última atualização: Maio de 2022.

***