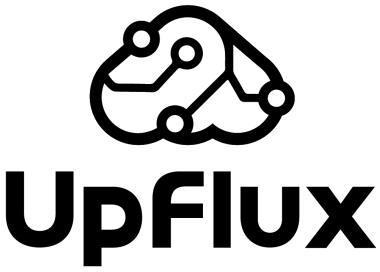
Política de Segurança da Informação

Comitê de Segurança da Informação

19 de fevereiro de 2024



Sumário

1 Introdução

Este documento descreve a Política de Segurança da Informação (PSI) da UpFlux, formalmente Smart Process S.A. Esta política regula o comportamento dos usuários e o acesso, a geração, a manipulação e o descarte dos ativos de informação, com o objetivo de preservar a integridade, confidencialidade e disponibilidade destes ativos durante a respectiva existência.

As políticas presentes neste documento descrevem a conduta considerada adequada para a manipulação de ativos de informação da UpFlux. Quaisquer condutas em desacordo com as políticas aqui descritas são consideradas incidentes de segurança da informação.

1.1 Apresentação

Este plano de evolução de segurança iniciou em 2019 e é revisado periodicamente, atualmente num ciclo de 6 meses. Já implementamos diversos controles, como registros (logs) de modificação de acesso, integração de diretórios de dados, procedimentos de gestão de incidentes, rastreamento de operações de leitura, interface programáveis (API) para controle de dados, uso de mecanismo de segundo fator de autenticação. Para 2024, precisa-se evoluir de maneira a melhorar a interação aos registros de acesso (log de login, de criação, de modificação e de exclusão).

1.2 Objetivos

- Definir regras relativas à gestão de segurança da informação.
- Balizar o comportamento dos colaboradores sobre os ativos da informação da UpFlux.
- Conscientizar os colaboradores sobre o correto uso dos recursos de informação da organização.
- Definir responsabilidades e ações a serem tomadas quando do não cumprimento desta política.

1.3 Declaração da Administração

A diretoria da UpFlux reconhece a importância dos ativos de informação da organização, colaboradores, clientes, fornecedores e parceiros, que estão sob sua responsabilidade. Esta diretoria está comprometida com a implementação de um Sistema de Gestão de Segurança da Informação (SGSI) em suas atividades, visando garantir os princípios de confidencialidade, integridade e disponibilidade, e compromete-se a implantar, manter, divulgar e fiscalizar esta política dentro da organização.

A diretoria da UpFlux define as seguintes diretrizes corporativas de Segurança da Informação:

a) A informação da empresa, colaboradores, clientes e fornecedores é importante e deve ser protegida.
b) Devem ser garantidos os aspectos de confidencialidade, integridade e disponibilidade das informações da empresa, colaboradores, clientes e fornecedores.
c) A gestão da segurança da informação deve ser feita por um comitê de segurança da informação que seja estabelecido e reconhecido pela diretoria.
d) A segurança da informação na empresa é responsabilidade de todos os colaboradores e ações devem ser desenvolvidas para a consolidação deste conceito.

e) Análises de risco e auditorias de segurança da informação devem e são realizadas periodicamente, a cada 6 meses.
f) As ações de segurança da informação consideradas críticas pela empresa devem ter um cronograma de execução claramente definido e ser executadas conforme tal, sob acompanhamento do Comitê de Segurança da Informação.

1.4 Escopo

Esta política de Segurança da Informação se aplica a todos os colaboradores da UpFlux e a todos os recursos disponibilizados pela empresa, sejam eles físicos, tecnológicos, informações em trânsito ou informações armazenadas.

A aplicação desta Política de Segurança da Informação para aqueles que não são colaboradores da UpFlux será regulada individualmente por cada contrato de prestação de serviço.

1.5 Conceitos e Definições

Com base na ABNT NBR ISO/IEC 27001[1] e em definições internas da empresa, para os efeitos desta Política de Segurança da Informação aplicam-se as seguintes definições fundamentais:

- **Fora do expediente:** sem o ponto marcado ou em horário de repouso para alimentação.
- **Dentro do expediente:** com o ponto marcado, exceto horário de repouso para alimentação.
- **Colaborador:** todos que possuem contrato previso na Consolidação das Leis do Trabalho (CLT) formalmente estabelecido com a empresa.
- **Prestador de serviço:** todos que possuem contrato de prestação de serviço formalmente estabelecido com a empresa;
- **Visitante:** todos que não possuem qualquer tipo de contrato estabelecido com a empresa.
- **Partes externas:** abrange prestadores de serviço e visitantes, ou seja, todos que não são colaboradores da empresa.
- **Compartilhamento:** um diretório publicado na rede de computadores, que pode ser de um setor, pessoal ou de acesso público.
- **Sistemas Corporativos:** todo e qualquer sistema de informação utilizado nos processos de negócio da empresa.
- **Ciclo de vida da informação:** compreende os estágios de criação, transporte, armazenamento, manuseio e descarte da informação.
- **Superior Imediato:** consiste no cargo de liderança imediatamente superior a um determinado colaborador. Abrange os cargos de Supervisor, Gestor, Gerente, Diretor e Presidente, conforme formalmente estabelecido no setor de Recursos Humanos (RH).
- **Responsável de setor:** é o colaborador que responder por determinado setor, abrange os cargos de Gestor, Gerente e/ou Diretor.
- **Rede Corporativa:** rede de computadores utilizado para trabalho.
- **Rede Visitantes:** rede exclusivamente para acesso à internet utilizada por visitantes e prestadores de serviço.
- **Rede Diretoria:** rede exclusivamente para acesso à internet utilizada pela diretoria e colaboradores autorizados por ela.

[1] ABNT. NBR ISO/IEC 27001: Sistemas de gestão da segurança da informação - Requisitos. Rio de Janeiro, 2020

1.6 Documentos Relacionados

Para efeitos de conformidade, análise de risco, auditoria, registro de incidentes e aplicação de medidas disciplinares, esta política de segurança da informação relaciona-se com os seguintes documentos corporativos:

- Documentos do Sistema de Gestão Integrado (SGI).
- Código de ética e conduta profissional.
- Documentos da gestão da segurança do trabalho.
- Termo de Propriedade Intelectual (PI).
- Termo de Confidencialidade.
- Termo de Responsabilidade no uso das Informações.

Estes documentos estão disponíveis para acesso público na seção **Termos e Condições**[2] do site da UpFlux.

1.6.1 Boas Práticas

Adotar as boas práticas em conformidade com documentação de método padronizado e consolidado fortalece a postura de segurança dos dados e sistemas contra as ameaças cada vez mais sofisticada. Com isso, em alinhamento o framework National Institute of Standards and Technology (NIST[3]), identificar ativos e riscos, proteger o contexto, detectar incidentes, responder com plano de ação e recuperar em rápida mitigação são ações estabelecidas como boa prática no cenário da UpFlux.

1.7 Autores

Esta Política de Segurança da Informação é de autoria do Comitê de Segurança da Informação.

A aplicação desta política, sua revisão e manutenção é de responsabilidade deste comitê. Seus respectivos integrantes estão listados em Anexo I - Integrantes do Comitê de Segurança da Informação, presente neste documento.

As dúvidas relativas à implementação desta política, bem como sugestões para alteração e melhoria, estão abertas para discussão por meio dos canais de comunicação disponibilizados pela empresa.

1.8 Divulgação e Distribuição

O conteúdo desta política de segurança deve ser divulgado a todos os colaboradores da UpFlux. A responsabilidade por esta divulgação é do Comitê de Segurança da Informação.

O conteúdo integral desta política de segurança está compartilhado a todos os colaboradores através dos canais de divulgação corporativa da empresa.

[2] https://www.upflux.net/pt/termos-e-condicoes/
[3] https://www.nist.gov/cyberframework/framework

1.9 Versão e Revisão

Esta Política de Segurança da Informação encontra-se na Versão 14, homologada em 19 de fevereiro de 2024, conforme ata do conselho de administração.

Este documento deve ser revisado e uma nova versão deve ser elaborada, homologada, divulgada e distribuída nos seguintes casos:

- Alteração significativa em um ativo de informação coberto por esta política.
- Criação de novos ativos de informação relevantes a esta política.
- No período máximo de 6 meses a partir da homologação desta política.
- A responsabilidade por disparar a revisão da política de segurança é do Comitê de Segurança da Informação.

1.10 Manutenção da Segurança da Informação

1.10.1 A UpFlux deve manter um Comitê de Segurança da Informação

a) O Comitê é responsável pela gestão da segurança da informação nos aspectos físicos e lógicos.
b) As reuniões do Comitê de Segurança da Informação deverão ocorrer com intervalo não superior a 3 meses, com os membros indicados, representantes de seus respectivos setores ou núcleos operacionais UpFlux.
c) A presença do oficial de proteção de dados (Data Protection Officer - DPO) é obrigatória para a reunião.

1.10.2 A UpFlux deve manter um Sistema de Classificação de Ativos de Informação

a) Os ativos de informação devem ser classificados de acordo com aspectos legais e requisitos de negócio.
b) A responsabilidade pelo sistema de classificação de ativos de informação é do Comitê de Segurança da Informação.
c) A responsabilidade pela classificação dos ativos de informação em cada setor é do responsável de setor.

1.10.3 A UpFlux deve realizar pelo menos uma Análise de Risco de Segurança da Informação a cada período não superior a 6 meses

a) A análise de risco deve abranger aspectos físicos e lógicos da segurança da informação.
b) A análise de risco deve resultar em um plano de ação para a redução dos riscos encontrados.

1.10.4 O UpFlux deve manter uma Política de Segurança para Fornecedores e Prestadores de Serviço

a) A Política de Segurança da Informação para fornecedores deve ser parte integrante dos contratos de prestação de serviços.
b) O UpFlux deve realizar auditorias de segurança da informação em seus fornecedores, quando as informações fornecidas forem de classificação RESTRITA ou CONFIDENCIAL.

1.10.5 A UpFlux deve manter um Plano de Continuidade de Negócio (PCN) de Tecnologia e Segurança da Informação

a) Desenvolvimento e revisão periódica do Plano de Continuidade de Negócio é do Coordenador de Segurança Lógica com o apoio do Comitê de Segurança da Informação.
b) O PCN deve conter uma relação de recursos físicos e lógicos e estabelecer a dependência entre estes recursos, para fins de continuidade de processos.
c) O PCN deve contemplar uma Análise de Impacto de Negócio contendo os principais processos de negócio da empresa com seus respectivos tempos de interrupção máxima aceitável.
d) O Plano de Continuidade de Negócio deve descrever as estratégias de continuidade para os recursos.

1.10.6 Todos os colaboradores da UpFlux devem ser treinados e conscientizados sobre Segurança da Informação

a) A responsabilidade pela aplicação dos treinamentos é do Comitê de Segurança da Informação.
b) O treinamento de segurança da informação deve estar contemplado no processo de integração de novos colaboradores.
c) Uma campanha de conscientização, com notícias e dicas de segurança da informação, que deve ser e são enviadas para todos os colaboradores, periodicamente, a cada 6 meses, conforme presente no Anexo II - Atividades cíclicas e recorrentes.
d) Adicionalmente à Política de Segurança da Informação, deve também ser desenvolvida e mantida uma Cartilha de Segurança da Informação.
e) Todos os colaboradores deverão assinar um termo de ciência da política de segurança da informação.
f) Todos os colaboradores deverão passar por avaliação quanto aos conhecimentos sobre a política da segurança da informação.
g) Uma atividade coletiva para fortalecer a conscientização sobre segurança da informação deve ser organizada a cada período não superior a 6 meses.
h) Colaboradores de alta gestão e com acesso a dados sigilosos devem passar por um preparo e capacitação mais profunda pelo seu tutor sobre aspectos e práticas de segurança.

1.10.7 O Sistema de Gestão de Segurança da Informação da UpFlux deve passar por auditorias periodicamente

a) O setor de Tecnologia da Informação (TI) e o setor administrativo são responsáveis pelo gerenciamento das auditorias de Segurança da Informação.
b) Devem ser realizadas auditorias internas por amostragem em períodos não superiores a 2 meses e externas a cada 12 meses.

1.10.8 A UpFlux deve definir políticas específicas para o tratamento de dados de pessoas físicas, conforme legislação vigente

a) Os dados de pessoa física serão controlados e tratados através de uma Política de Proteção de Dados, a qual será uma política específica derivada da Política de Segurança da Informação Organizacional.

b) O desenvolvimento, manutenção e aplicação da Política de Proteção de Dados é responsabilidade do Comitê de Segurança da Informação, sob coordenação do Setor de Tecnologia da Informação (TI) e disponível para contato no endereço de correio eletrônico ti@upflux.net.

2 Segurança Cibernética

2.1 Autenticação

a) O acesso às informações e aos ambientes deve ser permitido apenas às pessoas autorizadas pelo Proprietário da Informação, levando em consideração o princípio do menor privilégio, a segregação de funções conflitantes e a classificação da informação.
b) O controle de acesso aos sistemas deve ser formalizado e contemplar a utilização credencial de acesso.
c) A monitoração de modificações de login e credenciais com mapeamento de data, hora e origem.
d) A monitoração de acesso mapeamento de data, hora e origem.
e) A desativação de usuários afastados ou remoção de credenciais de usuários desligados. A alteração de credenciais de usuários que tenham mudado de função.
f) A revisão periódica das autorizações concedidas.

2.2 Antivírus

a) Todas as estações de trabalho de uso por parte de colaboradores, bem como gerência e diretoria, são asseguradas por solução antivírus através de ferramenta local, instalada em cada dispositivo.
b) A ferramenta de antivírus é atualizada a cada 1 semana, recebendo novas definições de vírus e ameaças, com base na base de dados da fornecedora da solução.
c) A instalação, remoção e manutenção da ferramenta de antivírus é de autorização e responsabilidade única do setor de Tecnologia da Informação (TI).
d) As varreduras em busca de anomalias ocorrem de maneira autônoma nos computadores dos colaboradores. As situações inconformes são notificadas por mensagem de correio eletrônico ao time de suporte de TI. A cada 1 semana é tarefa desta equipe analisar os registros (logs) do serviço de antivírus de maneira a identificar a existência de ocorrência de inconsistências, fazer a tratativa de quarentenas e adotar ações necessárias à normalidade de funcionamento do cenário.
e) As situações anômalas são classificadas quanto ao grau de risco. Os casos de baixíssimo e baixo risco são resolvidos como atividade trival, e os casos de alta criticidade são levados ao Comitê de Segurança da Informação, conforme previsto neste documento no item de Medidas Disciplinares.

2.3 Firewall

a) A rede interna e servidores nela presentes estão protegidos por um mecanismo de segurança de rede (firewall), baseada em uma solução proprietária do fornecedor Fortinet Fortigate 60F.

b) Este mecanismo é atualizado a cada 1 semana, recebendo novas definições disponibilizadas na base de dados da empresa fornecedora da solução aos seus clientes, assinantes do serviço.
c) A instalação, remoção e manutenção do serviço de firewall é de autorização e responsabilidade única do setor de Tecnologia da Informação (TI).

2.4 Testes de Intrusão

a) Testes de Intrusão (pentest) interno e externo nas camadas de rede e aplicação devem ser realizados no mínimo a cada 6 meses. É definida a primeira quinzena dos meses de março e de setembro para a execução das análises de segurança.

2.5 Gestão de atualizações e Varredura de Vulnerabilidades

Para garantir a segurança contínua dos sistemas e dados da UpFlux está implementada uma abordagem sistemática para a gestão de atualizações e a identificação de vulnerabilidades. Nos ambientes hospedados em provedores de nuvem, como PaaS (Plataforma como Serviço) e DBaaS (Banco de Dados como Serviço), a infraestrutura e os recursos são gerenciados conforme modelos certificados de atualização para cada plataforma. Isso assegura que os sistemas da UpFlux estejam regularmente atualizados com os patches e hotfixes mais recentes, garantindo a integridade do sistema e mitigando vulnerabilidades para manter a continuidade dos negócios, em acordo com nosso PCN.

O código desenvolvido para a solução UpFlux é analisado por mecanismos integrados de segurança, como SonarQube, em tempo de compilação e monitorado pelo Audit.NET quanto à modificação. Periodicamente, com intervalos iguais ou menores a 5 dias, o código é analizado conforme as boas práticas propostas por Open Web Application Security Project (OWASP) em sua documentação. São também utilizados OWASP Application Security Verification Standard (ASVS) e o OWASP Web Security Testing Guide, que oferecem diretrizes detalhadas para verificar a segurança de aplicações desenvolvidas. E, em complemento, utiliza-se o conjunto de ferramentas de segurança, como o OWASP ZAP (Zed Attack Proxy) associado ao mecanismo Web Application Firewall (WAF).

Em frente à ocorrência de vulnerabilidades, a aplicação de atualizações segue uma priorização com base na gravidade dos problemas analisados:

a) **Crítico:** Patches para vulnerabilidades com alto risco de exploração. Implantação em até 2 dias.
b) **Importante:** Patches para questões significativas que representam um risco potencial. Implantação em até 2 semanas.
c) **Moderado/Baixo:** Patches não críticos. Implantação em até 1 mês.

2.6 Criptografia

a) A criptografia utilizada deve seguir os padrões de segurança dos órgãos reguladores, boas práticas técnicas e regras de segurança da informação.
b) A UpFlux sempre utiliza provedores de gerenciamento de chaves do cliente ao configurar sua conexão e criptografia, conforme padrões: Amazon Web Services Key Management Service, Azure Key Vault, ou Google Cloud Platform Key Management Service.

2.7 Data Loss Prevention - DLP

a) O banco de dados está em uma rede de interconexão de nuvens privadas (Virtual Private Cloud Peering) com a infraestrutura de serviço de plataforma unificadas e integradas, aumentando desta forma a segurança.
b) Todas as conexões, por mais que estejam protegidas por firewalls e que não tenham exposição externa ainda continuam com o uso de protocolo de transporte seguro para os dados em trânsito.
c) Para prover mais segurança na criptografia do tráfego de rede e segurança dos nossos pacotes trafegados utilizamos a configuração padrão do Transport Layer Security (TLS) que criptografará todo o tráfego de entrada e saída do banco de dados, que são criptografados de acordo com protocolos típicos adotado pelo mercado (SSL/TLS Criptografia PKCS #1 SHA-256 com RSA).
d) Quanto ao descanso os dados, estes também passam por criptografia de dados para armazenamento seguro.

2.8 Rastreabilidade

a) A trilha de auditoria sempre deve ser automatizada para captar os componentes de sistema para reconstruir os seguintes eventos: os usuários, as operações aplicadas às informações, ações executadas (como a leitura, a criação, a alteração ou a remoção).

3 Segurança Lógica

3.1 Acesso à Internet

3.1.1 Diretrizes gerais

a) A UpFlux se reserva o direito de monitorar todo e qualquer acesso à internet fornecido pela empresa aos seus colaboradores, a fim de garantir o uso adequado deste recurso.
b) A UpFlux se reserva o direito de bloquear os sites que considerar inadequados, sem prévio aviso.
c) Todo o acesso à internet através da rede corporativa ou rede de visitantes deve ser feito por meios passíveis de autenticação do usuário.
d) A internet não deve ser usada para acesso a conteúdo imoral ou ilícito (ex. pornografia ou conteúdos que violem direitos autorais).
e) A internet não deve ser usada para acesso a material ofensivo ou de assédio a outros colaboradores.
f) Apenas o responsável de setor poderá autorizar o acesso à internet, para colaboradores de seu respectivo setor, através de solicitação via sistema de chamados.
g) Não é permitido ao colaborador, em nenhum caso, compartilhar o acesso à internet de seu dispositivo móvel (celular, smartphone, etc.).

3.1.2 Acesso à internet durante o expediente

a) O acesso à internet pode ser usado para fins pessoais, desde que não prejudique as atividades profissionais.

b) Deve ter acesso à internet durante o expediente apenas os usuários que necessitam deste acesso para o cumprimento de suas atividades profissionais.
c) Os usuários que possuam acessos à internet durante o expediente devem utilizá-lo exclusivamente para fins de interesse da UpFlux.

3.1.3 Acesso à internet fora do expediente

a) O acesso à internet para atividades pessoais através de equipamentos da UpFlux somente é permitido no horário do almoço e desde que o colaborador não necessite de liberação extra para tal acesso.
b) Não é permitido o acesso à internet para fins pessoais antes ou após o expediente, em nenhum caso.

3.1.4 Acesso de partes externas

a) Todo acesso à internet feito por visitantes deve ocorrer em rede específica para esta finalidade e separada da rede corporativa.
b) Quando necessário, os responsáveis por visitantes devem solicitar ao setor de Tecnologia da Informação (TI) a senha para o acesso de visitantes à internet.
c) Visitantes não devem acessar a internet através da rede corporativa, em nenhum caso.
d) A rede de visitantes da UpFlux não deve ser usada por colaboradores da empresa, em nenhum caso.
e) A responsabilidade pelo correto acesso à internet do visitante é do colaborador que o acompanha em sua visita.
f) A Rede Diretoria deve ser utilizada apenas por colaboradores formalmente autorizados pela diretoria.
g) A responsabilidade pelo uso adequado da Rede Diretoria é exclusivamente do colaborador autorizado ao uso desta respectiva rede.

3.2 Acesso à Rede Corporativa

3.2.1 Diretrizes gerais

a) A UpFlux se reserva o direito de monitorar o acesso à rede corporativa para garantir o uso adequado deste recurso.
b) O acesso à rede corporativa somente deve ser possível por meio de mecanismos de autenticação do usuário.
c) A rede corporativa somente pode ser acessada por colaboradores durante seu expediente e para fins de interesse da UpFlux.
d) A rede corporativa, durante o horário de almoço pode ser utilizada para fins pessoais, a exemplo de uso para fins acadêmicos.
e) Qualquer tipo de dispositivo tecnológico (ex. Computador portátil, pen drive, USB drive, HD externo, celular, smartphone) pessoal de colaboradores não deve se conectar à rede corporativa em nenhum caso.

3.2.2 Acesso de partes externas

a) Prestadores de serviço poderão acessar a rede corporativa exclusivamente para o desempenho de seus serviços e acompanhados por um colaborador da UpFlux.
b) Preferencialmente, as informações que um visitante necessita para o desempenho de suas atividades devem lhe ser encaminhadas por um colaborador da UpFlux, ou seja, o acesso direto do visitante à rede corporativa deve ocorrer somente em casos de estrita necessidade.
c) O acesso do prestador de serviço à rede corporativa deve ser solicitado pela liderança responsável pelo visitante, com pelo menos 24 horas de antecedência, ao setor de Tecnologia da Informação (TI).
d) O setor de Tecnologia da Informação (TI) se reserva o direito de realizar uma homologação no equipamento do prestador de serviço antes de autorizar o acesso à rede corporativa.
e) O acesso de prestadores de serviço à rede corporativa será regulado pelo contrato de prestação de serviços.

3.2.3 Acesso remoto

a) O acesso remoto de um colaborador à rede corporativa deve ser possível somente por meio de recurso exclusivamente fornecido e autorizado pelo setor de Tecnologia da Informação (TI), a exemplo de um túnel de rede virtual privada ou terminal remoto (textual, ou gráfico).
b) Somente será autorizada a conexão remota caso a entidade externa forneça todos os dados solicitados pelo setor de Tecnologia da Informação (TI) para uma conexão segura e com protocolos vigentes.
c) Quando o acesso remoto for feito por um prestador de serviços, cabe ao colaborador responsável pelo prestador de serviços avaliar a criticidade do acesso e solicitar acompanhamento do setor de Tecnologia da Informação (TI) quando julgar necessário.
d) O acesso remoto de prestador de serviços à rede corporativa deve estar limitado ao exato momento em que o prestador de serviços necessita de este acesso, sob responsabilidade do setor de Tecnologia da Informação (TI).

3.3 Armazenamento e Manuseio de Informações

3.3.1 Diretrizes gerais

a) Todas as informações corporativas devem ser armazenadas em servidores e não em estações de trabalho.
b) Informações particulares podem ser armazenadas em estação de trabalho, porém podem ser excluídas pelo setor de Tecnologia da Informação (TI) a qualquer momento e sem prévio aviso. A empresa não possui qualquer responsabilidade sobre este tipo de informação.
c) Colaboradores que utilizam computadores portáteis corporativos são responsáveis pela segurança das informações armazenadas nestes, bem como pela atualização destas informações nos servidores corporativos.
d) No caso de demissão, é responsabilidade do setor de Recursos Humanos (RH) informar ao setor de Tecnologia da Informação (TI) o desligamento do colaborador antes de informar ao próprio colaborador. Uma vez informado, é de responsabilidade do setor de Tecnologia da Informação (TI) salvar as informações corporativas do colaborador (ex. documentos em rede) antes de seu desligamento.

3.3.2 Compartilhamento de informações

a) Estações de trabalho não devem compartilhar informações pela rede, todos os compartilhamentos devem ser feitos através de servidores corporativos.
b) Todo compartilhamento deve pertencer a um setor e estar sob responsabilidade de um responsável de setor.
c) O responsável de setor deve informar ao setor de Tecnologia da Informação (TI) qualquer alteração nos direitos de acesso dos compartilhamentos sob sua responsabilidade.
d) O responsável de setor deve revisar os direitos de acesso de seus compartilhamentos periodicamente, cada 12 meses, conforme previsto no Anexo II - Atividades cíclicas e recorrentes.
e) Cada colaborador é responsável pelas informações que publica nos compartilhamentos de rede e deve garantir a informação seja publicada na destinação correta (pasta ou diretório), conforme o propósito de cada informação.
f) As informações do compartilhamento público serão excluídas periodicamente, a cada 12 meses, pelo setor de Tecnologia da Informação (TI), sem prévio aviso.
g) No compartilhamento público devem ser colocadas apenas informações temporárias e que sejam públicas, ou seja, que podem ser acessadas por todos os colaboradores.

3.3.3 Dispositivos de armazenamento removível

Entende-se por dispositivos de armazenamento removível os HDs externos, pendrives, memory stick e unidades regravaváveis de mídias óticas, entre outros meios similares de transportes físico de dados.

a) O uso de dispositivos de armazenamento removível corporativos deve ser autorizado pelo responsável de setor com justificativa e prazo determinado.
b) Dispositivos de armazenamento removível pessoal de colaboradores não podem ser utilizados para fins profissionais.
c) A autorização de dispositivos de armazenamento removível deve ser realizada por dispositivo e não por estação de trabalho.
d) Não devem ser utilizados dispositivos de armazenamento removível para troca de informações internas na empresa. Para tal deve-se utilizar a rede corporativa.
e) Dispositivos de armazenamento removível devem ser transportados de modo seguro, compatível com a criticidade da informação neles contida.

3.3.4 Backup de informações corporativas

a) O colaborador não deve fazer backup de informações corporativas por conta própria, a responsabilidade pelo backup é do setor de Tecnologia da Informação (TI).
b) Cada colaborador é responsável por garantir que suas informações importantes estão armazenadas em um servidor e incluídas no backup corporativo.
c) Em nenhum caso será feito o backup de informações pessoais/particulares de colaboradores ou mesmo de informações não corporativas.

3.3.5 Backup de informações de nossos clientes

a) Por padrão, nós utilizamos banco de dados gerenciados na região AWS Ohio que oferecerem tolerância a falhas para falhas de sistemas, junto com backup e recuperação e mecanismos

para permitir a recuperação de desastres com gerenciamento automático com log de todas as operações.

b) Todos os bancos de dados são isolados entre os clientes.

c) O processo de backup é realizado automaticamente e mantidos por até 6 meses. Por padrão temos três políticas de retenção, conforme a seguinte frequência:

   I. O backup a cada 6 horas é mantido por 3 dias.
   II. O backup semanal é mantido por 3 semanas.
   III. O backup mensal é mantido por 6 meses.

d) Os dados armazenados no UpFlux são protegidos por criptografia AES-256 com rotação de chaves de segurança, utilizando criptografia simétrica.

e) Os backups são automaticamente programados para serem executados a cada 6 horas, seguindo o Tempo de Recuperação (RTO[4]) padrão. Vale ressaltar que o RTO é diretamente influenciado pelo volume de dados, sendo que o Ponto de Recuperação (RPO[5]) pode atingir uma taxa de 5GB por hora. Em uma abordagem orientada pelos custos, proporcionamos a flexibilidade de personalizar o processo de backup, ajustando os níveis de Tempo de Recuperação (RTO) e Ponto de Recuperação (RPO) de acordo com as necessidades específicas do cliente. Há a opção de replicar os backups em múltiplas regiões e estabelecer políticas personalizadas. Esses dados são geralmente uma reprodução exata das informações armazenadas nos sistemas transacionais. Em casos de necessidade, é possível recarregar os dados diretamente da fonte, em vez de realizar uma restauração completa a partir do backup.

3.4 Propriedade Intelectual

3.4.1 Diretrizes gerais

a) Não é permitido o armazenamento de músicas e vídeos nas estações de trabalho ou servidores, exceto os de propriedade intelectual da própria UpFlux, como aqueles gerados para vídeos instrucionais.

b) Vídeos e músicas utilizados para fins corporativos devem ser armazenados e utilizados em ferramenta específica para tal finalidade, devidamente homologada pelo setor de Tecnologia da Informação (TI).

c) Não é permitido descarregar (baixar, fazer download) software comercial ou qualquer material cujo direito de uso pertença a terceiros (copyright), sem que haja um contrato de licenciamento ou outro tipo de licença de autorização de uso.

d) Cada usuário é responsável por garantir que sua estação de trabalho não viole direitos de propriedade intelectual, dúvidas devem ser sanadas com o setor de Recursos Humanos (RH).

e) O usuário não é autorizado a instalar aplicativos (softwares) por conta própria em sua estação de trabalho. Esta instalação de softwares é de responsabilidade do setor de Tecnologia da Informação (TI).

f) Solicitações de instalação de software devem ser feitas pelo responsável do setor com a devida justificativa do uso do software.

[4]Recovery Time Objective (Objetivo do Tempo de Recuperação)
[5]Recovery Point Objective (Objetivo do Ponto de Recuperação)

g) Somente podem ser executados softwares homologados pelo setor de Tecnologia da Informação (TI).
h) Documentos de propriedade intelectual da UpFlux somente poderão ser copiados, divulgados ou publicados, com autorização do responsável de setor ao qual o documento pertence.

3.5 Uso de Sistemas Corporativos

3.5.1 Diretrizes gerais

a) As definições de direitos de acesso nos módulos de sistemas corporativos são de responsabilidade do responsável de setor ao qual o módulo pertence.
b) As solicitações de direitos de acesso devem, primeiramente, ter um parecer do analista de suporte responsável pela segurança da informação.
c) Sempre que necessário o responsável de setor deverá solicitar ao setor de Tecnologia da Informação (TI) a alteração de direitos de acesso em seus módulos.
d) Cada colaborador somente deve ter acesso aos sistemas corporativos na medida de suas necessidades profissionais.
e) Pelo menos a cada 12 meses os direitos de acesso aos sistemas corporativos devem ser revisados pelo responsável de setor, sob responsabilidade do Comitê de Segurança da Informação.
f) O acesso aos sistemas corporativos deve ser feito por meio de credenciamento, com uso de par de usuário e senha que identifique o colaborador de maneira única antes de qualquer ação no sistema.
g) Os sistemas corporativos devem fornecer controle de acesso que possibilite a liberação de acessos somente às funções estritamente necessárias a cada colaborador.

3.6 Uso de e-mails

3.6.1 Diretrizes gerais

a) O e-mail corporativo pertence à UpFlux e pode ser monitorado quando esta julgar necessário, sem prévio aviso.
b) Somente deve ter acesso ao envio e recebimento de e-mail os colaboradores que necessitem deste recurso para suas atividades profissionais.
c) O e-mail corporativo deve ser usado para fins profissionais e excepcionalmente para fins pessoais, desde que não prejudique as atividades profissionais.
d) O colaborador não deve encaminhar e-mails cujo conteúdo não tenha relação com o trabalho.
e) O colaborador não deve cadastrar o e-mail corporativo em formulários ou listas de discussão que não tenham relação com o trabalho (ex. compras on-line).
f) As mensagens de correio eletrônico relacionadas com o trabalho não devem ser enviados para destinatários não relacionados com a informação (ex. para o e-mail pessoal do colaborador).

3.6.2 Uso do e-mail pessoal

a) O colaborador não poderá acessar o e-mail pessoal ou qualquer e-mail não administrado pela UpFlux durante o expediente, em nenhum caso.
b) Fora do expediente é permitido o acesso ao e-mail pessoal do colaborador, desde que o colaborador não precise de liberações de acesso adicionais para tal uso.

3.7 Uso de Senhas

3.7.1 Diretrizes gerais

a) A senha do usuário é pessoal e intransferível e o usuário será responsabilizado pelas ações realizadas autenticado com sua senha.
b) As senhas de usuários não devem ser compartilhadas com outros usuários ou mesmo com o setor de Tecnologia da Informação (TI), em nenhum caso. No ato da criação de cada senha destinada aos colaboradores é definido de maneira impositiva a troca desta senha após o primeiro acesso, preservando assim a pessoalidade desta credencial.
c) As senhas de colaboradores, quando criadas ou alteradas pelo setor de Tecnologia da Informação (TI), devem impor um grau de complexidade de não-memorização, contendo no mínimo oito caracteres, alternância entre letras minúsculas e maiúsculas, caracteres especiais e números, em vez de senhas padrão ou com elementos mnemônico. Informações pessoais não devem fazer parte da senha do usuário, bem como sequências previsíveis de letras ou números.
d) Em caso de demissão, o setor de Recursos Humanos (RH) deve solicitar ao setor de Tecnologia da Informação (TI) que todas as credenciais do colaborador desligado sejam desabilitadas, conforme manual de procedimentos (Políticas nos processos internos) de desligamento de colaboradores.
e) Em caso de mudança de setor de colaborador, o responsável de setor ao qual o colaborador está saindo deve solicitar ao setor de Tecnologia da Informação (TI) o bloqueio de todos os acessos do colaborador ao seu setor.
f) Em caso de férias de funcionários o setor de Recursos Humanos (RH) deve informar ao setor de Tecnologia da Informação (TI) a situação de férias para que o setor de Tecnologia da Informação (TI) faça o bloqueio temporário das credenciais do funcionário.
g) A integração de mecanismos de credenciamento e autenticação é feito com pareamento de chaves fortes, a fim de estabelecer a relação de confiança entre os serviços de diretórios de autenticação de usuários (Microsoft Active Directory, Microsoft Entra, OpenID, etc.).
h) A autenticação dos colaboradores no serviço de diretório de contas ocorre com camada adicional de segurança por meio de fator de segunda ou múltiplas camadas de proteção. A ativação deste recurso é imposta automaticamente após a troca da senha do primeiro acesso do colaborador.
i) A renovação de senhas temporárias deve ser imposta após o primeiro acesso do usuário proprietário da conta, definindo assim a personificação e exclusividade no conhecimento desta informação de credencial.

3.7.2 Senhas institucionais

a) Todas as senhas institucionais devem possuir um responsável formalmente definido.

b) Somente o responsável formalmente definido pode administrar os direitos de acesso da conta institucional.
c) As senhas institucionais podem ser compartilhadas somente após autorização formal do responsável formalmente definido.
d) As senhas institucionais devem ser alteradas sempre que um colaborador que possuía a senha seja transferido ou desligado.
e) As senhas institucionais devem estar relacionadas com um e-mail corporativo para recuperação de senhas, e nunca relacionadas com e-mails pessoais.

3.8 Software de Mensagens Instantâneas

3.8.1 Diretrizes gerais

a) Somente poderão ser utilizados softwares de mensagens instantâneas devidamente homologados pelo setor de Tecnologia da Informação (TI). Atualmente, o serviço apto a esta finalidade é o produto Microsoft Teams.
b) A UpFlux se reserva o direito de monitorar o uso dos softwares de mensagens instantâneas corporativos.
c) Somente deve ter acesso a contatos externos de mensagens instantâneas os colaboradores formalmente autorizados responsável de setor ao qual o colaborador pertence.
d) Os softwares de mensagens instantâneas devem ser utilizados exclusivamente para fins profissionais, sem exceções.
e) Colaboradores não devem fazer uso de contas pessoais de softwares de mensagens instantâneas, em nenhum caso.

3.9 Gerenciamento de Partes Externas

3.9.1 Diretrizes gerais

a) Toda execução de serviço por partes externas deve estar associada a um setor específico, sendo que o responsável de setor será também responsável pelas atividades da parte externa dentro da UpFlux.
b) O responsável de setor deve garantir que a parte externa tenha acesso somente às informações estritamente necessárias.
c) Conforme necessidade, o responsável de setor poderá solicitar a assinatura de um termo de confidencialidade contendo a definição de todo o ciclo de vida da informação passada à parte externa.
d) Todos os contratos de prestação de serviço devem incluir cláusulas que responsabilizem o prestador de serviço pelo uso adequado das informações, sistemas e recursos aos quais ele tiver acesso.

3.10 Ambientes de Segurança Física

3.10.1 Diretrizes gerais

a) A UpFlux se reserva o direito de monitorar seus colaboradores em seu ambiente de trabalho, respeitando sempre os dispositivos constitucionais fundamentais como a intimidade, vida privada, honra e imagem.

b) Todos os colaboradores devem informar a portaria ou o responsável pela segurança física sobre deficiências em controles de segurança física (portas, janelas, alarme, luzes, etc.) quando observados.
c) Os locais que possuem sistema de monitoramento devem apresentar placas informativas sobre o monitoramento.

3.10.2 Fotos e Vídeos em ambiente interno

a) Fotos e vídeos em ambiente interno à empresa somente podem ocorrer através de equipamentos corporativos e para fins de interesse da empresa.
b) Fotos e vídeos de quaisquer documentos ou informações da empresa somente para ocorrer através de equipamentos corporativos e para fins de interesse da empresa.
c) Partes externas não podem utilizar seus próprios equipamentos para retirada de fotos e vídeos na empresa, quando necessário as fotos e vídeos devem ser registradas por equipamentos da UpFlux e depois compartilhadas com a parte externa envolvida.

3.10.3 Diretrizes para perímetro externo

a) O perímetro externo deve possuir monitoramento de vídeo 24x7 e a iluminação deve ser adequada, de modo a permitir boa qualidade do monitoramento.
b) A UpFlux deve manter portaria 24x7 com ronda periódica de segurança física.
c) O perímetro externo deve possuir barreiras físicas que impeçam a entrada não autorizada de pessoas.
d) Os portões que fornecem acesso à empresa devem permanecer fechados enquanto não estiverem sendo utilizados.
e) Os acessos ao ambiente de operações devem ser assegurados por tecnologia de identificação biométrica.

3.10.4 Diretrizes para perímetro interno

a) Os dispositivos de rede (switches) da empresa devem possuir proteção de acesso físico, a fim de prevenir o uso/acesso por pessoas não autorizadas.
b) Todos os setores devem ter armários e/ou gavetas com chaves para o armazenamento de documentos que contenham informações importantes.
c) A critério do responsável de setor, salas devem permanecer trancadas quando não estiverem em uso.

3.10.5 Acesso de partes externas

a) A entrada e saída de visitantes devem ser registradas na portaria, com data, hora e responsável interno pelo visitante.
b) Os visitantes devem ser recebidos na recepção por um colaborador que deve acompanhá-los durante toda a visita.
c) Visitantes ficam sob responsabilidade do colaborador que o acompanha.
d) Veículos de partes externas somente podem entrar na empresa quando isto for estritamente necessário para o desempenho de sua atividade profissional.

3.11 Controle de Equipamentos de Tecnologia

3.11.1 Diretrizes gerais

a) Os equipamentos de tecnologia da informação fornecidos pela UpFlux são de propriedade da empresa e devem ser utilizados para atender aos interesses da empresa.
b) Cada colaborador é responsável pelo uso adequado dos equipamentos de tecnologia da informação fornecidos a ele pela UpFlux. As dúvidas sobre o uso adequado devem ser sanadas com o setor de Tecnologia da Informação (TI).
c) O uso de notebooks e celulares corporativos disponibilizados pela UpFlux deve ser autorizado somente após assinatura de termo de responsabilidade sobre a segurança da informação para uso deste equipamento.
d) A UpFlux não se responsabiliza por quaisquer tipos de equipamentos pessoais em suas instalações físicas.

3.11.2 Movimentação de equipamentos

a) Apenas prestadores de serviços formalmente autorizados podem sair com equipamentos da UpFlux para manutenção, mediante apresentação de Nota Fiscal (NF) na recepção.
b) Nenhum equipamento poderá ser retirado da UpFlux para fins pessoais de quaisquer colaboradores.
c) A movimentação de equipamentos de tecnologia da informação dentro da UpFlux deve ser realizada exclusivamente por colaboradores do setor de Tecnologia da Informação (TI). Esta movimentação é registrada em plataforma de gerenciamento (Gestionnaire Libre de Parc Informatique - GLPI).

3.11.3 Uso de dispositivos móveis pessoais

a) Colaboradores podem fazer o uso de dispositivos móveis pessoais como celulares e smartphones dentro das dependências da empresa, desde que observadas todas as diretrizes desta política de segurança da informação e dos documentos relacionados.
b) Colaboradores não devem fazer uso de computadores pessoais (notebooks, desktops, etc.) dentro das dependências da empresa, exceto com autorização formal da diretoria.

3.12 Controle de Documentos Físicos

3.12.1 Armazenamento de documentos físicos

a) Documentos importantes, a critério do responsável de setor, devem ficar armazenados em local que impeça o acesso de pessoas não autorizadas (ex. armário ou gaveta com chaves).
b) Ao deixar seu local de trabalho o colaborador deve se certificar de que documentos importantes estejam devidamente armazenados.
c) O ambiente do arquivo morto deve permanecer trancado quando não estiver em uso.
d) Somente colaboradores autorizados por seu responsável de setor podem ter acesso ao arquivo morto, sob responsabilidade da portaria/segurança.
e) Ao ser transferido de setor ou se desligar da empresa o colaborador deve fazer a devolução formal dos documentos físicos que estão em sua posse, sob responsabilidade do responsável de setor.

3.12.2 Manuseio de documentos físicos

a) A saída de documentos de um determinado setor pode ser controlada através de um sistema de protocolo de documentos, a critério de cada responsável de setor.
b) O descarte de documentos impressos importantes deve ser realizado através de picotadora de papel, ao invés de serem reaproveitados, por exemplo, para rascunho de impressoras.
c) Partes externas somente podem ter acesso a documentos físicos para o estrito cumprimento de suas atividades profissionais e com a ciência do responsável de setor ao qual o documento pertence.

3.13 Controle de Chaves e Alarmes

3.13.1 Chaves externas

a) A administração deve manter um inventário de chaves de todos os ambientes físicos relevantes para segurança da informação e patrimonial.
b) O inventário de chaves externas deve ser revisado a cada 6 meses pelo setor de segurança patrimonial.
c) As chaves de todos os setores devem ficar na portaria, podendo ser retiradas somente por colaboradores devidamente autorizados por seu respectivo responsável de setor.
d) A portaria deve registrar toda utilização de chaves externas por parte de colaboradores.

3.13.2 Chaves internas

a) Somente colaboradores devidamente autorizados por seu superior imediato podem possuir chaves internas de seus setores. Ao ser transferido ou desligado o colaborador deve devolver todas as chaves que estão em sua posse, sob responsabilidade do setor de Recursos Humanos (RH).
b) Deve haver um inventário de chaves internas com responsável e justificativa das liberações, sob responsabilidade da segurança patrimonial.
c) As chaves pertencentes à armários e gavetas podem ficar em posse de respectivos colaboradores.

4 Políticas nos processos internos

A UpFlux possui um Guia de Processos bem definido em suas subdivisões:

Em **Suporte e Operações** tem-se o processo de:

- Gestão de incidentes (dúvidas, atividades operacionais e técnicas).
- Requisição de melhorias para a plataforma ou App.
- Gestão de Mudança - GMUD.
- Gestão de problemas.
- Requisição para Site Reliability Engineering (SRE) / Infra.

Em **Continuidade e Segurança**, tem-se processo para:

- Resposta a incidente de segurança e gestão de vulnerabilidades.
- Comunicação de falhas e relações públicas.
- Investigações forenses e auditoria externa.
- Contratação e seleção de provedores de computação em nuvem.
- Continuidade e criticidade de serviços virtuais e ativos.
- Recuperação de desastre.

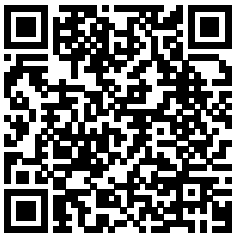
Para a Liberações de acesso para colaboradores, estão bem definidos os processo de:

- Contratação e liberações de acesso - Novos colaboradores.
- Liberação de acesso - Novos acessos para colaboradores.
- Eliminação acessos e dados - Desligamento de colaboradores.

Não diferente, estão bem definidos os processos para:

- Canais e Parcerias, com Guia de Processos de Canais.
- Vendas Diretas, com Processo de Vendas.
- Sucesso do Cliente, com o Guia de Processos de Customer Value.
- Pré-Vendas, com Guia de Processos de Pré-Vendas.
- Vendas Indiretas, com Guia de Processos de Canais.

Estes processos bem documentados estão disponíveis por meio do acesso ao código gráfico (QR-Code) a seguir.



5 Medidas Disciplinares

As medidas disciplinares para um incidente de segurança serão discutidas e deliberadas pelo Comitê de Segurança da Informação.

A aplicação de medidas disciplinares é responsabilidade do gestor/superior imediato do setor acompanhado de dois membros do Comitê de segurança da informação.

São medidas disciplinares:

- Reforço de conscientização.
- Advertência não registrada (verbal).
- Advertência registrada ou escrita.
- Suspensão de direito de acesso ou recurso.
- Desligamento com ou sem justa causa.
- Processos jurídicos na esfera civil ou criminal.
- Outras medidas disciplinares definidas pelo Recursos Humanos (RH) e pelo setor jurídico.

E por estar de acordo com as diretrizes e normas definidas neste documento de Política de Segurança da Informação, a administração da UpFlux se compromete com a distribuição, divulgação, manutenção e aplicação deste documento em sua organização.

Cleiton dos Santos Garcia
Diretor e Cofundador

Anexo I - Integrantes do Comitê de Segurança da Informação

Os integrantes do CSI estão elencado a seguir, em ordem alfabética, conforme definido na homologação deste documento em 19 de fevereiro de 2024:

- Cleiton dos Santos Garcia (cleitonsg@upflux.net)
- Maib Ferreira de Oliveira (maib@upflux.net)
- Trober Jaime Machado (trober.j@upflux.net)

[fim da lista]

Anexo II - Atividades cíclicas e recorrentes

Cronograma de Atividades Cíclicas e Recorrentes

As atividades cíclicas e recorrentes prevista neste documento, em versão 14, com data de homologação de 19 de fevereiro de 2024 estão presentes da tabela a seguir:

Atividade	Frequência
Revisão do PSI	A cada 6 meses
Reunião do CSI	A cada 3 meses
Análise de Risco	A cada 6 meses
Semana de Conscientização	A cada 6 meses
Auditoria Interna	A cada 2 meses
Auditoria Externa	A cada 12 meses
Análise do antivírus	A cada 1 semana
Análise do firewall	A cada 1 semana
Teste de penetração (pentest)	A cada 6 meses
Acesso de partes externas	A cada 24 horas
Revisão de sistemas corporativos	A cada 12 meses
Controle de chaves externas	A cada 6 meses
Varreduras de Vulnerabilidades	A cada 5 dias
Gestão de atualizações críticas	Em até 2 dias
Gestão de atualizações importantes	Em até 2 semanas
Gestão de atualizações moderadas	Em até 1 mês

Tabela 1: Cronograma de atividades cíclicas e recorrentes

Página de assinaturas

Cleiton Garcia
979.315.510-87
Signatário

HISTÓRICO

22 fev 2024 09:19:47 — **Taynara Caroline da Silva Cambruzzi** criou este documento. (E-mail: taynara.c@upflux.net)

23 fev 2024 13:59:04 — **Cleiton dos Santos Garcia** *(E-mail: cleitonsg@upflux.net, CPF: 979.315.510-87)* visualizou este documento por meio do IP 131.100.93.87 localizado em Jaraguá do Sul - Santa Catarina - Brazil

23 fev 2024 13:59:13 — **Cleiton dos Santos Garcia** *(E-mail: cleitonsg@upflux.net, CPF: 979.315.510-87)* assinou este documento por meio do IP 131.100.93.87 localizado em Jaraguá do Sul - Santa Catarina - Brazil