POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. INTRODUÇÃO

A informação é uma atividade crítica para as empresas e, por esse motivo, precisa ser devidamente protegida. O uso cada vez mais intenso da tecnologia da informação e da interconectividade pelas empresas expõe as informações a ameaças e vulnerabilidades, tornando cada vez mais necessário garantir a sua segurança, integridade, confidencialidade, disponibilidade e autenticidade. De acordo com a ABNT NBR ISO/IEC 27002 (2022, p. X), “seja qual for a forma apresentada ou o meio através do qual a informação é compartilhada e armazenada, é recomendado que ela seja sempre protegida adequadamente”.

A presente Política de Segurança da Informação está baseada nas recomendações propostas pela norma ABNT NBR ISO/IEC 27002:2022, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como está de acordo com as leis vigentes no Brasil. Outras Políticas de Segurança da Informação foram consultadas e utilizadas como referências de normas e procedimentos de segurança da informação.

2. OBJETIVO

Este documento tem por objetivos definir normas e procedimentos de segurança que visem disciplinar o uso da tecnologia de informação, garantindo a segurança da informação e orientando os colaboradores quanto a sua importância, conduta e procedimentos adotados pela CREDFRANCO.

3. APLICAÇÃO

Esta Política aplica-se a qualquer colaborador com acesso às informações da CREDFRANCO, Parceiros, Substabelecidos e afins, e dá ciência de que seus sistemas, computadores e redes poderão ser monitorados, com prévia informação, conforme previsto nas leis brasileiras.

É obrigação de cada colaborador manter-se atualizado em relação aos procedimentos e normas aqui relacionadas, buscando orientação sempre que não estiver absolutamente

seguro quanto à obtenção, uso e/ou descarte de informações.

Esta política estará sempre disponível para consulta dos colaboradores no sistema web da CREDFRANCO.

4. PRINCÍPIOS

A informação produzida ou recebida como resultado de sua atividade profissional pertence à CREDFRANCO.

Divulgar informações confidenciais ou estratégicas é crime previsto nas leis de propriedade intelectual, industrial (Lei nº 9279) e de direitos autorais (Lei nº 9610).

A segurança da informação depende de pessoas comprometidas, processos gerenciais de controle e sistemas de segurança da informação.

Tais normas são fornecidas a título de orientação aos colaboradores e demais envolvidos. Caso os procedimentos ou normas aqui estabelecidos sejam violados, o Comitê de Segurança da Informação, juntamente com a Diretoria da CREDFRANCO, reserva-se o direito de aplicar as punições cabíveis aos colaboradores responsáveis pela violação da política.

5. COMITÊ DE SEGURANÇA DA INFORMAÇÃO

A CREDFRANCO instituiu um Comitê para gerenciar a segurança da informação, o qual é formado por um representante de cada uma das seguintes áreas: TI, Diretoria, Recursos Humanos e Governança e Compliance.

O Comitê deverá se reunir formalmente pelo menos uma vez a cada seis meses. Reuniões adicionais devem ser realizadas sempre que for necessário deliberar sobre algum incidente grave ou definição relevante para a CREDFRANCO.

6. RESPONSABILIDADES

A CREDFRANCO entende que a Política de Segurança da Informação somente será eficaz com o comprometimento de TODOS!

São objetos da Política os serviços e recursos colocados à disposição dos colaboradores, tais como: computadores, telefones celulares, notebooks, correio eletrônico, Internet (*wi-fi*, modem e rede cabeada), informações armazenadas em arquivos físicos ou em diretórios da rede, nuvem corporativa e mídias digitais, além de sistemas de aplicação.

As normas descritas no decorrer deste documento devem sofrer alterações sempre que necessário, sendo que estas devem ser registradas e divulgadas pela empresa, considerando-se o tempo hábil para que eventuais providências sejam tomadas.

Caberá aos responsáveis hierárquicos zelar pelo cumprimento das responsabilidades. Cada colaborador será informado acerca de quem se reportará para fins desta Política.

6.1 Dos Usuários

- Respeitar esta Política de Segurança da Informação;
- Assinar e praticar o Termo de Compromisso, Sigilo e Confidencialidade como condição imprescindível para que seja concedido o acesso aos ativos de informação pela empresa;
- Assinar e praticar o Termo de Recebimento e Responsabilidade pelos recursos da CREDFRANCO como condição imprescindível para que sejam concedidos os recursos informacionais pela empresa;
- Responder pela guarda e proteção dos recursos computacionais colocados à sua disposição para o trabalho;
- Responder pelo uso exclusivo e intransferível de suas senhas de acesso;
- Ativar suas senhas de proteção para Correio Eletrônico (e-mail) e Sistema Operacional, sob orientação da área de TI;
- Buscar conhecimento necessário para a correta utilização dos recursos de *hardware* e *software*, consultando a área de TI, quando necessário;
- Garantir os cuidados mínimos com a segurança da informação, quando as atividades forem executadas fora dos escritórios da CREDFRANCO, como no caso de reuniões externas, trabalhos em casa ou viagem etc.;

- Relatar prontamente à área de TI qualquer fato ou ameaça à segurança dos recursos, como quebra da segurança, fragilidade, mau funcionamento, presença de vírus, etc.;
- Assegurar que as informações e dados de propriedade da CREDFRANCO ou dos clientes e parceiros externos não sejam disponibilizados a terceiros ou utilizados para outros fins, a não ser com autorização por escrito do responsável hierárquico e do cliente;
- Relatar para o seu responsável hierárquico e à área de TI o surgimento da necessidade de um novo *software* para suas atividades;
- Devolver os recursos colocados à disposição pela CREDFRANCO ao término do contrato de trabalho, nas mesmas condições em que recebeu, assinando a devolução do Termo de Recebimento e Responsabilidade pelos recursos;
- Responder pelo prejuízo ou dano que vier a provocar à CREDFRANCO ou a terceiros em decorrência da não obediência às diretrizes e normas aqui referidas.

6.2 Dos Responsáveis Hierárquicos:

- Apoiar e zelar pelo cumprimento desta Política, servindo como modelo de conduta para os colaboradores sob a sua gestão;
- Exigir a assinatura do Termo de Compromisso, Sigilo e Confidencialidade dos colaboradores como condição imprescindível para que seja concedido o acesso aos ativos de informação pela empresa;
- Exigir a assinatura do Termo de Recebimento e Responsabilidade pelos recursos da CREDFRANCO como condição imprescindível para que sejam concedidos os recursos informacionais pela empresa;
- Atribuir, na fase de contratação e de formalização dos contratos individuais de trabalho CLT, prestação de serviços ou de parceria, a responsabilidade pelo cumprimento da PSI CREDFRANCO;
- Autorizar o acesso e definir o perfil do usuário junto à área de TI;
- Autorizar as mudanças no perfil do usuário junto à área de TI;

- Orientar os usuários sobre os princípios e procedimentos de Segurança da Informação,
- Comunicar à área de TI, antecipadamente, a data de saída de colaboradores a fim de assegurar os procedimentos de bloqueio de acesso aos sistemas e de devolução de recursos informacionais disponibilizados;
- Notificar imediatamente ao gestor de liberação da área de TI quaisquer vulnerabilidades e ameaças à quebra de segurança;
- Assegurar treinamento para o uso correto dos recursos computacionais e sistemas de informação;
- Advertir formalmente e aplicar sanções cabíveis ao usuário que violar os princípios ou procedimentos de segurança, relatando imediatamente o fato ao gestor de liberação da área de TI;
- Obter aprovação técnica do gestor da área de TI antes de solicitar a compra de *hardware*, *software* ou serviços de informática;
- Orientar os colaboradores quanto à devolução dos recursos colocados à disposição pela CREDFRANCO ao término do contrato de trabalho, nas mesmas condições em que recebeu, assinando a devolução do Termo de Recebimento e Responsabilidade pelos recursos;
- Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI.

6.3 Da Área de TI

- Configurar os equipamentos, sistemas e redes para cumprir os requerimentos desta PSI;
  Testar a eficácia dos controles utilizados e informar aos gestores sobre os riscos residuais;
- Restringir o acesso de colaboradores aos logs e trilhas de auditoria das suas próprias ações, de forma a garantir que não sejam excluídos;
- Garantir segurança do acesso público e manter evidências que permitam a sua

rastreabilidade para auditoria ou investigação;

- Controlar o acesso aos recursos de processamento da informação da CREDFRANCO e ao processamento e comunicação da informação por colaboradores externos;
- Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes;
- Administrar, proteger e testar as cópias de segurança dos programas e dados ao negócio da CREDFRANCO;
- Gerenciar o descarte de informações, em qualquer formato, a pedido dos custodiantes;
- Garantir que as informações de um usuário sejam removidas antes do descarte ou mudança de usuário;
- Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio;
- Criar e gerenciar credenciais de acesso aos colaboradores na CREDFRANCO, para uso de computadores, sistemas, bases de dados e qualquer outro ativo de informação;
- Efetuar revisão periódica das credenciais a cada 90 dias, com validação dos perfis atribuídos pelo Gestor da Área;
- Certificar que não exista em hipótese alguma, perfis ou usuários duplicados – cada usuário deverá ter EXCLUSIVAMENTE uma credencial;
- Proteger todos os ativos de informação da CREDFRANCO contra códigos maliciosos e ou vírus;
- Garantir que processos de mudança não causem vulnerabilidades e fragilidades no ambiente de produção;
- Definir as regras formais para instalação de *software* e *hardware*, exigindo o seu cumprimento dentro da CREDFRANCO;
- Realizar inspeções periódicas de configurações técnicas e análise de riscos;

- Gerenciar o uso, manuseio e guarda de assinaturas e certificados digitais;
- Garantir, assim que solicitado, o bloqueio de acesso de usuários por motivo de desligamento da CREDFRANCO;
- Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso;
- Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas pode ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
- Monitorar o ambiente de TI, a capacidade instalada da rede e dos equipamentos, tempo de resposta no acesso à internet e aos sistemas críticos da CREDFRANCO, indisponibilidade aos sistemas críticos, incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante), a atividade de todos os colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, *upload*/*download* de arquivos, entre outros);
- Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial ou solicitação do gerente (ou superior);
- Orientar os colaboradores externos que utilizam redes fora dos escritórios da CREDFRANCO, sobre os cuidados mínimos com a segurança da informação;
- Realizar inspeção física nas máquinas de propriedade da CREDFRANCO;
- Receber e conferir os recursos colocados à disposição para os colaboradores ao término do contrato de trabalho, garantindo as mesmas condições em que foram entregues para execução do trabalho;
- Gerenciar o relacionamento com os prestadores de suporte de TI: Suprema Informática(Meet Tecnologia).

6.3 Do Comitê de Segurança da Informação

- Propor as metodologias, sistemas e processos específicos que visem a aumentar a segurança da informação;
- Promover a conscientização dos colaboradores em relação à importância da segurança da informação;
- Apoiar a avaliação e a adequação de controles de segurança da informação para novos sistemas ou serviços;
- Buscar alinhamento com as diretrizes corporativas da CREDFRANCO;
- Revisar essa PSI a cada 6 meses ou 1 ano ou, se necessário, quando houver algum incidente de segurança da informação e conseqüente mudança de procedimentos e normas;
- Comunicar aos colaboradores qualquer mudança nos procedimentos de controles que possam afetar a execução do seu trabalho e a segurança da informação.

7. SOBRE OS RECURSOS COMPUTACIONAIS

Os recursos de TI alocados pela CREDFRANCO aos seus colaboradores são destinados exclusivamente às atividades relacionadas ao trabalho.

Quando o colaborador utilizar dispositivos de sua propriedade como ferramenta de trabalho na CREDFRANCO, seu uso será disciplinado, no que couber, por esta PSI, zelando sempre pela segurança da informação.

É proibida a intervenção do colaborador para manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, bem como a transferência e/ou a divulgação de qualquer *software*, programa ou instruções de computador para terceiros (pirataria).

Quando o contrato de trabalho terminar ou não estiverem sendo mais utilizados os recursos informacionais concedidos pela CREDFRANCO, estes deverão ser encaminhados à área de TI pelos colaboradores que os receberam para a remoção das informações, descarte ou reuso. A área de RH deverá ser comunicada da devolução ou

troca de qualquer recurso informacional, para atualização do Termo de Recebimento e Responsabilidade pelos recursos.

8. SOBRE O CONTROLE DE IDENTIFICAÇÃO (LOGIN E SENHA)

Senhas são um meio comum de validação da identidade do usuário para obtenção de acesso a um sistema de informação, serviço ou dispositivo/mídia (telefone corporativo, notebook, mídias, máquinas fotográficas etc.). A concessão de senhas deve ser controlada, considerando:

- Senhas temporárias devem ser alteradas imediatamente, e não devem ser armazenadas de forma desprotegida;
- A troca de senha será exigida a cada mês para todos os colaboradores que utilizarem computadores e é recomendada essa periodicidade, também, para os demais recursos informacionais da CREDFRANCO. Recomendam-se esses mesmos procedimentos aos colaboradores externos, que utilizam seus próprios recursos para a execução das atividades.
- As senhas serão bloqueadas após três tentativas sem sucesso, sendo que o administrador da rede e o usuário devem ser notificados sobre estas tentativas. Para o desbloqueio é necessário que o usuário entre em contato com a área de TI.

As responsabilidades dos administradores dos sistemas e da rede incluem o cuidado na criação e alteração das senhas dos usuários, além da necessidade de manter atualizados os dados dos mesmos.

As responsabilidades do usuário incluem, principalmente, os cuidados com a manutenção da segurança dos recursos, tais como sigilo das senhas.

- As senhas são sigilosas, individuais e intransferíveis, não devendo ser divulgadas em nenhuma hipótese;
- Tudo que for executado com a senha de usuário da rede ou de sistema será de inteira responsabilidade do usuário. As senhas são efetivas apenas quando

usadas corretamente e sua escolha e uso requerem alguns cuidados como:

i. Não utilizar informações pessoais fáceis de serem obtidas, como o número de telefone, nome da rua, nome do bairro, cidade, data de nascimento, etc.;
ii. Não utilizar senhas somente com dígitos ou com letras;
iii. Utilizar senha com pelo menos, oito caracteres;
iv. Misturar caracteres maiúsculos e minúsculos;
v. Misturar números, letras e caracteres especiais;
vi. Incluir pelo menos um caractere especial;
vii. Utilizar um método próprio para lembrar a senha, de modo que ela não precise ser escrita em nenhum local, em hipótese alguma;
viii. Não anotar a senha em papel ou em outros meios de registro de fácil acesso;
ix. Não utilizar o nome do usuário;
x. Não utilizar o primeiro nome, o nome do meio ou o sobrenome;
xi. Não utilizar nomes de pessoas próximas, como da esposa (o), dos filhos, de amigos;
xii. Não utilizar palavras que estão no dicionário (nacionais ou estrangeiras);
xiii. Não utilizar senhas com repetição do mesmo dígito ou da mesma letra;
xiv. Não fornecer sua senha para ninguém, por razão alguma;
xv. Utilizar senhas que podem ser digitadas rapidamente, sem a necessidade de olhar para o teclado.

9. CONTROLES DE CONTAS GENÉRICAS

Em hipótese alguma será permitida a utilização de contas genéricas, salvo para utilização de contas de serviço, desde que essas credenciais estejam documentadas e associadas a um responsável, ou que não possua vínculo definido no ambiente da CREDFRANCO. Toda credencial será identificada e associada ao colaborador, que por sua vez, será inteiramente responsável por quaisquer ações indevidas que venha a ocorrer. A senha atrelada à conta criada é pessoal e intransferível.

10. GESTÃO DE ACESSO PRIVILEGIADO

A gestão de acesso privilegiado é tratada dentro da política PO-28-POLITICA-DE-CONCESSAO-E-REVOGACAO-ACESSOS

11. DAS TELAS E MESAS LIMPAS

A partir desta data, o papel de parede e proteção de tela de todos os micros deverá seguir a padronização da CREDFRANCO.

O usuário deve cuidar para que papéis, mídias e imagens nos monitores não fiquem expostos ao acesso não autorizado. O cuidado com as mesas limpas deve ser ponto crítico de atenção, principalmente, nos escritórios em que os clientes, parceiros e públicos dos projetos transitam facilmente.

Os computadores deverão ser bloqueados quando não estiverem sendo utilizados. Quando o computador ficar em *stand-by* por mais de um minuto a sessão será finalizada, solicitando *login* e senha novamente ao usuário.

12. DO DESCARTE

11.1. Sobre o descarte das mídias

Mídias contendo informações de propriedade da CREDFRANCO ou dos projetos e seus clientes deverão ser destruídas antes de seu descarte.

CDs, DVDs, e documentos em papel deverão passar pelo triturador antes de serem encaminhadas ao lixo. HDs e *pendrive*s devem ser encaminhados a TI para a destruição da informação ou *backup* antes do descarte ou reutilização.

11.2. Sobre o Descarte dos Dados

Todos os contratos que possuem dados são devidamente descartados e eliminados do Banco de Dados sem possibilidade de recuperação pelo sistema de descarte, após o término da prestação dos serviços ou do período estabelecido em contrato.

O Sistema de Descarte foi desenvolvido pelo setor de desenvolvimento, sendo

executado nos servidores de armazenamento de dados pessoais, todos os primeiros sábados de cada mês às 08:00 hrs, vez que o serviço foi previamente agendado pelo SysAdmin no servidor.

Comentado [1]: Revisar com Thays e Fernando. 29/01/2026

13. SOBRE A CLASSIFICAÇÃO DA INFORMAÇÃO

O gestor de cada área ou projeto deve estabelecer os critérios relativos ao nível de confidencialidade da informação produzida por sua área em: Pública, Confidencial ou Interna, para garantir um nível adequado de proteção. Esses critérios garantirão a definição de como as informações serão tratadas e protegidas.

Para a classificação da informação deverá ser levado em conta o valor, requisitos legais, sensibilidade e criticidade para a CREDFRANCO.

14. DO SIGILO E CONFIDENCIALIDADE

Toda informação disponibilizada ou coletada pelo colaborador, em razão do desempenho de suas funções e atividades, é de propriedade da CREDFRANCO e classificada como confidencial, tendo seu uso restrito às suas atividades, incluindo-se, dentre outras, todas e quaisquer informações orais e/ou escritas, transmitidas e/ou divulgadas pela empresa.

Informação confidencial significa, sem se limitar a, toda e qualquer informação de qualquer natureza - técnica, operacional, comercial e jurídica -, incluídas em descrição ou documentos que envolvam o know-how da empresa, planos de negócios, métodos de contabilidade, técnicas e experiências acumuladas, documentos técnicos e administrativos, contratos, papéis, estudos, pareceres, pesquisas, transmitidas pela empresa ao (a) colaborador (a) ou por ele (a) coletada.

- O colaborador concorda em usar as informações confidenciais recebidas da empresa com o propósito restrito de se fazer cumprir o estabelecido e acordado no contrato de trabalho.
- O colaborador que receber informação confidencial somente poderá usá-la para

o propósito estabelecido no item anterior, e zelará para que tal informação confidencial não seja, de qualquer forma, divulgada ou revelada a terceiros.

- Exceto quando imprescindíveis ao desenvolvimento das ações da CREDFRANCO e integre as suas atividades, não será permitido ao colaborador que receberá informação confidencial produzir cópias ou backup, por qualquer meio ou forma, de qualquer um dos documentos a ele fornecidos ou documentos que tenham chegado a seu conhecimento em virtude do contrato, considerando que todas sejam informações confidenciais.
- Quando fornecida ou revelada por outras pessoas ou clientes, toda informação permanecerá sendo de sua propriedade, somente podendo ser usada pela CREDFRANCO ou pelos colaboradores para os fins de execução do contrato. Tais informações confidenciais, incluídas as cópias realizadas, serão retornadas às pessoas e clientes, ou então destruídas pela empresa, tão logo tenha terminado a necessidade de seu uso ou tenha sido solicitado por eles e, em qualquer caso, na hipótese de término da vigência do contrato, observados as condições nele estabelecidas.
- O colaborador que receber informação confidencial se obriga a:
    i. Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor dessas informações, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objeto referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o seu uso indevido por qualquer pessoa que, por qualquer razão, tenha tido acesso a elas.
    ii. Responsabilizar-se por impedir, por qualquer meio em direito admitido, a divulgação ou a utilização de informações.
    iii. Restituir imediatamente o documento (ou outro suporte/mídia) que contenha as informações confidenciais às pessoas ou clientes, sempre que estes a solicitar ou sempre que estas deixarem de ser necessárias, e não guardarem para si, em nenhuma hipótese, cópia, reprodução ou segunda via das mesmas.
- Fica ciente o colaborador que receber informação confidencial que as obrigações de confidencialidade, tanto quanto as outras responsabilidades e obrigações,

vigorarão durante e após todo o contrato de trabalho, mesmo após o seu desligamento da empresa.

- O colaborador que recebe e tem conhecimento de informação confidencial, reconhece e aceita que, na hipótese de violação de quaisquer dos tópicos mencionados acima, estará sujeito (a) às sanções e penalidades legais, em especial a prevista no art. 482, da Consolidação das Leis do Trabalho, que trata da rescisão do contrato de trabalho por justa causa, sem prejuízo das perdas e danos que der causa, estas estimadas pela empresa, inclusive as de ordem moral ou concorrencial, bem como as de responsabilidades civis e criminais respectivas.

15. SOBRE PROTEÇÃO - ANTIVÍRUS

A CREDFRANCO, por intermédio da área de TI, disponibiliza *software* corporativo de antivírus instalado para todos os colaboradores.

O antivírus é atualizado automaticamente na estação de trabalho do usuário sempre que uma nova versão é disponibilizada pelo fabricante através do aplicativo servidor.

A área de TI da CREDFRANCO não recomenda que o usuário remova ou altere as configurações do antivírus a fim de não comprometer a segurança que o *software* proporciona.

As checagens do disco rígido (HD) da estação de trabalho estão programadas para execução periódica automática, conforme definições da área de TI no aplicativo servidor.

É importante a instalação, pelos usuários, de antivírus nos telefones corporativos, a fim de garantir segurança das informações acessadas nos dispositivos.

Nos casos em que é permitido ao usuário o uso de mídias externas, como *pendrive*s e HDs, são recomendados o seu escaneamento assim que for conectado ao computador.

16. DO E-MAIL CORPORATIVO

Quanto à utilização do e-mail corporativo (usuário@credifranco.com.br):

- Acessar com frequência o e-mail corporativo, a fim de se informar sobre as atividades da CREDFRANCO;
- Manter a conta de e-mail atualizada, evitando acúmulo de e-mails e arquivos desnecessários;
- Observar a cota máxima de e-mails armazenados, estipulada e gerenciada pela área de TI;
- Utilizar o padrão abaixo para o corpo do texto e assinatura dos e-mails:

- Não utilizar o e-mail corporativo da CREDFRANCO para o envio ou recebimento de mensagens não relacionadas ao trabalho, correntes, spams ou e-mails enviados em grande quantidade e/ou para vários destinatários que não sejam solicitados ou autorizados pela empresa. É proibido utilizar o e-mail corporativo para reenviar ou propagar mensagens em cadeia, correntes ou pirâmides, independente da vontade do destinatário de receber tais mensagens;
- Não utilizar o e-mail corporativo da CREDFRANCO para o envio de mala direta, publicidade, material comercial, anúncios, informativos, campanhas ou propagandas que não tenham sido previamente solicitados ou autorizados pela empresa;
- Não enviar e-mails para os grupos de e-mail da CREDFRANCO que não sejam estritamente relacionados ao trabalho e autorizados pela CREDFRANCO ou por seus representantes;
- Não fornecer ou cadastrar o e-mail corporativo da CREDFRANCO em sites de propaganda, redes sociais, notícias, compras ou qualquer outro site que não seja de total interesse e autorizado pela empresa.
- Não alterar quaisquer das informações do cabeçalho do remetente;
- Não enviar e-mails a destinatários que não os querem receber. Quando um destinatário solicitar a interrupção do envio de e-mails, o usuário deverá acatar

imediatamente a solicitação, e informar a CREDFRANCO e seus representantes casos o envio tenha sido por eles solicitado;

- Caso o Comitê de Segurança da Informação julgue necessário, as seguintes ações poderão ser tomadas pela área de TI:
  i. bloqueio de e-mails com arquivos anexos que comprometam a segurança, o uso da rede ou o andamento das atividades relacionadas ao trabalho;
  ii. bloqueio de e-mails para destinatários ou domínios que comprometam a segurança, o uso da rede ou o andamento das atividades relacionadas ao trabalho;
  iii. bloqueio de e-mails para vários destinatários, ou que possam caracterizar o domínio credifranco.com.br como propagador de spam.
- Mensagens recebidas de origem desconhecida deverão ser pré-visualizadas e eliminadas imediatamente, sem leitura de seu conteúdo, para evitar contaminação por vírus e outros riscos.
- O uso indevido do e-mail é de inteira responsabilidade do usuário, podendo o mesmo ser responsabilizado por eventuais danos causados.
- Em nenhuma hipótese a CREDFRANCO será responsabilizada perante quaisquer usuários ou terceiros pela perda de mensagens e/ou respectivo conteúdo.

17. DA REDE CREDFRANCO

17.1 Do Direito de Uso

A rede CREDFRANCO e os equipamentos que a compõem têm como finalidade única e exclusiva permitir aos seus usuários a prática de atividades relacionadas ao trabalho, à pesquisa e à disseminação de informações de interesse da CREDFRANCO e de suas unidades.

Têm direito de uso da rede os empregados, diretores, prestadores de serviços terceirizados e demais usuários autorizados pela CREDFRANCO e por suas unidades.

O uso da internet, acesso à rede e criação de e-mail corporativo (usuário@credifranco.com.br) serão previamente autorizados pela CREDFRANCO ou

por seus representantes através de comunicação à área de TI.

O direito de uso da rede cessa quando o usuário encerrar seu vínculo regular com a CREDFRANCO, seja através do desligamento por qualquer motivo, suspensão do contrato de trabalho ou serviço prestado ou pelo encerramento de atividades que justifiquem seu acesso à rede.

Caso o usuário venha a exercer nova atividade relacionada à CREDFRANCO após o encerramento do vínculo regular, deverá ter sua autorização de uso da rede e acessos revistos, não podendo fazer uso dos direitos que lhe foram concedidos em situação anterior.

15.2 Responsabilidades Individuais

O usuário tem as seguintes responsabilidades na segurança e sigilo da rede da CREDFRANCO:

i. Zelar pela rede e pelos equipamentos que utiliza, não sendo permitida qualquer remoção, desconexão de partes, substituição, reconfiguração ou qualquer alteração nas características físicas ou técnicas dos equipamentos integrantes da rede;
ii. Estar ciente de que o *login* de acesso ou senha à rede é pessoal e intransferível, devendo, portanto, proceder de forma responsável, garantindo o sigilo de sua senha, trocando-os de acordo com as orientações da CREDFRANCO e escolhendo códigos de difícil decodificação;
iii. Respeitar áreas de acesso restrito, não executando tentativas de acesso a áreas e/ou equipamentos alheios às suas permissões de acesso;
iv. Não tomar atitude ou ação que possa, direta ou indiretamente, danificar ou indisponibilizar recursos da rede por qualquer intervalo de tempo;
v. Não executar programas que tenham como finalidade a decodificação de senhas, a monitoração da rede, a leitura de dados de terceiros, a propagação de vírus de computador, a destruição parcial ou total de arquivos ou a indisponibilização de serviços;
vi. Não instalar ou executar programas, instalar equipamentos ou executar

ações que não sejam previamente autorizados pela CREDFRANCO ou que possam facilitar o acesso à rede de usuários não autorizados;

vii. Não fazer uso de direitos especiais de acesso ou de qualquer outro privilégio já extintos com o término do período de ocupação de cargo ou função dentro da CREDFRANCO;

viii. Utilizar a rede corporativa de maneira profissional, ética, segura e legal, mesmo em horários de intervalo e fora do horário de trabalho;

ix. Em caso de dúvidas em relação à utilização e segurança da rede, contatar previamente a área de TI através de e-mail ou outros meios de comunicação que venham a ser oferecidos, e seguir suas orientações.

15.3 Adição de Recursos

É vedada aos usuários a adição de quaisquer recursos à rede, sejam eles microcomputadores, impressoras, ou outros equipamentos.

A adição de novos equipamentos pelo usuário deve ser solicitada por comunicação interna e deverá ser aprovada pela CREDFRANCO. e, uma vez aprovada, a adição será realizada apenas pela área de TI.

Todos os equipamentos ligados à rede devem obedecer aos padrões de instalação, de utilização e de designação de endereços e domínio.

O usuário está ciente que a adição de recursos sem a autorização da CREDFRANCO compromete a administração e a segurança da rede, assim como a assistência ao equipamento.

18. DO ARMAZENAMENTO DE ARQUIVOS DE TRABALHO

Todos os arquivos contidos nos servidores de rede devem ser exclusivamente de interesse da CREDFRANCO. É proibida a criação de pastas pessoais nos servidores da rede.

É proibida, também, a produção e armazenamento de arquivos de trabalho em nuvens não corporativas (*OneDrive* pessoal, Dropbox, Google docs etc.) e nas próprias máquinas, por não ter garantia de *backup* (poderão ser perdidos caso ocorra uma falha

no computador) e compartilhamento com todos os colaboradores envolvidos.

Todos os arquivos produzidos para os serviços da CREDFRANCO devem ser salvos no *Servidor de Arquivos interno e Google Drive (Corporativo)*.

A criação de pastas departamentais ou de projetos nos servidores de rede deverão refletir a estrutura organizacional da CREDFRANCO.

A partir da implantação desta Política, todos os arquivos que não sejam do interesse da CREDFRANCO deverão ser excluídos dos equipamentos para evitar problemas futuros com as auditorias.

19. DO BACKUP DE ARQUIVOS

Compete ao gestor da área TI criar e manter cópias de segurança (*backup*s) apenas dos dados armazenados nos servidores de rede.

Todos os arquivos que estiverem armazenados no *Servidor de Arquivos* estão resguardados por *backup* automaticamente, além de controle de versionamento e responsáveis pelas alterações.

É de responsabilidade exclusiva do usuário a cópia de segurança (*backup*) e a guarda dos dados gravados localmente nos computadores.

20. DA UTILIZAÇÃO DA NTERNET

A internet foi instalada para viabilizar a busca de informações e agilizar determinados processos da CREDFRANCO, podendo ser utilizada para fins pessoais pelos seus colaboradores, desde que não prejudique o andamento dos trabalhos.

O uso indevido do acesso à Internet é de inteira responsabilidade do usuário, que pode ser responsabilizado legalmente por eventuais danos causados. A utilização indevida da internet promove riscos significativos para os ativos de informação e, por esse motivo, torna-se imprescindível seu monitoramento e controles de uso.

A auditoria dos acessos à internet pode levar ao conhecimento dos responsáveis

hierárquicos, relatórios com nomes dos usuários, páginas consultadas, tempo de consulta e o conteúdo navegado. Utilização da internet e aplicativos:

i. Viabilizar as atividades relacionadas ao trabalho, à pesquisa e à disseminação de informações de interesse da CREDFRANCO e de suas unidades;
ii. Não instalar ou acessar sites ou *software*s de conteúdo impróprio ou não relacionado ao trabalho, como sites ou *software*s de conversação instantânea que não seja o *Skype for Business*, redes sociais (ex. Facebook, LinkedIn), sites de compras, sites de entretenimento, jogos, vídeo e música, e outras comunidades ou sites, exceto quando autorizado pela CREDFRANCO;
iii. Não baixar ou instalar programas transmissores de músicas e afins para tocadores de MP3, MP4, rádios on-line, programas P2P como Kazaa, Emule, Edonkey, dentre outros.
iv. Utilizar com parcimônia os serviços de streaming;
v. Não utilizar a rede para fazer *download*s ou *upload*s não autorizados ou não relacionados às atividades da CREDFRANCO ou que não sejam previamente autorizados;
vi. Utilizar apenas os *software*s autorizados pela área de TI para a navegação na internet.

21. SOBRE JOGOS

Os jogos estão terminantemente proibidos.

22. DOS APLICATIVOS DE MENSAGENS INSTANTÂNEAS

Os colaboradores da CREDFRANCO se comprometem a:

- Utilizar os aplicativos de mensagem instantânea (*Whatsapp*, Telegram ou correlatos) para fins corporativos somente quando necessário ou quando este for o único ou o melhor meio para promover a troca de informações urgentes, não

sigilosas nem confidenciais.

- Em grupos criados para discussão de temas relacionados às atividades da empresa, devem restringir o conteúdo das mensagens aos assuntos corporativos.
- Não realizar a troca de mensagens com conteúdo relevante, de cunho sigiloso ou confidencial por meio desses aplicativos, em acordo com a PSI.
- Evitar o uso desses aplicativos para envio de arquivos relacionados ao trabalho, como relatórios, planilhas, etc., em acordo com a PSI;
- Preferir os serviços corporativos de e-mail e mensagens instantâneas (Google Chat) para realizar contatos e trocar mensagens;
- Respeitar os horários regulamentares de folga dos demais colaboradores, fazendo contato fora do horário de trabalho apenas quando estritamente necessário;
- Preferir o uso do número corporativo para comunicação via aplicativos de mensagens instantâneas.
- Não divulgar a terceiros o conteúdo das mensagens instantâneas, sob qualquer hipótese, exceto quando autorizado pelos responsáveis hierárquicos.

23. DOS SOFTWARES

Os *software*s homologados e instalados nos computadores e servidores de rede são de propriedade exclusiva da CREDFRANCO, sendo proibidas as cópias integrais ou parciais, bem como a instalação de *software*s piratas.

Pirataria é considerada crime e *software*s piratas causam prejuízos tanto materiais como funcionais, além de denegrir a imagem da empresa. Por esta razão, estão terminantemente proibidos.

A instalação de *software*s não autorizados (Pirataria) constitui crime contra a propriedade intelectual, de acordo com a Lei 9.609 de 19/02/98, e o infrator está sujeito à pena de detenção e multa.

A CREDFRANCO mantém contratos especiais com alguns fabricantes de *software* e

poderá estender a utilização de alguns deles nos computadores pessoais dos colaboradores, bastando ao colaborador solicitar a instalação à área de TI.

É proibido o uso de e-mails, correios eletrônicos ou mensagens instantâneas de forma contrária à lei, à moral, aos bons costumes, à ordem pública ou que infrinjam os direitos à propriedade intelectual ou industrial pertencente a terceiros.

O conteúdo e a utilização de e-mails, correios eletrônicos ou mensagens instantâneas deve ser de caráter exclusivamente profissional.

24. DAS AUDITORIAS

Auditorias serão realizadas e relatórios serão gerados periodicamente.

Todos os usuários da rede da CREDFRANCO estão sujeitos à auditoria de redes. Os procedimentos de auditoria e de monitoramento de uso serão realizados periodicamente ou sempre que solicitados pela diretoria ou área de TI ou profissional contratado para este fim, com o objetivo de observar o cumprimento das normas deste regulamento pelos usuários da rede e com vistas à gestão de desempenho e segurança da informação.

Havendo evidência de atividade que possa comprometer a segurança da rede ou que descumpra as regras estabelecidas por este regulamento, será permitido ao administrador da rede auditar e monitorar as atividades de um usuário, além de inspecionar seus arquivos, registros de acesso, contas de e-mail corporativo e acesso aos sistemas e sites de comunicação interna da empresa, sendo o fato imediatamente comunicado à Diretoria ou seus representantes. Os dados apurados no computador serão mantidos em sigilo pela direção da CREDFRANCO.

A CREDFRANCO poderá, a qualquer tempo, implantar aplicativos de segurança, monitoramento e gravação do uso da rede e internet, instalar *softwares* e *hardwares* para proteger a rede e garantir a integridade dos dados e programas, instalar *firewall*, inspecionar arquivos armazenados na rede, seja em disco local, virtual ou nas áreas privadas da rede, a fim de assegurar o cumprimento das regras aqui estabelecidas.

25. DISPOSIÇÕES FINAIS

A segurança da informação deve ser entendida como parte fundamental da cultura interna da CREDFRANCO. Qualquer incidente de segurança subentende-se como alguém agindo contra a ética e os valores regidos pela instituição.

Todas as práticas que ameacem a segurança da informação serão tratadas com a aplicação de ações disciplinares, desde uma advertência verbal até rescisão contratual por justa causa, levando em consideração fatores como: função exercida pelo colaborador, período utilizado, local de utilização, horário de utilização, prejuízo real ou potencial causado à CREDFRANCO, além de responder legalmente por atividades que descumpram a legislação brasileira, entre outros.

26. REVISÕES E ATUALIZAÇÕES

Visando promover uma melhor experiência aos Colaboradores, Clientes e Parceiros CREDFRANCO, os termos desta Política poderão ser atualizados ou adaptados, anualmente, conforme o início de cada ano, para que reflitam as nossas práticas, bem como estejam sempre em conformidade com a legislação aplicável.

27. CONSIDERAÇÕES FINAIS

Esta Política deverá ser adotada a partir desta data e todas as alterações estruturais que se fizerem necessárias deverão ser previamente aprovadas pela área de Governança e Compliance.

Histórico de Revisões

Versão	Data		Revisões	Aprovador	Área
	Atualização	Aprovação			
01	-	18/04/2021	Emissão da Política	Everton Alves	Tecnologia da Informação
02	28/06/2022	07/06/2022	Atualização do Layout e Revisão do Conteúdo	Bárbara Fideles/Gustavo Ferreira	Governança e Compliance/ Tecnologia da Informação

03	14/06/2023	14/06/2023	Revisão de Conteúdo	Emily Assumpção/Gustavo Ferreira	Governança e Compliance/ Tecnologia da Informação
04	21/09/2023	21/09/2023	Inclusões de subitem e Revisão de Conteúdo	Emily Assumpção/Fernando Bulhões	Governança e Compliance/ Tecnologia da Informação
05	21/12/2023	01/03/2024	Atualização do item 9	Gustavo Ferreira/Emily Assumpção/Hemerson Rodrigues	Tecnologia da informação /Governança e Compliance
06	07/02/2025	07/02/2025	Atualização do item 10 e revisão de conteúdo	Gustavo Ferreira / Hemerson Rodrigues / Thays Cristina	Tecnologia da Informação / Compliance
07	29/01/2026		Atualização do item 18 e 22	Gustavo Ferreira Hemerson Rodrigues Thays Cristina Lais Cristina Gabriel Bortoloto	Tecnologia da Informação Compliance